Study on the Intention and Behavior Complying with Accounting Information System Security Policy: The Case of Vietnam

Trung Nguyen Quoc(✉) and Binh Nguyen Huu

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

Abstract. The digital-driven economy leads to many opportunities and many challenges for businesses concerning information system security. This is the reason why more managers concentrate on promulgating and enforcing accounting information system security policies. Research on AISSP compliance behavior, therefore, receives much attention from researchers. However, research on this topic is still very limited in Vietnam. In business practice, organizations usually use sanctions to deter employees who do not comply with the security policy. However, previous research results show inconsistency regarding the effectiveness of a motivated as well as a deterrent approach to compliance. These different results can be explained based on cultural differences as previous studies argued that research on information systems security policy compliance behavior based on motivation and deterrence mechanisms needs to be considered in the impact of a specific cultural factor. This motivated us to research AISSP compliance in the context of Vietnam. This study explores the cognitive factors and personal characteristics affecting the intention and behavior to comply with accounting information system security policy (AISSP) based on deterrence theory, protection motivation theory, and the theory of reasoned action. Our results demonstrate that the intention and behavior of accountants to comply with AISSP are positively influenced by the punishment severity, AISSP compliance attitude, response efficacy, and uncertainty avoidance. The results add to the body of literature and inform future research on AISSP compliance. From the management aspect, the results help organizations recognize the problems that need to be addressed to ensure AISSP compliance from accountants.

Keywords: Punishment Severity · Uncertainty Avoidance · Response Efficacy · AISSP Compliance Attitude · Intention To Comply With AISSP · and AISSP Compliance Behavior

1 Introduction

In the current digital world, businesses are facing many threats to information systems in general and accounting information systems in particular. The more the operation of the accounting information system is increasingly supported by the Internet and information

© The Author(s) 2023
P. Tra Lam and P. Quang Huy (Eds.): ICECH 2022, AEBMR 238, pp. 77–92, 2023.
https://doi.org/10.2991/978-94-6463-150-0_6

technology advances, the more these threats enlarge. If organizations and system users are not fully aware of dangers and their systems are not well protected, they face an increasing level of this system security risk.

Coping with these challenges, from the management aspect, information system security policies are issued to guide and direct the behavior of system users to achieve the accounting information system security objective. The problem, however, is that system users (i.e. employees, managers, etc.) do not always voluntarily comply with the information system security policy dealing with their coping appraisal, such as response efficacy [42]. Therefore, enforcing information system security policies is a primary concern of managers. As result, organizations often promote their coping appraisal of potential loss or damage arising from the threatening event as well as use sanctions to deter employees who do not comply with the security policy.

From the research aspect, more and more researchers are interested in the security policy issues and policy compliance behavior of system users [3]. Many studies have applied deterrence theory to explain the influence of the sanctioning mechanism on the intention and behavior to comply with the information system security policy [25]. However, previous research results show inconsistency regarding the effectiveness of a deterrent approach to compliance [39]. The cause of the problem may stem from the effect of cultural differences. [10] show that there is a difference in compliance behavior with information security policies and procedures between employees with different cultural characteristics. According to [2], divergent culture is believed to influence the psychology of individuals. Thus, individuals with different cultures will respond dissimilarly to individual information system security policies compliance behavior mechanisms. In addition, studies have shown that distinct culture has a powerful influence on individual attitudes and behavior. In the field of information systems, research results suggest that different culture influences the development, adoption, use, and management of organizational information systems [9].

The above analysis shows that research on information system security policy compliance behavior based on motivation and deterrence mechanism needs to be considered in the effect of individual different cultural characteristics such as uncertainty avoidance. Specifically, uncertainty avoidance has been treated at an aggregate level as a characteristic of cultures [16]; this term is defined as the extent to which the members of a culture feel threatened by uncertain or unknown situations [17]. However, few studies have examined the effect of culture on information systems security compliance behavior [19]. Therefore, this study aims to propose a research model of security policy compliance behavior based on protection motivation theory, deterrence theory as well as the effect of uncertainty avoidance. Understanding the influence of different cultures not only helps explain the empirical discrepancy among studies but also guides further theory development [39].

The remainder of this paper is arranged as follows: In the next section, our research hypotheses are developed based on theories and focus on the influence mechanism of significant predictors on AISSP compliance behaviors; and the research model is then proposed. Then, the research methodology is presented to show how we conduct the study. Next, analyses and results are performed. Finally, the discussion and conclusion are presented.

