Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

WILLINGNESS AND ABILITY TO PERFORM INFORMATION SECURITY COMPLIANCE BEHAVIOR: PSYCHOLOGICAL OWNERSHIP AND SELF-EFFICACY PERSPECTIVE

Hung-Wei Huang
1111 Job Bank, fighter_of_space@yahoo.com.tw

Neeraj Parolia
Towson University, nparolia@towson.edu

Keng-Ting Cheng
National United University, ktcheng@nuu.edu.tw

Recommended Citation

Huang, Hung-Wei; Parolia, Neeraj; and Cheng, Keng-Ting, "WILLINGNESS AND ABILITY TO PERFORM INFORMATION SECURITY COMPLIANCE BEHAVIOR: PSYCHOLOGICAL OWNERSHIP AND SELF-EFFICACY PERSPECTIVE" (2016). *PACIS 2016 Proceedings*. 57.
http://aisel.aisnet.org/pacis2016/57

WILLINGNESS AND ABILITY TO PERFORM INFORMATION SECURITY COMPLIANCE BEHAVIOR: PSYCHOLOGICAL OWNERSHIP AND SELF-EFFICACY PERSPECTIVE

Hung-Wei Huang, 1111 Job Bank, Taiwan, fighter_of_space@yahoo.com.tw

Neeraj Parolia, e-Business and Technology Management Department, Towson University, USA, nparolia@towson.edu

Keng-Ting Cheng, Department of Information Management, National United University, Taiwan, KTCheng@nuu.edu.tw

Abstract

Information security policy effectiveness relies on how well an individual employee can follow the specified instruction described in security policies. The actual taking place of such compliance behavior is determined by individuals' willingness and capability of performing such behavior. In this study, we used psychological ownership to represent the driver of willingness and self-efficacy to represent individuals' capability belief. In addition to understanding the impacts of these two variables on compliance behavior, we also explore their antecedents. Data collected from 234 employees in organizations with specific security policies were used to examine the proposed hypotheses. We confirmed the positive impact of self-efficacy but, surprisingly, found the negative impact of psychological ownership. Such a result generates some interesting implications for researchers and practitioners.

Keywords: Information security policy compliance, Psychological ownership, Self-efficacy.

1 INTRODUCTION

In addition to strengthening infrastructure, organizations should also construct effective policies to advance secure information within an organization. The effectiveness of information security policies relies on how well individual employees comply with requirements and perform desired behaviors (e.g. Boss et al. 2009; Chan et al. 2005; D'Arcy et al. 2009; Ifinedo 2012; Lee et al. 2004; Vance et al. 2012). Researchers have adopted different theories to explore potential antecedents of compliance behavior, such ad deterrence theory, protection motivation theory, and control theory(D'Arcy et al. 2009). Deterrence theory points out that knowing the severity and certainty of punishment drive individuals to perform desired behavior. Protection motivation theory argues that sensing the threat and knowing individuals own capability in reacting to such threat determining individuals' intention to perform protection behavior (Herath & Rao 2009a). In addition, control theory further suggests that compliance behaviors can be promoted by both formally through security policy and informally through personal attachment to the environment (Hsu et al. 2015).

Researchers and practitioners have spent a significant amount of effort in understanding how to strengthen individual employees' motivation to comply with security policies. Organization theory has pointed out that individual tend to take certain behaviors to protect the organization when they sense an ownership toward the organization. Psychological ownership, a concept that individual sense ownership toward a particular target, is also associated with behavior or job performance (Van Dyne & Pierce 2004). Individuals tend to develop commitment toward organization when they sense ownership toward the organization. As an outcome, desired behaviors are more likely to be observed when individuals have a strong commitment. It is, therefore, interesting to know whether individuals' sense of ownership toward information drive them to take actions to protect the information. Specifically, whether individual employees tend to comply with security policies when they believe that the own the information. In addition, if psychological is a major driver of compliance behavior, how to promote psychological ownership is, therefore, an interesting question as well. However, a lack of related systematic research on the impact of psychological ownership leaves this questions unanswered.

