Influencing factors of employees' information systems security police compliance: An empirical research in China

Liu Chongrui[1], Wang Cong[2*], Wang Hongjie [1], Niu Bo[3]

[1]Department of Management, Beijing Electronic Science and Technology Institute Beijing, China
[2]School of Economics and Management, Institute of Disaster Prevention Sanhe, China
[3]Department of Economics and Management, Beijing City University, Beijing, China

Abstract. It is widely agreed that information systems security police compliance plays a pivotal role in safeguarding organizational information security. This study empirically investigated organizational and individual factors in predicting employees' ISSP compliance. With a survey data of 525 civil servants in China, results showed that organizational information security training and information security climate were significantly related to employees' ISSP compliance. Specifically, information security climate had stronger effect on ISSP compliance than information security training. Furthermore, it was found that employees' perceived severity, perceived vulnerability and response efficacy were positively related to employees' ISSP compliance. We discussed the key implications of our findings for managers and researchers.

1 Introduction

The widespread application of computers and internets has benefited to organizational efficiency and high performance. Despite the benefits, organizational information systems are more likely to be threatened by cyberattacks and deserved to develop security initiatives. However, monitoring systems, such as data leak prevention, content monitoring technologies which offer technical solutions to the information security problems are not sufficient in providing total protection. With the human factor becoming the weakest link, information security researchers began to highlight employees' compliance to information system security policy and identified a mass of antecedents predicting information systems security police (ISSP) compliance[1][2][3].

However, as Dhillon and Backhouse (2001) pointed out, empirical research drawing on the socio-organizational view to developing key motivators for improving employee security compliance was still lacking[4]. Additionally, the present research draws inconsistent conclusion on the relationship between ISSP compliance and its antecedents. For example, in terms of organizational related antecedents, Greene and D'Arcy (2010) found that information security climate was positively related to employees' security compliance[5], while Ifinedo (2018) found that information security climate failed to significantly predict employees'ISSP compliance[6]. In terms of individual related antecedents, Siponen et al. (2014) found that employees' perceived severity of threat was significantly accorelated with ISSP compliance[7]. While Ifinedo (2012) didn't support that perceived severity was a robust predictor of ISSP compliance in his research[8].

This study took Chinese civil servants as example and investigated the organizational and individual antecedents in Eastern culture context. We captured information security climate and information security training as organizational informal factor and formal factor respectively. Meanwhile, drawing on protection motivation theory (PMT), we captured perceived severity, perceived vulnerability and response efficacy as individual threat appraisal and coping appraisal. This study would contribute information security research in following respects: (1) enriched ISSP compliance related research in East culture context. (2) clarified the inconsistent conclusion on the relationship between ISSP compliance and its antecedents under a different culture context.

2 Literature review

2.1 ISSP compliance behavior

Information system security policies (ISSP) are defined as a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations[9]. A rich stream of research has identified numerous antecedents of employees' ISSP compliance. For example, Moody et al. (2018) proposes a unified model of information security policy compliance to examine the different antecedents[1]. Cram, D'Arcy, & Proudfoot (2019) conducted a meta-analysis to classified 401 independent variables as the antecedents of ISSP compliance behavior[3].

[*] Corresponding author: batbibby@hotmail.com

2.2 Information security climate and ISSP compliance

Information security climate reflects a collection of norms, beliefs, values, and fundamental assumptions shared by organizational members on how information security matters. Most empirical research showed that information security climate was significantly related to employees' compliance with ISSP[10]. For example, Jaafar and Ajis（2013）found IS climate was a robust determinant of ISSP compliance behavior[11]. However, a handful of scholars draw diverse conclusion organizational security climate did not have a significant impact on ISSP compliance. For example, Ifinedo (2018) found that organizational security climate did not predict significantly compliance behavior[6]. The inconsistent conclusion conducted in Western context is deserved to be verified again in a Eastern culture context.

2.3 Information security training and ISSP compliance

Information security training is an educational process by which employees fulfill the necessary conditions for information security at the organization[12]. As such, information security training may provide general knowledge and necessary skills for information security[13]. A mature IS training could provide employee with security experience, beliefs and perception of severity of information security, then improve employees' compliance with organizational rule and policy[14][15]

2.4 Perceived severity and ISSP compliance

There are inconsistent conclusions on the relationship between perceived severity and ISSP compliance. Most researchers found that employees with higher perceptions of IS security threats were more inclined to comply with ISSP[6][7][8]. For example, Siponen et al. (2014) found that perceived severity of IS security threats had significant and positive effects on employees' ISSP compliance[7]. Cram et al. (2019) in their meta-analysis also showed that threat severity category is positive related to ISP compliance (β=0.342)[3]. However, Ifinedo (2012) did not support that perceived severity was a significant predictors of information system security behavioral compliance[8].