2 Theoretical Background and Statements of Hypotheses

2.1 AISSP Compliance Behaviors

Dominant and used most often theories in the studies of Information Systems Security Policy (ISSP) are Deterrence Theory (DT), Technology Acceptance Model, Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), and Protection Motivation Theory (PMT) [25]. It should be noted that each theory can be applied independently or in combination with other theories to discover antecedents affecting ISSP compliance behaviors that depend on the corresponding research context.

By definition, ISSP compliance behavior is the act of complying with the requirements for employee responsibilities and obligations, managing organizational security, understanding the sanctions, and coping against the non-compliance act [38]. Besides, according to [37], ISSP compliance behavior is also demonstrated by measuring how individuals encourage and support others in the organization to comply with ISSP.

Researchers tend to use a combination of theories to explain the effects of antecedents on individuals' ISSP compliance behaviors, such as PMT, TRA, and GDT [26]; PMT and Social cognitive theory [43]; PMT and GDT [15]; PMT and TPB [20]; PMT and GDT [41].

This study uses a combination of PMT [31], DT [6], and TRA [11] and aims to explain and establish the influence mechanism of significant predictors on AISSP compliance behaviors.

2.2 Punishment Severity

In the study of the deterrence theory of [6], sanctions are represented by a construct: punishment severity, which means the severity of deterrence. When the penalty for the violation is severe (punishment severity), DT predicts that potential offenders will be inhibited from engaging in antisocial behavior. [27] also conclude that the severity of the penalty significantly affects the attitude toward an organization's software copyright infringement. Besides that, the perceived severity of sanctions has a mediating effect on the relationship between security countermeasures and the intention to misuse information systems [19]; this shows that non-compliance with security policies can be prevented by imposing penalties. When avoiding punishment resulting from ISSP non-compliance actions, [38] assumes that employees will develop their perception of certainty and severity due to their personal and observational experiences of sanctions. [41] indicated that sanction severity has a direct effect on ISSP compliance intention. Besides that, [4] concluded that attitude toward compliance has a mediating effect on the relationship between perceived sanction severity and behavioral intent. Furthermore, [33] showed that sanction severity positively influences employees' attitudes toward preventing delinquent behavior in the domain of information security. Thus, the seriousness of detection has an impact on the individual's intentions to comply with AISSP; we propose the hypothesis:

H_{1a}: Punishment severity has a positive effect on the intention to comply with accounting information systems security policy.

H_{1b}: Punishment severity has a positive effect on accounting information systems security policy compliance behaviors.

2.3 Uncertainty Avoidance

According to [18], all human beings have to face the fact that we do not know what will happen tomorrow: the future is uncertain, but we have to live with it anyway. And ways of handling uncertainty are part and parcel of any human institution in any country. Uncertainty avoidance is one of the dimensions of national culture, which can be defined as the "extent to which the members of a culture feel threatened by ambiguous or unknown situations" [18]. Rather than leading to reducing risk, uncertainty avoidance leads to a reduction of ambiguity. So people in uncertainty-avoiding cultures look for structure in their organizations, institutions, and relationships that makes events interpretable and predictable.

[18] argue that people in a strong uncertainty avoidance society usually need laws and regulations, which can lead to rules or rule-oriented behaviors. But countries with weak uncertainty avoidance can show the opposite. People think that regulations should be established only in case of absolute necessity. They believe that many problems can be solved without formal regulations. But the paradox here is that although rules in countries with weak uncertainty avoidance are less sacred, they are often better followed. These arguments show that people in different uncertainty avoidance cultures show different perceptions, attitudes, and behavior toward the need for rules to follow the regulations. In countries with weak uncertainty avoidance, a feeling prevails that if laws do not work, they should be withdrawn or changed. In countries with substantial uncertainty avoidance, laws can fulfill a need for security even if they are not followed [18].

In the context of ISSP compliance research, [39] argue that, for individuals high in uncertainty avoidance, sanctions can be treated as a mechanism to deter them from non-compliance behaviors because this research result shows that higher degrees of uncertainty avoidance will decrease risk-taking [24]. Safety or security is likely to prevail over other needs where uncertainty avoidance is strong [18]. This means that if individuals fear uncertainty, they prefer to maintain attitudes, intentions, and behaviors in ISSP compliance than being non-compliant with those as the chance of getting detected and facing an uncertain outcome.