Therefore, the purpose of this study is to understand the impact of individuals' psychological ownership toward information on compliance behavior. Furthermore, given that motivation and capability are critical drivers of behavior, we also take self-efficacy into consideration. Self-efficacy is often used as manifest as competence or belief toward competence. In addition to understanding the impact of psychological ownership and self-efficacy on compliance behavior. We also attempt to understand the ways to enhance psychological ownership and improve self-efficacy. By answering these questions, this study contributes to information security research by showing that compliance behavior is also a function of individuals' psychological ownership. This study also provides guidance for practitioners to follow.

2 LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1 Compliance behavior

Compliance is required and expected behavior performed by individual employees. Since this is the basis for security behaviors, significant efforts have bene entered to understand the drivers of such behavior. Theories adopted to explain the taking place of such behavior include deterrence theory, protection motivation theory, agent theory, the theory of planned behaviors, the theory of reasoned action, or the combinations of the above theories. Deterrence theory based study (e.g. Chen et al. 2012) examined the impact of certainty and severity of reward and punishment on individuals' willingness to comply with security policies. While reward and punishment can be tangible, it may be in an intangible form, such as social pressure (Herath & Rao 2009a). In addition to external drivers, intrinsic motivation also plays a critical role in driving individuals to comply with such behavior (Son 2011). Some researchers (e.g. Bulgurcu et al. 2010; Hu et al. 2012) investigate into compliance behaviors from a theory of planned behavior perspective. The results mainly align with original theory that compliance behavior is a function of attitude, subjective norm, and perceived behavioral control. Another research stream adopted protection motivation theory to explore drivers of compliance behavior (e.g. Siponen et al. 2014; Siponen et al. 2006). According to protection motivation theory, the motivation of complying with information security to protect information is high when threat appraisal is high (e.g. individuals find the threats to be severe and the system is vulnerable) and when coping appraisal is high (e.g. individual are confident toward their capability in performing such behavior and are believe that taking those behaviors can actually secure information). One recent stream is to study the antecedents from the control perspective. In addition to traditional formal control approach (Boss et al. 2009), the importance of informal control has also been emphasized (Hsu et al. 2015).

2.2 Psychological ownership

Psychological ownership is defined as a state in which individuals feel as though the target of ownership (or a piece of that target) is theirs (i.e., it is 'MINE')" (Pierce et al. 2003 p.86). Human beings develop the sense of possession toward tangible or intangible targets. Such a sense of possession has affective, behavioral, and emotional consequences. When one develops psychological ownership toward on object, he/she sense a connection between him/herself toward the target. Individuals develop psychological ownership because of the needs to have a place, strengthen self-identity, and build confidence. Different from physical ownership which represents individuals actually possess the target from a legal perspective.

There are three routes lead to psychological ownership. First, controlling the target route means individuals tend to believe that they possess the target if they have the right to determine the place, the use, or who can access the target. In an organization, individuals develop ownership toward the organization when they believe they can control the organization through participating in the decision-making process. Second, investing the self into the target refers to the condition that individuals spend a significant amount of time and efforts on creating or maintaining the target. In an organization, when one spends a significant amount of time or effort on creating a target (e.g. information system), it is very likely for him or her to develop ownership of the information system. Third, knowing the target intimately indicates that individuals tend to develop ownership when they are very familiar with the target. For example, as the tenure increase, individuals tend to believe that they are not only employee of the organization. Instead, they are integrated with the organization and, therefore, they own the organization.

Past studies have classified psychological ownership into organization-based and job-based two types. Organization-based psychological ownership refers to employee's feelings of possession of organization and, on the other hand, job-based psychological ownership refers to individuals' psychological connect to their specific jobs or roles. These two foci positively correlate with each other, and job-based psychological ownership is an antecedent of organization-based psychological ownership. Job-related experiences, in general, affect perceptions of organization. While most studies focus on organization-based psychological ownership, several studies pay especially attention on job-based psychological ownership. Some researchers include both types of ownership in one study (e.g. Pierce et al. 2004).

