Research on Influencing Factors of Extra-Role Information Security Policy Compliance Behaviour Based on Structural Equation Model

Cong Wang[1](✉), Chongrui Liu[2], Jidong Yao[3], and Longfei Li[3]

[1] School of Economics and Management, Institute of Disaster Prevention, Xueyuan Avenue, Sanhe, China
wangcong@cidp.edu.cn

[2] Department of Management, Beijing Electronic Science and Technology Institute, Fufeng Road, Beijing, China
lcr0122@sina.com

[3] Department of Economics and Management, Beijing City University, Muyan Road, Beijing, China

Abstract. Information security noncompliance behaviour of employees within an organization is one of the primary reasons for the high frequency of information security incidents. The issue of information security compliance behaviour has attracted attention and importance. The information came from a poll of 525 Chinese civil officials. This study identified variables through empirical analysis that can forecast extra-role information security policies (ISP) compliance behaviours. Structural equation model (SEM) was established and the data was analysed by SmartPLS (Partial Least Square). The findings demonstrated a substantial relationship between peers' behaviour and extra-role ISP compliance by employees and the company information security atmosphere. Additionally, it was discovered that both the relationship between peer behaviour and extra-role behaviour and the relationship between the information security climate and extra-role behaviour were being mediated by employees' ISP compliance intention and response efficacy. Practical implications are discussed in conclusion.

Keywords: information security police compliance intention · information security climate · extra-role behaviour · structural equation model · Partial least squares

1 Introduction

In recent years, the frequent occurrence of information security incidents has made enterprises gradually realize the necessity of information security management. However, over-reliance on security technology has overlooked the potential risks to information security caused by the misuse and abuse of information assets by employees. Internal threats from organization employees have become the primary cause of information security incidents [13]. The notion around management control states that organizations

Z. Zhan et al. (Eds.): EIMSS 2022, AHCS 7, pp. 547–556, 2023.
https://doi.org/10.2991/978-94-6463-024-4_57

frequently utilize control mechanisms to persuade employees to abide by information security regulations or to halt employees' inappropriate behaviour. Previous research has shown that information security climate or culture, among the process controls in formal organizational control, has a facilitating effect on information security policy compliance behaviour [7]. D'Arcy and Green [4] emphasized that the safety monitoring behaviour of an organization creates a safety culture and employees are influenced by this safety culture to enhance their intention to comply with safety policies [4]. Organizational information security climate is the value system and ethics corresponding to the organization's information system strategy, and it is an organizational culture that protects the security of information assets. It is an organizational culture that protects the security of information assets and is a reflection of the organization's core values. It guides employees to consciously protect all kinds of information resources of the organization [9]. Meanwhile, social controls in organizational informal controls, such as social norms and peers' behaviours significantly influence employees' breach intentions [2]; peer behaviours are negatively related to employees' breach intentions [14].

However, can individuals go further that the information security climate promotes individuals' information security extra-role behaviours besides their own compliance with information security policies? Extra-role behaviour refers to the behaviour that is not explicitly stated in an ISP and does not rely on the use of rewards or penalties to encourage performance [6]. However, there is no clear conclusion on how significant information security climate relation to ISP compliance and information security extra-role behaviours. Also, the impact of formal controls on employees' information security behaviours differs in different cultural contexts in the Eastern and Western cultures. Under different types of information security policies, previous studies found differences in the effectiveness of formal and informal controls.

To examine the organizational and personal antecedents within the setting of Oriental culture, this study uses Chinese civil officials as an example. We consider peer behaviour and the information security climate to be influential variables. At the same time, using social control theory (SCT) for reference, we take compliance intention and ISS response efficacy as mediating variables. This study will make contributions to the research on information security in the following aspects: (1) it enriches the research on ISP compliance in the context of Oriental culture. (2) The impact mechanism of environmental factors such as information security climate and peer behaviour on information security policy compliance is clarified. (3) By including extra-role behaviours as dependent variables, we also contributed to SCT by expanding its scope.

2 Literature Review

2.1 Information Security Climate and Extra-Role Information Security Behaviours

Information security climate refers to the common and accepted practices in the workplace that define how organizations approach information security [10]. Perceptions of the information security climate include employees' perceptions of the information security behaviours of their colleagues and supervisors [1, 3, 5, 8]. Employee behaviour is influenced by specific rules and social interactions as well as the information security climate at work [6]. Most empirical studies have shown that information security climate is significantly associated with employee compliance with ISP [5]. For example, to some extent, organizational security climate and social influences (e.g., subjective norms and attachment) can influence compliance behaviour [2]. Jaafar and Ajis [8] found that ISP compliance behaviour can be significantly influenced by the IS climate. Although extra-role behaviours receive little attention, the designated security activities in ISPs are typically regarded as in-role behaviours. It is important to examine the connection between the information security environment and extra-role information security behaviour from an Eastern cultural perspective.