Accordingly, the following hypotheses are posited for examining the effect of uncertainty avoidance on the individual's AISSP compliance behavior mechanisms:

H_{2a}: Uncertainty avoidance has a positive effect on the intention to comply with accounting information systems security policy.

H_{2b}: Uncertainty avoidance has a positive effect on accounting information systems security policy compliance behaviors.

2.4 Response Efficacy

Response efficacy comes from the structure coping appraisal of protection motivation theory. Based on PMT, according to [42], coping appraisal refers to an individual's ability to manage and prevent potential loss or damage arising from a threatening event.

Specifically, response efficacy is related to beliefs about the benefits obtained from the actions taken by the individual [32]. This means, if an individual has less confidence in the effectiveness of a measure to cope the threats, this individual may not be willing to accept it [30]. For the scope of this article, response efficacy is the belief of employees that compliance with the AISSP will effectively reduce a safety threat. Accordingly, the individuals believe that when the ISSP in their organization has guidelines and coping mechanisms to prevent threats and dangers effectively, they are more likely to develop their attitude and intention to adopt this policy [15]. [15] also note that PMT explains the influence of motivational factors, including response effectiveness and self-efficacy, on the compliance behavior of individuals in different contexts, thereby showing the importance of improving employee motivation and examining the influence of these factors on compliance behavior. In addition, based on PMT, [22] indicate that response efficacy has a positive impact on employee behavioral intent in using antispyware software tools.

Similarly, according to [26], coping appraisal positively affects the intention to comply with ISSP by mediating the role of attitude towards ISSP compliance. In an experimental research model, [20] also asserts that self-efficacy, response efficacy, and attitude toward compliance also positively influence ISP behavioral compliance intentions of employees. On these bases, the following research hypotheses are proposed:

H_{3a}: Response efficacy has a positive effect on the intention to comply with accounting information systems security policy.

H_{3b}: Response efficacy has a positive effect on accounting information systems security policy compliance behaviors.

2.5 AISSP Compliance Attitude

In the context of ISSP compliance behaviors, many research results using the theory of reasoned action show that attitude has a positive effect on the intention of individuals to comply. [7]; [20], [21]; [26]; [34]; [35]. In this study, the attitude to comply with ISSP addresses the importance, benefits, and usefulness of adopting security technology and practices [15]. Experimental studies on the mechanism of action of attitude to comply with ISSP achieved the following results: [20] affirms that attitude toward compliance positively influences ISP behavioral compliance intentions of employees. Next year, [4] indicates that attitude, perceived behavioral control, organizational commitment, and subjective norms significantly affect behavioral intent. Continuing this research trend, [5] publish attitude and intention are substantial predictors of actual early compliance behavior towards information security policy. On these bases, the following research hypotheses are proposed:

H_{4a}: Accounting information systems security policy compliance attitude has a positive effect on the intention to comply with accounting information systems security policy.

H_{4b}: Accounting information systems security policy compliance attitude has a positive effect on accounting information systems security policy compliance behaviors.

2.6 Intention to Comply with AISSP

According to the model of theory of reasoned action theory, a person's behavior is determined by an individual's behavioral intention to perform it. Ajzen (1985) has indicated that several factors can influence the relationship between intention and behavior. The intention is the immediate antecedent of behavior, considered to be under the control of the will. In other words, TRA concludes that individual behavior is controlled by behavioral intention, where behavioral intention is a function of personal attitudes and subjective norms for behavioral performance. Thus, previous research theories have shown that the intention to comply with ISSP affects the behavior of ISSP compliance.

Besides, the relationship between intention and behavior has been extensively tested in the theory of PMT, GDT, and TPB. Siponen, Pahnila, and Mahmood (2006) studied the effect of PMT concepts on intentions and behaviors to comply with ISSP. [38] researched the impact of GDT constructs on ISSP behavioral intention and compliance. All of these studies concluded that the intention to comply with ISSP impacts ISSP compliance behavior. Thus, we propose the hypothesis:

H_5: Intention to comply with accounting information systems security policy has a positive effect on accounting information systems security policy compliance behaviors.