In addition to job and organization, researchers have studies several foci of psychological ownership, such as idea and role. In IS area, the concept of psychological ownership toward information has been proposed to understand whether it affects one's perception of the threats and coping resources toward external security threats (Boss et al. 2015). However, there is no attempt has been made to understand whether the behavior of individual employee associates with psychological ownership toward information.

2.3 Self-efficacy

Self-efficacy is the strength of one’s belief in his/her own ability to complete task (Bandura 1977). As a component of social cognition theory, it represents a concept that Individuals’ behavior is affected by their self-evaluation (Bandura 1986). Individuals with strong self-evaluation tend to believe the possibility to reach the defined goal is high. As an outcome, they are willing to put more effort into achieving such goal. Even though this theory originated from learning-related research, it has been widely adopted in different areas.

In information systems area, computer self-efficacy has been broadly studied (e.g. Compeau & Higgins 1995). As the increase of security research, the importance of self-efficacy in information security has been highlighted. For example, Rhee et al. (2009) proposed that self-efficacy in information security lead to protection –related behaviors. Since individual employee’s compliance with information security policies is critical to the success of information security policies, it is, therefore, important to understand the extent to which employees are confidence toward performing such behavior. Self-efficacy to perform security-related behaviors is defined as an employee’s judgment of personal skills, knowledge, or competency about fulfilling the requirements of the ISP (Bulgurcu et al. 2010). In this study, we examine its impact on compliance behavior and also explore its antecedents.

2.4 Hypotheses development

Psychological ownership has been shown to have a positive impact on personal behavior or performance (Pierce et al. 2003). This impact may be directly or indirectly through increasing individuals’ commitment toward the organization. Employees with a strong commitment toward the organization are more likely to spend time and effort on desired activities. Psychological ownership of information refers to the extent to which individuals believe that information related to their tasks is theirs. Individuals, therefore, have a higher motivation to protect information security in the organizations (Shih & Liou, 2015). Therefore, it is expected that psychological ownership has a positive impact on compliance behaviors.

H1: Psychological ownership has a positive impact on compliance behavior

Self-efficacy is one’s belief in his/her ability to succeed in performing one behavior (Bandura 1977). Originated from social cognition theory, the concept of self-efficacy has been applied in many areas to understand the drivers of certain behaviors. This concept is also often integrated with other theories. For example, self-efficacy is often used to represent the level perceived behavioral control in studies based on the theory of planned behavior. Researchers, in general, argue a positive relationship between self-efficacy and behavior or its intention. Higher self-efficacy represents a higher level of beliefs on performing the action. In our study, target behaviors are those specified in information security policies. While some of those behaviors are complicated and need certain skills, the taking place of those behaviors is contingent on other factors. For example, one is more likely comply with information security and perform those behaviors when their efficacy toward performing those behaviors is high. Empirical studies also point out that self-efficacy is critical for security-related behaviors (Bulgurcu et al. 2010; Rhee et al. 2009). Therefore, we proposed the following.

H2: Self-efficacy has a positive impact on compliance behavior

In addition to hypothesizing the impact of self-efficacy on psychological ownership, we also attempt to understand their antecedents. For psychological ownership, by following the routes concept proposed by Pierce et al. (Pierce et al. 2001), we suggest three antecedents. Psychological ownership toward information is high when individuals can control information, when they invest a significant amount of time and effort in creating or working with the information, and when they are very familiar with the information. First, being able to control the information means that individuals can determine the ways to use the information, the places to store the information, or the individuals who can access the information. It is reasonable that individuals tend to believe that they have the information under such condition. Second, when individuals spend time or effort on creating the information or maintaining the information, they tend to believe that the information is theirs. Third, as indicated by Pierce et al. (2001), psychological ownership develops as one's familiarity toward the object increases. We argue that this also applies to our research context. It is easier for individuals to form ownership or believe that they own the information when they are more familiar with the content of information, the reason to have that information, or the history of the information. Therefore, we proposed the followings.