2.5 Perceived vulnerability and ISSP compliance

Most research showed that perceived vulnerability had significant impact on employees' compliance behavior[8][16][17]. For example, Siponen et al. (2014) found that perceived vulnerability of information system security threat had significantly positive effect on employees' ISSP compliance[7]. However, a few publications found a negative corelation between perceived vulnerability and security policy compliance[18].

2.6 Response efficacy and ISSP compliance

When an individual possesses requisite knowledge and skill to provide protection from a threat or danger, the individual is more likely to adopt an adaptive behavior[17]. Accordingly, it can be infered that individuals who can avert threats and dangers in themselves will be more inclined to develop an intention to adopt it[19]. Han et al.[12] and Siponen et al.[20] proposed that response efficacy is also a common determinant of ISSP compliance. However, some scholars in their empirical research found that response efficacy did not significantly predict users' attitudes towards compliance[7].

3 Method

3.1 Research goal

This study was intended to investigate the influence of organizational and individualfactors on ISSP compliance in Eastern countries. The hypotheses are proposed as following:

H1: Information security climate is positively associated with ISSP compliance.

H2: Information security training is positively associated with ISSP compliance.

H3: Perceived severity is positively associated with ISSP compliance.

H4: Perceived vulnerability is positively associated with ISSP compliance.

H5: Response efficacy is positively associated with ISSP compliance.

3.2 Data collection

In order to ensure the representativeness of the samples, we adopted stratified sampling method to select civil servants from Beijing, Fujian Province, Hebei Province, Shandong Province province et al. On one hand, we chose a professional platform named "Wenjuanxing" for data collection and made different questionnaire links based on different survey areas. Methods Convenience sampling and snowball sampling were used to select respondents. In the process of collecting the questionnaire, the research team emphasized the academic research purpose and anonymity of this survey. The questionnaires were sent to 42 departments and councils of central government in China. The number of questionnaires sent to each institution was from15 to 20 in consideration of each institution size. The questionnaires were collected from Sep. 2019 to May. 2020. After discarding a few questionnaires with incomplete or unreliable answers, 525 valid questionnaires were obtained. Table 1 displays the characteristics of the respondents.

Table1. Profiles of respondents

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

3.3 Measure

All Items were assessed along a 5-point Likert-type scale with 1 indicating “strongly disagree” and 5 indicating “strongly agree.”

The measure of perceived severity, perceived vulnerability and response efficacy were adapted from Li et al.[15]and Ifenido[8].The measure of information security climate and information security training werewas respectively adopted from Kessler et al.[21] and D’Arcy et al.[13]. ISSP compliance is adopted from Arcy & Teh (2019)’ measure with a four-item scale[22].

3.4 Data analysis and results

We selected Partial Least Squares (PLS) using Smart PLS 2.0 for data analysis.

The reliability of the measurements was assessed by the composite reliability (CR) index. As shown in Table 2, the composite reliabilities for all constructs are greater than the 0.7 threshold. Furthermore, the Average variance extracted (AVE) are larger than the threshold of 0.5. In addition, all standardized item loadings were significant ($p < 0.001$) and at least 0.707.

Table 2 (a) Descriptive and Composite reliability

	Mean	S.D	AVE	CR
1.Information security.climate	3.02	1.26	0.868	0.975

2.Information security.training	3.18	1.36	0.932	0.986
3.Perceived severity	3.30	1.43	0.941	0.979
4.Perceived vulnerability	3.23	1.40	0.936	0.983
5.Response efficacy	3.24	1.39	0.956	0.985
6.ISSP compliance	3.29	1.43	0.950	0.987

Table 2 (b) Analysis of Correlation

	1	2	3	4	5
1.Information security.climate	1				
2.Information security.training	0.05	1			
3.Perceived severity	0.40	0.21	1		
4.Perceived vulnerability	0.34	0.36	0.14	1	
5.Response efficacy	0.19	0.26	0.27	0.21	1
6.ISSP compliance	0.35	0.20	0.21	0.24	0.26

3.5 Data analysis and results

Results of the structural model assessment are presented in Table 4. The model explained 73.2% of the variance of employees' ISSP compliance. All the hypotheses were supported as following: information security climate, information security training, perceived severity, perceived vulnerability, response efficiency had significant effect on ISSP compliance. Specially, in terms of organizational factor, information security climate has a stronger effect on ISSP compliance than information security training. In terms of individual factor, response efficacy has a stronger effect on ISSP compliance than perceived severity and perceived vulnerability.

Table 3 Path loadings and t values

Hypotheses	**Path coefficient**	**t-value**	**P-value**
H1:Information security climate—— ISSP compliance	0.196	3.942	$p<0.01$
H2: Information security training—— ISSP compliance	0.154	2.087	$p<0.05$
H3: Perceived severity—— ISSP compliance	0.133	2.076	$p<0.05$
H4: Perceived vulnerability—— ISSP compliance	0.215	3.585	$p<0.001$
H5:Response efficacy—— ISSP compliance	0.292	4.170	$p<0.001$

4 Discussion

This study confirmed that both organizational factor (i.e. information security training and information security climate) and individual factor (i.e. perceived severity, perceived vulnerability and response efficacy) could make a statistically significant contribution to the prediction of ISSP compliance/ in Eastern culture. Our study conducted under different culture provided evidence in support of prior research conclusions (e.g. Greene & D'Arcy, 2010).