In summary, based on summarizing and arguing related theories, a theoretical model has been built showing the relationship between six research concepts, including: (1) Punishment severity; (2) Uncertainty avoidance; (3) Response efficacy; (4) AISSP compliance attitude; (5) Intention to comply with AISSP; (6) AISSP compliance behaviors.

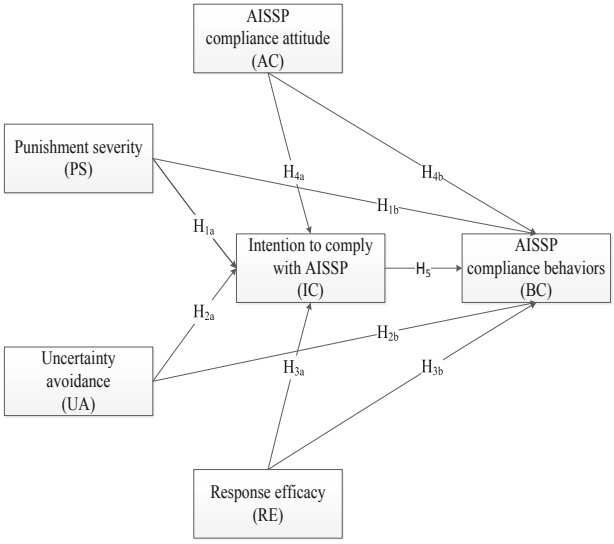

Fig. 1. Proposed research model

3 Research Methodology

3.1 Data Collection and Participants

This study used a self-administrated questionnaire for collecting data from accountants in organizations in Vietnam. The accountants, including the chief accountant, general accountants, and accountants, were chosen to be the potential informants because this study aims to investigate compliance behavior toward AISSP. Accountants are direct users who use accounting information systems for collecting, storing, processing, and providing information so the security of accounting information systems is strongly dependent on their attitude and behaviors toward AISSP.

Potential informants were selected by convenience sampling - a non-probability sampling technique. The survey forms were sent to 300 email addresses of potential informants through the Google form tool from May 30th, 2021 to June 15th, 2021. We invited each of these potential informants individually to participate by sending an invitation emailed to them, attached with a link to the questionnaire on Google form. To convince the participants, we explained in the invitation the purpose of the study, ensured the confidentiality of the potential informants' identities and the information they would provide, as well as offered to provide them with a summary of the results if they needed.

With a total of 300 questionnaires sent, the study received 240 responses, corresponding to a response rate of 80%. After eliminating 26 invalid responses from respondents who is not accountant, incomplete responses, feedback with response time being too short, etc., the study got 214 valid responses. The respondents' profiles in Table 1 show that almost respondents are female, with a rate of 87, 85%. There are 57,94% of organizations spending budget on maintaining AISSP, and 75,70% of those have applied for AISSP over six months.

3.2 Variable Measurement

This study employs a five-item scale developed by [38] to measure AISSP compliance behaviors. Intention to comply with AISSP, punishment severity, and AISSP compliance attitude, each of them was measured by a three-item scale adapted from [15]. To measure uncertainty avoidance, a scale including seven items developed by [23] is employed. In terms of response efficacy, the study measured this variable by a three-item scale adapted from [40]. Respondents were required to verify their agreement with statements pertaining to these items, on a scale ranging from 1 = "strongly disagree" to 7 = "strongly agree.

Table 1. Profiles of respondents.

	Frequency *(n=214)*	Percentage		Frequency *(n=214)*	Percentage
Gender			*Firm size (assets in VND billion)*		
Male	26	12,15	≤10	57	26,64
Female	188	87,85	11–50	45	21,03
Age			51–100	35	16,36
< 25	33	15,42	101–200	15	7,01
25-34	135	63,08	201–500	13	6,07
35-44	36	16,82	501–1.000	10	4,67
> 44	10	4,67	>1.000	39	18,22
Industry sector			*Firm size (full-time equivalent employees)*		
Banking, insurance, investment funds	11	5,14	≤ 50	94	43,93
Chemicals and pharmaceuticals	6	2,80	51–200	69	32,24
Milk, food, and meat products	6	2,80	201–500	23	10,75
Electricity and electronics	9	4,21	501–1.000	12	5,61
Health and social aid	11	5,14	1,001–5,000	9	4,21
IT	4	1,87	5,001–10,000	1	0,47
Processing industry and manufacturing	31	14,49	>10,000	6	2,80
Wholesale and retail	41	19,16	*Industry type*		
Telecommunication	3	1,40	Manufacturing	52	24,30
Transport and warehouse	14	6,54	Commerce	43	20,09
Construction	22	10,28	Service	76	35,51
Others	56	26,17	Manufacturing, Service	5	2,34
Type of Ownership			Manufacturing, Commerce	10	4,67
100% foreign-owned enterprise	53	24,77	Commerce, Service	20	9,35
SOEs (≥ 51% states capital)	18	8,41	Manufacturing, Commerce, Service	8	3,74
Private company	128	59,81	*Budget for maintaining AIS security*		
Joint venture with international partner	6	2,80	Yes	124	57,94
Joint venture with a local partner	5	2,34	No	90	42,06
Others	4	1,87	*Time AISSP has been applied*		
			≤ 6 months	52	24,30
			> 6 months	162	75,70