H3: Control right has a positive impact on psychological ownership

H4: Investing self has a positive impact on psychological ownership

H5: Knowledge has a positive impact on psychological ownership

On the other hand, for self-efficacy, we proposed that having IT and security educational background, receiving relevant training from internal or external, and experiencing security threats before increase one's efficacy in complying with behaviors listed in the security policies. First, education background provides individuals with sufficient knowledge of information technologies and how to secure information (Dodge Jr et al. 2007). It is reasonable that people with information technologies related educational background are more familiar with the structure of hardware and software. They have relatively more knowledge about potential threats from external (e.g. the types of virus and how they attack) and are more familiar with the way to prevent those attacks. Since those also listed in the security policies, as a result, they are more confident that they can perform those behaviors required by security policies.

Second, to assure employees can follow information security policies, organizations, in general, provide training to individuals who access to hardware and software (Parle et al. 1997). Employers can provide training through workshops, face-to-face training programs, or online training programs. Training allows individuals to understand potential threats from internal and external, be better aware of the content of security policies, know what conducts to avoid or to perform, and learn how to protect information (Herath & Rao 2009b). The above activities allow individuals to be more confident of their capabilities in dealing with information security issues.

Lastly, experiences also provide a basis for individuals to understand what must be done to avoid potential threats. Experiences with information leaking, virus attack, or other types of attack give individuals a sense of how severe it would be and how vulnerable current information system can be. In addition, experiences in facing such conditions also allow individuals to know what might have to be done to avoid similar experiences. Therefore, we hypothesize the followings.

H6: Training has a positive impact on self-efficacy

H7: Background has a positive impact on self-efficacy

H8: Experience has a positive impact on self-efficacy

3 RESEARCH METHOD

The research model of this study is shown in Figure 1. To verify this research model, we are planning to conduct a survey research. All items to capture concepts of each construct were adopted from literature. Through validating the proposed hypotheses, this study contributes to security studies in this area by showing the impact of psychological ownership on compliance behavior. In addition, we also identify possible antecedents to develop psychological ownership. Based on our research, researchers can further explore the impact of different targets or foci of psychological ownership and practitioners may have a better understanding about how to assure employee’s psychological ownership if it is critical for compliance behaviors.