2.2 Peer Behaviour and Extra-Role Information Security Behaviours

Cheng et al. [2] explored the effects of social bonding and social pressure using employees in Chinese companies. The study showed that peer behaviour had a significant impact on employees' intention to breach. Subsequently, Song [14] validated the same model proposed by Cheng et al. [2] with employees in U.S. firms, and found that peer behaviour was negatively related to employees' breach intentions. The higher the expectations that people feel from their colleagues or leaders about their information security obedience behaviour or the higher the social pressure, the more inclined to obey the information security policy of the company. Hsu et al. [6] argued that employees who are bonded with their colleagues are more likely to show extra-role behaviours when there is a strong information security climate. Employees are more likely to exhibit extra-role behaviours when they are strongly motivated to help others, and to exhibit more helping behaviours when they know exactly how to help others. In this research, we expected the positive relationship between peer behaviour and extra-role information security behaviours.

2.3 Mediating Effect of ISP Compliance Intention

According to earlier studies, the propensity of employees to adhere to information security policies is positively connected with the information security atmosphere [5]. That is, when an organization implements information security practices while allowing employees to perceive a strong information security climate in the organization, employees are more likely to bring intentions that are consistent with information security. Daily interactions of workers in the workplace can have an impact on individual work behaviours. Previous research has concluded that coworker socialization has a positive impact on information security compliance intentions and behaviours [8]. Besides, attitudes and psychology largely influence behaviour; therefore, on the one hand, employees' information security compliance intentions may lead to information security compliance behaviours, while on the other hand, their information security non-compliance intentions may lead to information security non-compliance. Therefore, we conclude that ISP compliance intentions mediates between the information security climate, peer behaviour, and extra-role behaviour.

2.4 Mediating Effect of Response Efficacy

Response efficacy is related to beliefs about the perceived benefits of actions taken by individuals [12]. Ifinedo (2012) stated that it adheres to ISP as an effective mechanism for detecting threats to an organization's information security assets. Climate and peer behaviour provides clues and cues to one's own behaviour, which further impacts experience with information security practice. Then climate and peer behaviour of information security could impact response efficacy. Ifinedo (2012) argued that ISP compliance behavioural intentions may be positively influenced by response efficacy. Therefore, it can be speculated that the response efficacy further positively affects the information security behaviour as well. Indeed, Ng et al. [11] examined a large body of literature in the field of information security and found that there is a consensus that the response efficacy can effectively motivate users to adopt information security behaviours. In this paper, we hypothesize that response efficacy mediates the relationship between the climate, peer behaviour and extra-role behaviours.

3 Method

We give the research model, research hypotheses, and survey sample in this section, all of which are based on the literature review, in order to test the effectiveness of the survey instrument.

3.1 Research Model and Hypotheses

This study was intended to investigate the relationship of information security climate, peer behaviour and extra-role behaviours in Eastern countries, as well as the mediating role of ISP compliance intention and response efficacy in the relationship. The hypotheses are proposed as following:

H1: Information security climate is positively related to extra-role behaviours.
H2: Peer behaviours is positively associated with extra-role behaviours.
H3: ISP compliance intention is mediating the relationship between information security climate, peer behaviour and extra-role behaviour.
H4: Response efficacy is mediating the relationship between information security climate, peer behaviour and extra-role behaviour.

The conceptual model and econometric model is shown as Fig. 1.

$$Y = (b_0 + a_0 b_1) + \left(a_1 b_1 + c'\right)X \tag{1}$$

where y represents the dependent variable, x represents the measured value of the independent variables.

3.2 Data Collection

To ensure the representativeness of the sample, civil servants were selected from Beijing, Fujian, Hebei, and Shandong using a stratified sampling method. In order to improve efficiency, we chose the form of Internet questionnaire for data collection, and we created different links to the questionnaire according to different survey areas. The survey was