4 Analyses and Results

4.1 Common-Method Bias

A potential problem is common method bias which could cause spuriousness in relationships among the variables in the model [28], as this study uses a collection of cross-sectional data using a key informant approach. Thus, we use Harman's single-factor test (with the support of SPSS software) to assess the common method bias problem. The analysis results show that no factor accounts for most of the variance; the first factor only accounts for 29.202% of the total variance extracted from the whole model. Therefore, it can be concluded that there is no evidence of common-method bias in this study [28].

4.2 Measurement Model

The study employed the PLS-SEM approach for assessing the psychometric properties of the theoretical model and proposed hypotheses. Data analysis was conducted by using SmartPLS 3.2.7 [29]. The measurement model results, including indicator loadings, average variance extracted (AVE), and composite reliability for evaluating the adequacy of outer-measurement models, were presented in Table 2. The results show that, excepting uncertainty avoidance, factor loadings of all remaining items were above the recommended threshold of 0.708 [13]. This demonstrates that the individual indicator reliabilities are satisfied. For uncertainty avoidance, the results show four of seven items had factor loadings lower than the recommended threshold of 0.708 [13]. Thus, these items were eliminated from the scale, after considering the content validity. The remaining three of the seven items (depict in Table 2) were kept for further analysis. The scale's internal consistency reliability was evaluated using Fornell and Larcker's (1981) measure of composite reliability. As presented in Table 2, all composite reliabilities range from 0.846 to 0.951, and this suggests a satisfactory scale of internal reliability [13]. Furthermore, AVE values for all constructs, ranging from 0.648 to 0.814, are greater than 0.5, following [13]. These results demonstrate adequate convergent validity of the outer-measurement models.

In terms of discriminant validity, the procedure recommended by Fornell and Larcker (1981) was employed for accessing this validity by comparing the square root of the AVE statistics with the correlations among the latent variables. The results in Table 3 depict that the square roots of the AVEs for each construct, ranging from 0.805 to 0.905, are greater than those of the off-diagonal elements. Furthermore, discriminant validity among constructs is attained when the correlation between two constructs (the off-diagonal entries) is not greater than their respective composite reliabilities. The figures in Table 2 and Table 3 demonstrate that all individual correlations (from 0.278 to 0.680) are lower than their respective composite reliabilities (from 0.846 to 0.951). These results generally provide strong support for the discriminant validity of the scales.

In addition, the study also uses an additional HTMT index, as suggested by [14], to assess discriminant validity. The results in Table 3 depict that HTMT attained values ranging from 0.339 to 0.794, which is lower than the threshold of 0.90 (for theoretical similar concepts) [14]. This result once again strongly confirms the discriminant validity of the scale.

Table 2. Scale items and latent variable evaluation.