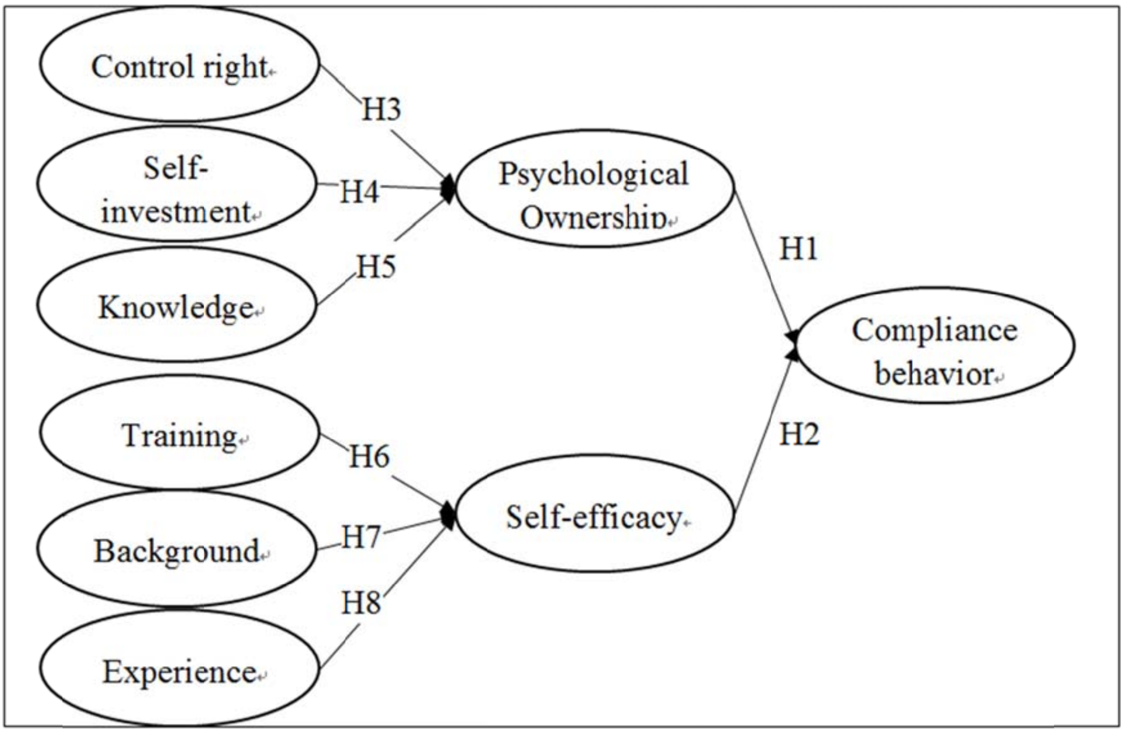

Figure 1. Research model

4 DATA ANALYSIS

This studies adopted a survey approach to collected required data to verify the proposed hypotheses. Target samples are employees who use information technologies (including computers, tablets, mobile phone, or other devices) at their works to process all kind of information. Except for one construct, items for rest constructs were adopted from past studies. We conducted a pilot test with 20 MBA students and then made minor modifications on few items. An online survey based on Google online service was created to collect required data. The data collection period ran from March to May 2015. A total of 256 individuals participated in this study. Excluding 22 of them are incomplete; the final usable sample is 234. Table 1 shows the demographic information of the 234 responses.

Variables	Categories	#	%	Variables	Categories	#	%
Gender	Male	53	22.6	Education	Graduate	33	14.1
	Female	181	77.3		College	188	80.3
Age	<= 25	28	11.8		Others	13	5.5
	26-30	75	32	Industry	Manufacturer	49	20.9
	31-35	70	22.9		Service	170	72.6
	36-40	23	9.8		Others	15	6.3
	41-45	14	6	Position	Employee	192	82.1
	>=46	24	10.2		Administrator	42	17.9

Table 1. Demographic information

Variables	*Mean*	*Std. Dev.*	*AVE*	*CR*	CO	SI	KN	TR	BG	EX	SE	PO	CB
Control	3.41	0.85	0.74	0.92	0.86								
Self-investment	3.39	0.81	0.73	0.92	0.48	0.85							
Knowledge	3.72	0.70	0.81	0.94	0.38	0.44	0.9						
Training	3.22	0.91	0.84	0.94	0.20	0.18	0.25	0.91					
Background	2.93	0.98	0.82	0.93	0.23	0.35	0.33	0.54	0.91				
Experience	2.83	0.93	0.58	0.80	0.06	0.08	0.06	0.08	0.17	0.76			
Self-efficacy	3.88	0.56	0.66	0.94	0.18	0.22	0.36	0.39	0.45	-0.12	0.81		
Psychological ownership	2.84	0.97	0.80	0.85	0.50	0.25	0.16	0.18	0.25	0.17	0.15	0.89	
Compliance behavior	4.19	0.59	0.91	0.97	0.09	0.10	0.29	0.23	0.16	-0.10	0.46	-0.12	0.95

Table 2. Descriptive analysis and correlation matrix

5 CONSTRUCT AND MEASUREMENT

For security compliance intention, a total of 3 items adapted from Williams and Anderson (1991) were used to measure the extent to which individuals tend to perform behaviors specified in security policy. For self-efficacy, three items adapted from Rhee et al. (2009) were used to capture the extent to which individuals have confidence in performing behaviors specified in security policies. For the antecedents of self-efficacy, several items adopted from Rhee et al. (2009) were used to capture the extent to which individuals have security related background, have related experience, and received training from organizations. For Psychological ownership, a total of 4 items were adapted from Van Dyne and Pierce (2004) were used to capture the extent to which individuals believe that they possess the information related to their works. For antecedents, items adopted from Buchem (2012) were used to capture the extent to which individuals can control the information, invest time and effort in the information, and have sufficient understanding toward the information. As shown in Table 2, those items used to measure used constructs meet minimum reliability and validity requirements.