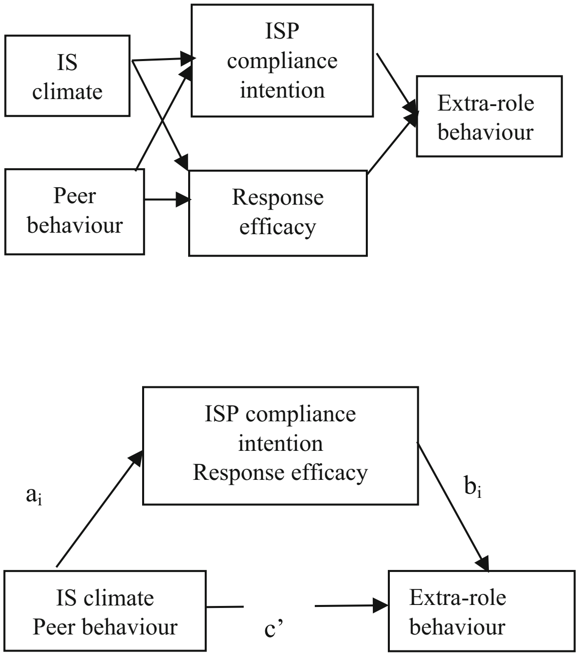

Fig. 1. Conceptual model

conducted among civil servants of 42 departments and councils of central government in mainland China. They received links to the questionnaire, which first described the purpose of the project and invited them to participate. We also emphasized and guaranteed the confidentiality and anonymity of the answers. To a certain extent, the authenticity of the questionnaire information was ensured. After discarding a few questionnaires with incomplete or unreliable answers, finally valid sample includes 525 civil servants. The final sample was 50.5% women, and more than 30% was distributed between the ages of 31 to 40. Table 1 displays the characteristics of the respondents.

3.3 Measure

All measurement scales are in the form of 5-point Likert-type scale (1 = strongly disagree; 5 = strongly agree). We measured participants' peer behaviour and response-efficacy using the scales adapted by Li et al. (2019). We measure information security climate and extra-role behaviours that were respectively adopted from Kessler et al. (2020) and Hsu et al. [6] ISP compliance intention was measured with the 4 items in the scale developed by Ifinedo [7].

Table 1. Samples

Item	Variable	Frequency	Percentage (%)
Gender	*Male*	260	49.5
	Female	265	50.5
Age	*Younger than 30*	146	27.8
	31–40	176	33.5
	41–50	126	24.0
	51 and above	77	14.7
Education background	*High school*	130	24.8
	Associate	112	21.3
	Bachelor	210	40.0
	Post graduate	73	13.9
Tenure	*Less than 1 year*	92	17.5
	2–5 year	151	28.8
	6–10 year	107	20.4
	11–15 year	75	14.3
	16 year and above	100	19.0
Type of employment	*Irregular*	219	41.7
	Regular	306	58.3
Marriage	*Yes*	359	68.4
	No	166	31.6
Position	*Staff*	319	60.8
	Assistant manager	112	21.3
	Manager	38	7.2
	Deputy director	56	10.7
Income satisfaction	*Very dissatisfied*	74	14.1
	dissatisfied	92	17.5
	Normal	216	41.1
	Satisfied	101	19.2
	Very satisfied	42	8.0
Size of institution	*Under 100*	190	36.2
	101–500	202	38.5
	501–1000	65	12.4
	Above 1000	68	13.0

Table 2 .

	Mean	S.D	AVE	CR
1. Information security Climate	3.02	1.26	0.868	0.975
2. Peer behaviour	2.92	1.22	0.932	0.916
3. ISP compliance intention	3.35	1.48	0.941	0.988
4. Response efficacy	3.24	1.39	0.956	0.985
5. Extra-role behaviour	3.21	1.37	0.923	0.986

4 Results

4.1 Reliability and Validity Analysis

Before correlation analysis and path analysis, we first conducted reliability and validity analyses to test and ensure questionnaire and data quality. Partial least squares (PLS) method is used for data analysis, and the software is SmartPLS 2.0.

Table 2 displays coefficient alphas for these scales that are > 0.9 and higher than the 0.7 cutoff. Additionally, the average variance extracted (AVE) of the constructs was > 0.8, exceeding the 0.5 cutoff. Additionally, all standardized item loadings were at least 0.7 and significant ($p < 0.001$). It can be seen that the quality of the questionnaire and data is satisfactory and the next step of data analysis and hypothesis testing can be performed.

4.2 Data Analysis

The correlations between the variables are shown in Table 3. Significant correlations can be found between all 5 variables ($p < 0.01$), laying a foundation for further path analysis. Results of the structural equation model assessment are shown in Table 4. The model explained 68.5% of the variance in employees' ISP compliance. All paths were significant in the predicted directions. Information security climate and peer behaviours both have significant effect on extra-role behaviours (H1 and H2 are supported, respectively). Also, the two independent variables have effect on ISP compliance intention and response efficacy, then both ISP compliance intention and response efficacy have effect on extra-role behaviours. Thus, in the relationship between independent and dependent variables, ISP compliance intention and response efficacy act as mediators (H3 and H4 are both supported).