Construct and items		Loading	*t*-test
Punishment severity (PS): AVE = 0.814; CR = 0.929			
PS1	The organization disciplines employees who break information security rules	0.917	71.550
PS2	My organization terminates employees who repeatedly break security rules	0.895	33.059
PS3	If I were caught violating organization information security policies, I would be severely punished	0.894	34.956
Uncertainty Avoidance (AU): AVE = 0.691; CR = 0.870			
UA1	I prefer structured situation than unstructured situation	0.866	28.196
UA2	I prefer concrete guidelines rather than extensive guidelines	0.887	32.512
AU5	I don't like ambiguous situation	0.733	12.501
Response Efficacy (RE): AVE = 0.652; CR = 0.848			
RE1	Complying with information security policies in our organization keep IS security breaches down	0.753	10.992
RE2	If I comply with information security policies, IS security breaches are scarce	0.817	17.909
RE3	Careful compliance with IS security policies helps to avoid IS security problems	0.849	27.877
AISSP compliance attitude (AC): AVE = 0.820; CR = 0.932			
AC1	Adopting security technologies and practices is important	0.908	46.729
AC2	Adopting security technologies and practices is beneficial	0.890	30.896
AC3	Adopting security technologies and practices is helpful	0.918	52.166
Intention to comply with AISSP (IC): AVE = 0.648; CR = 0.846			
IC1	I am likely to follow organizational security policies	0.861	30.070
IC2	It is possible that I will comply with organizational IS security policies to protect the organization's IS	0.730	11.789

(*continued*)

Table 2. (*continued*)

Construct and items		Loading	*t*-test
Punishment severity (PS): AVE = 0.814; CR = 0.929			
IC3	I am certain that I will follow organizational security policies	0.818	20.866
AISSP compliance behaviors (BC): AVE = 0.794; CR = 0.951			
BC1	I comply with ISSP with regard to the access and use of information assets in my organization	0.919	60.368
BC2	I comply with ISSP with regard to e-mail communications	0.822	17.594
BC3	I comply with ISSP with regard to use of the Internet and network resources	0.911	37.613
BC4	I comply with ISSP with regard to anti-virus protection	0.899	49.223
BC5	I comply with ISSP with regard to the prevention of unauthorized access to computer systems	0.901	45.639

Table 3. Discriminant validity and tests of differences between correlations.

	1__	2__	3__	4__	5__	6__
1. AC	**0.905**					
2. BC	0.652	**0.891**				
	0.706					
3. IC	0.608	0.680	**0.805**			
	0.736	*0.794*				
4. PS	0.537	0.546	0.430	**0.902**		
	0.601	*0.596*	*0.513*			
5. RE	0.396	0.370	0.380	0.278	**0.807**	
	0.474	*0.425*	*0.500*	*0.339*		
6. UA	0.523	0.582	0.528	0.299	0.389	**0.832**
	0.612	*0.662*	*0.673*	*0.352*	*0.490*	

Notes: PS: Punishment severity; UA: Uncertainty avoidance; RE: Response efficacy; AC: AISSP compliance attitude; IC: Intention to comply with AISSP; BC: AISSP compliance behaviors. 1st value (off diagonal) = correlation between variables; 2nd value (*italic*) = HTMT ratio; bold diagonal values: square root of AVE

Table 4. PLS-SEM results for the hypothesized relationships.

H	*Independent variables*	Intention to comply with AISSP (IC)		AISSP compliance behaviors (BC)	
		Path Weights (β)	Critical ratio (*t*-value)	Path Weights (β)	Critical ratio (*t*-value)
H_{1a}	PS	0.130	2.476***		
H_{1b}	PS			0.202	1.716*
H_{2a}	UA	0.262	3.904***		
H_{2b}	UA			0.226	3.833***
H_{3a}	RE	0.098	1.761*		
H_{3b}	RE			0.011	0.209
H_{4a}	AC	0.362	5.374***		
H_{4b}	AC			0.207	1.939**
H_5	IC			0.350	4.938***
R^2		0.451		0.629	
Indirect effect RE  IC  BC: β = 0.034, *t* = 1.531*					

Notes: PS: Punishment severity; UA: Uncertainty avoidance; RE: Response efficacy; AC: AISSP compliance attitude; IC: Intention to comply with AISSP; BC: AISSP compliance behaviors; *, **, *** denotes significance at 10%, 5%, and 1% respectively (two-tailed t-test).

4.3 Structural Model

The structural model was assessed by using PLS-SEM technique based on SmartPLS 3.2.7 [29], Bootstrapping with 1000 samples. This technique was employed because PLS-SEM makes no distributional assumptions (Chin, 1998). R2 in Table 4 shows that the model strongly predicts variation in endogenous variables. Specifically, the model explains 45.1% of the variation in intention to comply with AISSP and 62.9% of the variation in AISSP compliance behaviors.