5.1 Hypotheses testing and discussion

PLS was used to verify the proposed hypotheses. As shown in Figure 2, even though the impact of both psychological ownership and self-efficacy were found to be significant, only self-efficacy aligns with the proposed direction. Therefore, H2 is supported but H1. Psychological ownership and self-efficacy explain 28 percent variance of compliance behavior. For the antecedents of psychological ownership, the impact of control is positive and significant. However, investment and knowledge have limited effects on psychological ownership only. The result only supports H3. Also, three antecedents explain 26 percent variance of psychological ownership. For self-efficacy, while all precursors were found to be significant, the negative impact of experience indicates a conflict with our hypothesis. Therefore, the test results only support H6 and H7. Furthermore, the three proposed antecedents explain 27 percent variance of self-efficacy.

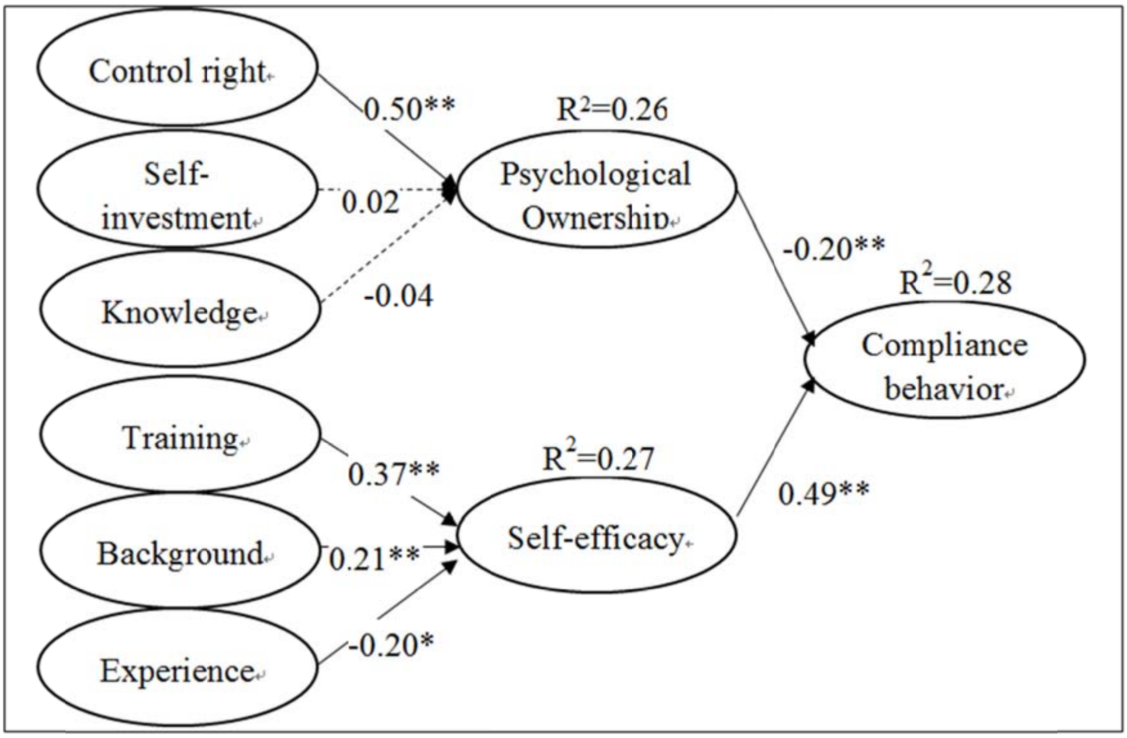

Figure 2. Path analysis

6 DISCUSSION

Among the eight proposed hypotheses, five of them are significant in the expected direction, two of them (self-investment and knowledge) were found insignificant, and two of them (psychological ownership and experience) are significant but in a different direction. Therefore, five out of 8 proposed hypotheses were supported.

For the antecedents of psychological ownership, while the control right has a positive and substantial impact, two of the three proposed antecedents were found to have no impact. This result indicates that individuals tend to believe that they own the data only if they can control the data. For example, they may have the right to use the data, can determine who can access the data, and determine how to utilize the data.