This study took Chinese civil servants as examples and enriched ISSP compliance related research in Eastern culture context. Previous ISSP compliance research mainly was conducted in Western culture context and reached different even opposite conclusion. This study deepened the understanding on the predictors of ISSP compliance in different culture.

Given the research conclusion, it has practical implications for designing effective ISP. First, we confirmed that information security climate and information security training is important predictors of ISSP compliance. This suggested that in addition to information security policies, organization can simultaneously create informal practice (i.e. organizational security climate) and formal practice (i.e. systematic IS security training) to enhance employees ISSP compliance. Second, following the prior study[16], we confirmed that perceived severity, perceived vulnerability and response efficacy are important strategies for motivating employees to engage in responsible security behaviors. It is vital for managers to recognize that any organization may rest on the extent to which its employees' perceived severity and vulnerability of risk.

There are also some limitations. First, all measures were self-reported. Although common method bias was not a problem for this study, it is still possible that participants might have provided "socially desirable responses". Further research should take cross-sectional survey or design longitudinal study to assess employees' compliant behavior over time at their workplace. Second, this study only focused on response efficacy as the coping appraisal. Further research could capture other variables such as self-efficacy, response cost as the coping appraisal.

Acknowledgment

This work is supported by the Fundamental Research Funds for the Central Universities"Research on information security literacy of civil servants in China" under Grant Number No. 328202009.

Supported by the Fundamental Research Funds for the Central Universities "Research on information security literacy of civil servants in China（No. 328202009）"

References

1. Moody, G.D., Siponen, M., and Pahnila, S. (2018) "Toward a unified model of information security policy compliance," Mis Quarterly, 42(1), 285-311.
2. Chua, H.N., Wong, S.F., Low, Y.C., &Chang, Y. (2018) Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics, 35(6),1770-1780.
3. Cram, W.A. , D'Arcy, J., & Proudfoot, J.G. (2019) Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-554.
4. Dhillon, G., & Backhouse, J. (2001) Current directions in is security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.
5. Greene, G., and D'Arcy, J. (2010) "Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance," in Proceedings of the 5th Annual Symposium on Information Assurance, Albany, NY.
6. Ifinedo, P. (2018) "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions," Information Resources Management Journal (31:1), pp. 53-82.
7. Siponen, M., Mahmood, M. A., and Pahnila, S. (2014) "Employees' Adherence to Information Security Policies: An Exploratory Field Study," Information & Management (51:2), pp. 217-224.
8. Ifinedo, P. (2012) "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," Computers & Security (31:1), pp. 83-95.
9. Lowry, P.B., and Moody, G.D. (2015) "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies," Information Systems Journal (25:5), pp. 465-488.
10. Goo, J., Yim, M.S., and Kim, D.J. (2014) "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate," IEEE Transactions on Professional Communication (57:4), pp. 286-308.
11. Jaafar, N.I., and Ajis, A. (2013) "Organizational Climate and Individual Factors Effects on Information Security Compliance Behaviour," International Journal of Business and Social Science (4:10), pp. 118-130.
12. Han, J., Kim, Y.J., and Kim, H. (2017) "An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective," Computers & Security (66), pp. 52-65.
13. D'Arcy, J., Hovav, A., and Galletta, D. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research (20:1), pp. 79-98.
14. Puhakainen, P., & Siponen, M. (2010) Improving employees' compliance through information systems security training: An action research study. MIS Quarterly: Management Information Systems, 34(4), 757–778.
15. Li, L., He, W., Xu, L., Ash, I., Anwar, M., &Yuan, X. (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management,45,13-24.
16. Ifinedo P. (2011) An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. Journal of Information Security and Privacy ;7(1):25-49.
17. Lee Y, Larsen KR. (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems;18(2): 177-87.
18. Johnston, A.C., Warkentin, M., and Siponen, M. (2015) "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," MIS Quarterly (39:1), pp. 113-134.
19. Herath T, Rao HR. (2009) Protection motivation and deterrence: a framework for security policy

compliance in organizations. European Journal of Information Systems, 18(2):106-25.

20. Siponen, M.T., Pahnila, S., and Mahmood, A. (2007) “Employees’ Adherence to Information Security Policies: An Empirical Study,” in New Approaches for Security, Privacy and Trust in Complex Environments (Proceedings of the 22nd IFIP TC 11 International Information Security Conference), H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms (eds.), Boston: Springer, pp. 133-144.
21. Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. (2020) Information security climate and the assessment of information security risk among healthcare employees. Health Informatics Journal, 26 (1):461-473.
22. D'Arcy, J., Teh, P. (2019) Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. Information and Management,56(7),1-14.