Table 3. Correlations (*p < 0.01)

	1	2	3	4
1. Information security climate	1			
2. Peer behaviour	0.20**	1		
3. ISP compliance intention	0.60**	0.36**	1	
4. Response efficacy	0.30**	0.46**	0.15**	1
5. Extra-role behaviour	0.52**	0.57**	0.35**	0.39**

Table 4. Path loadings and t values

Variables	Path coefficient	t-value	P-value
Information security climate—ISP compliance intention	0.371	3.824	p < 0.01
Information security climate—Response efficacy	0.464	4.607	p < 0.01
Peer behaviour—ISP compliance intention	0.174	2.706	p < 0.05
Peer behaviour—Response efficacy	0.262	2.585	p < 0.05
ISP compliance intention—Extra-role behaviour	0.305	4.076	p < 0.01
Response efficacy—Extra-role behaviour	0.297	4.102	p < 0.01

5 Discussion and Conclusion

Previous studies on ISP compliance were mainly conducted in the context of western culture, and different or even opposite conclusions were drawn. This study contributes to the pertinent research on ISP compliance in the context of Oriental culture, using Chinese public officials as an example. According to this study, peer behaviour and the information security climate can both predict extra-role conduct related to ISP compliance in the context of Oriental culture. And the two organizational factors can influence ISP compliance behaviour through personal factors that is ISP compliance intention and response efficacy.

The findings have practical implications for the design and implementation of effective ISPs. First, we identified the information security climate and peer behaviour as significant predictors of extra-role behaviour of ISP compliance. This suggests that, in addition to formal controls, such as information security policies, organizations can simultaneously create a strong organizational security climate through a number of measures, and engage in team building (i.e. impacting peer behaviour and coworker's bonding) to enhance employee compliance with ISPs. Second, we further identified that ISP compliance intention and response efficacy motivates employees to engage and exhibit information security behaviours. IS climate and peer behaviour can promote extra-role behaviour through willingness to comply and response efficacy. Information security behaviours can be stimulated by these factors a step further, i.e., they are not limited to in-role behaviours, but can further generate extra-role behaviours.

Although this paper has made some research progress, it still has some research limitations. First, the data in this study were primarily employee self-reported data, and although the results of the related test indicated that common method bias was not a problem here and did not affect the findings of this study, future studies should consider using data from multiple sources or integrating more precise data collection methods such as longitudinal studies, experimental studies, and case studies to collect data or evaluate employees' ISP compliant behaviour and perform statistical processing. Second, this study only used ISP compliance intentions and response efficacy as mediators. Further studies can consider other variables such as self-efficacy, response cost in influencing ISP behaviour to play a mediating role.

Acknowledgements. The support of MPA students who assisted in data collection as well as anonymous responses is gratefully acknowledged by the authors. This work was supported by grants from the Fundamental Research Funds for the Central Universities (Grant No. ZY20210316).

References

1. Chan M, Woon I, Kankanhalli A (2005) Perceptions of information security at the workplace: linking information security climate to compliant behaviour. Percept Inf Privacy Secur 1:18–41
2. Cheng L, Li Y, Li W (2013) Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Comput Secur 39:447–459
3. Dang-Pham D, Kautz K, Pittayachawan S, Bruno V (2019) Explaining the development of information security climate and an information security support network: a longitudinal social network analysis. Australas J Inf Syst 23:1–28
4. D'Arcy J, Greene G (2014) Security culture and the employment relationship as drivers of employees security compliance. Inf Manag Comput Secur 22(5):474–489
5. Goo J, Yim MS, Kim DJ (2014) A path to successful management of employee security compliance: an empirical study of information security climate. IEEE Trans Prof Commun 57(4):286–308
6. Hsu SC, Shih SP, Yu WH, Lowry PB (2015) The role of extra-role behaviours and social controls in information security policy effectiveness. Inf Syst Res 26(2):282–300
7. Ifinedo P (2018) Roles of organizational climate, social bonds, and perceptions of security threats on is security policy compliance intentions. Inf Resour Manag J 31(1):53–82
8. Jaafar NI, Ajis A (2013) Organizational climate and individual factors effects on information security compliance behaviour. Int J Bus Soc Sci 4(10):118–130
9. Li J, Wang W, Xie Y (2015) Research on the role and construction of organization's information security culture. J Intelligence 3:162–166
10. Lowry PB, Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Inf Syst J 25:465–488
11. Ng B-Y, Kankanhalli A, Xu Y (2009) Studying users' computer security behaviour: a health belief perspective. Decis Support Syst 46(4):815–825

12. Rogers R (1983) Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In: Cacioppo J, Petty R (eds) Social psychophysiology: a sourcebook. Guilford Press, New York, pp 153–176
13. Schultz E (2005) The human factor in security. Comput Secur 24(6):425–426
14. Song A (2018) Evaluation of the intents of noncompliance with the organizational information systems security policy. University of Phoenix, Phoenix