The results as shown in Table 4 indicate the positive and statistically significant relationships between the following variables: punishment severity and intention to comply with AISSP, punishment severity and AISSP compliance behaviors with β = 0.130, *t* = 2.476 and β = 0.202, *t* = 1.716 respectively; uncertainty avoidance and intention to comply with AISSP (β = 0.262, *t* = 3.904), uncertainty avoidance and AISSP compliance behaviors (β = 0.226, *t* = 3.833); response efficacy and intention to comply with AISSP (β = 0.098, *t* = 1.761); ISSP compliance attitude and intention to comply with AISSP, ISSP compliance attitude and AISSP compliance behaviors with β = 0.362, *t* = 5.374 and β = 0.207, *t* = 1.939 respectively; and intention to comply with AISSP and AISSP compliance behaviors (β = 0.350, *t* = 4.938). These results support hypotheses H_{1a}, H_{1b}, H_{2a}, H_{2b}, H_{3a}, H_{4a}, H_{4b}, and H_5, respectively.

Nevertheless, the results reveal no direct relationship between response efficacy and AISSP compliance behaviors (β = 0.011, *t* = 0.209). This means that H_{3b} is not

supported. Thus, we conducted further analyses to verify the magnitude and the statistical significance of the indirect effect between response efficacy and AISSP compliance behaviors based on the procedure suggested by [44]. The results in Table 4 indicate that response efficacy indirectly affects AISSP compliance behaviors through the full mediating role of intention to comply with AISSP ($\beta = 0.034$, $t = 1.531$).

5 Discussion and Conclusion

Security of information systems in general and accounting information systems, in particular, are receiving more and more attention, especially when information technology advances have been widely applied in accounting. The security of an accounting information system is influenced by many factors, in which, the human factor plays an important role. This indicates that accounting information system security is not only a technology issue but also a management issue. Therefore, many businesses in Vietnam have established and maintained accounting information system security policies to regulate the behavior of relevant individuals, thereby aiming to ensure the security of the accounting information system. However, the security of the accounting information system depends on the policy compliance behavior of employees and managers. The policy has no meaning if people don't follow it. Therefore, this study aims to provide empirical evidence on the factors affecting intention and behavior to comply with AISSP.

Our results demonstrate that the intention and behavior of accountants to comply with AISSP are positively influenced by the punishment severity, AISSP compliance attitude, response efficacy, and uncertainty avoidance. Accordingly, these results imply that accountants comply with AISSP when: (1) they are fully aware of the benefits to be derived from compliance; (2) they have a clear understanding of the penalties they face if they do not comply; (3) they have belief in the effectiveness of the measures proposed in the AISSP; and (4) they tend to avoid uncertainty or uncertain situations.

Our study makes the following contributions: from a theoretical aspect, our findings have added to the existing literature body on accounting information system security and AISSP. Particularly, it adds to the limited research on factors affecting AISSP compliance behavior in the context of Vietnam. In addition, our study also creates a premise for future studies to continue exploring accounting information system security, a relatively new topic in Vietnam. In terms of the management aspect, the results help organizations recognize the problems that need to be addressed to ensure AISSP compliance from accountants, thereby improving the effectiveness of AISSP. Specifically, the AISSP should also describe the penalties for non-compliance or policy violations, and this information should be clearly communicated to employees. This measure will motivate accountants to comply with the policy because they are aware of the penalties they will incur if they do not. This measure will be even more effective for accountants who tend to prefer to avoid uncertainty. In addition to issuing policies, organizations also need to clarify the benefits that come from complying with the policy, as well as the effectiveness of the policy. This will contribute to changing the perception of accountants toward AISSP compliance, thereby ensuring that accountants proactively comply with AISSP for the organization's benefit instead of mandatory behavior.

The findings of our study should be interpreted in light of several limitations. First, a single questionnaire was used for measuring all variables of the study, thus, the relationship between variables may be somewhat overestimated. Second, we use subjective and self-reported measures for all variables, so more objective measures are recommended to be adopted in future studies. Third, using convenience sampling to collect data is maybe making sampling bias through under- or over-representing subgroups of enterprises.

References

1. Ajzen, I.: From intentions to actions: A theory of planned behavior. In Action control. Springer, 11–39 (1985).
2. 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).
3. Alias, R. A.: Information security policy compliance: Systematic literature review. Procedia Computer Science, 1216–1224 (2019).
4. Aurigemma, S.: A Composite Framework for Behavioral Compliance with Information Security Policies. Journal of Organizational and End User Computing, 32–51 (2013).
5. Bélanger, F., Collignon, S., Enget, K., & Negangard, E.: Determinants of early conformance with information security policies. Information & Management 54(7), 887-901 (2017).
6. Blumstein, A.: Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. National Academy Press (1978).
7. 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).
8. Chin, W.: The partial least squares approach to structural equation modeling. Modern methods for business research 295(2), 295-336 (1998).
9. Choe, J.: The consideration of cultural differences in the design of information systems. Information & Management 41(5), 669-684 (2004).
10. Connolly, L. Y., Lang, M., & Wall, D. S.: Information security behavior: A cross-cultural comparison of Irish and US employees. Information Systems Management 36(4), 306-322 (2019).
11. Fishbein, M., & Ajzen, I.: Belief, attitude, intention, and behavior: An introduction to theory and research (1977).
12. Fornell, C., & Larcker, D. F.: Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 18(1), 39-50 (1981).
13. Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M.: A primer on partial least squares structural equation modeling PLS-SEM. 2nd edn. Sage publications (2017).
14. Henseler, J., Ringle, C. M., & Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science 43(1), 115-135 (2015).
15. 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 (2009).
16. Hofstede, G.: Values and culture. Culture's consequences: International differences in work-related values (1980).
17. Hofstede, G., Hofstede, G., & Minkov, M.: Cultures and Organizations: The Software of the Mind. McGraw-Hill, New York, London (1991).

18. Hofstede, G., Hofstede, G. J., & Minkov, M.: Cultures and Organizations: Software of the Mind. 3rd edn. McGraw-Hill, New York, London (2010).
19. Hovav, A., & D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. Information & Management 49(2), 99-110 (2012).
20. 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).
21. 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).
22. Johnston, A. C., & Warkentin, M.: Fear appeals and information security behaviors: an empirical study. MIS quarterly 549–566 (2010).
23. Kellaris, J. J., & Jung, J. M.: Cross-national differences in proneness to scarcity effects: The moderating roles of familiarity, uncertainty avoidance, and need for cognitive closure. Psychology & Marketing 21(9), 739-753 (2004).
24. Ladbury, J. L., & Hinsz, V. B.: Uncertainty avoidance influences choices for potential gains but not losses. Current psychology 28(3), 187-193 (2009).
25. 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).
26. Pahnila, S., Siponen, M., & Mahmood, A.: Employees' behavior towards IS security policy compliance. In: 40th Annual Hawaii International Conference on System Sciences. HICSS 2007, Hawaii (2007).
27. Peace, A. G., Galletta, D. F., & Thong, J. Y.: Software piracy in the workplace: A model and empirical test. Journal of Management Information Systems 20(1), 153-177 (2003).
28. 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), 879-903 (2003).
29. Ringle, C. M., Wende, S., & Becker, J.-M.: SmartPLS 3. Boenningstedt: SmartPLS GmbH. Homepage, http://www.smartpls.com, last accessed 2015.
30. 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).
31. Rogers, R. W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology 91(1), 93-114 (1975).
32. 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).
33. Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M.: Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems 97, 587-597 (2019).
34. 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).
35. Safa, N. S., Von Solms, R., & Furnell, S.: Information security policy compliance model in organizations. Computers & Security 56, 70-82 (2016).
36. Siponen, M., Pahnila, S., & Mahmood, A.: Factors influencing protection motivation and IS security policy compliance. Innovations in Information Technology (2006).
37. Siponen, M., Pahnila, S., & Mahmood, M. A.: Compliance with information security policies: An empirical investigation. Computer 43(2), 64-71 (2010).

38. 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).
39. Trang, S., & Brendel, B.: A meta-analysis of deterrence theory in information security policy compliance research. Information Systems Frontiers 21(6), 1265-1284 (2019).
40. 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).
41. 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).
42. Woon, I., Tan, G.-W., & Low, R.: A protection motivation theory approach to home wireless security. In: ICIS 2005 proceedings, p. 31 (2005).
43. 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).
44. Zhao, X., Lynch Jr, J. G., & Chen, Q.: Reconsidering Baron and Kenny: Myths and truths about mediation analysis. Journal of consumer research 37(2), 197-206 (2010).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.