The insignificant coefficient of self-investment indicates that individuals may not develop ownership toward the data even they spend significant time on creating the data. One possible reason is that many of our respondents are frontline employees who use information systems developed by management information systems department to perform routine tasks. Even though employees use the information system to process routine tasks, data is stored in the central database instead of on their computer. Also, even though employees may create the data through entering information physically, they have a limited right to access it. They even cannot alter the content without permission. As a result, employees do not develop ownership toward the data.

Also, individuals do not develop ownership toward the data even knowing what the data is, why the data is needed, and how the data is created and used. Many of our samples are frontline employees and knowing the data may not be sufficient for such type of employees to generate ownership. The small averaged score of psychological ownership indicates that employees, in general, do not believe that they own the information related to their work.

For two links with a direction different from our initial expectation, the result is even more interesting. First, we expect that individuals tend to have higher confidence in dealing with information security if they have experiences with information leaking, virus attack, or other information security issues. However, our study reaches an opposite conclusion. Having related experiences (countering security threats or problems before) is associated with self-efficacy negatively. However, this result is not unreasonable. People who have experience with information security issue may find that information leak or virus attack still happen even they have tried very hard to prevent it. Since information leak still happen after those individuals take some actions to protect information, people suffer from security problems tend to believe that they may not be able to perform security policy behaviors correctly or may have done something wrong in the process. Such perception reduces their confidence toward adequately performing correct security practices. As an outcome, low efficacy is then observed.

Psychological ownership also shows a negative impact on compliance behavior. One plausible explanation is that individuals' psychological ownership toward information leads them to believe that they can use the information the way they want, including bring the data home, save it in any places they want, or change the content without permission from others. However, security policies in general limit individuals' access, use, and storage of the data. Following security policies precisely implies that individuals must give up their control of information or data. In general, following steps specified in the policies increase the level inconvenience. Doing so also reduces the extent to which employees can control data. As an outcome, their willingness to comply with the security policies is then low. Therefore, a negative relationship between psychological ownership is then observed.

7 CONCLUSION

In this study, we focused on understanding how one's compliance behavior is affected by individuals' psychological ownership toward information and efficacy toward performing practices demanded by security policies. Besides, we also attempt to explore potential antecedents of psychological ownership and self-efficacy. Data collected from 234 information systems users shows some results contradicted to our initial expectations.

This result contributes to both psychological ownership and information security literature in the following ways. First, we show that psychological ownership may not always have a positive impact on desired behavior. The surprising result implies that foci of psychological ownership are critical. While past studies largely focus on organization-based and/ or job-based psychological ownership, we shifted the focus to information-based psychological ownership and found that information-based psychological ownership has no impact on organization-based behaviors. However, compliance behavior is one type of in-role behavior and may be strongly driven by job-baed or organization-based psychological ownership. We, therefore, encourage future research to take both organization-based psychological ownership and information-based psychological ownership into consideration at the same time to further clarify the impacts of different levels of psychological ownership.

Second, for information security literature, we drew one interesting conclusion that having security related experience does not give individuals more competence toward reacting to similar situations. In fact, individuals may find themselves less confident after experiencing security leaking or virus attack. The result implies that people with such experience tend to believe that they cannot do things perfectly to prevent information leak. As an outcome, they have less confident toward performing behaviors related to information security. Future research may explore the potential ways to ease such problem.

References

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191-215.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall, Inc.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, *39*(4), 837-864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. (2009). If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164.

Buchem, I. (2012). Psychological ownership and personal learning environments: Do sense of ownership and control really matter? In *PLE Conference Proceedings* (Vol. 1, No. 1).

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

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

Chen, Y., Ramamurthy, K., and Wen, K.W. (2012). Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157-188.

Compeau, D. R., and Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19(2), 189-211.

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), 79-98.

Dodge Jr, R. C., Carver, C., and Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73-80.

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

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

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. Information Systems Research, 26(2), 282-300.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Lee, S. M., Lee, S. G., and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.

Parle, M., Maguire, P., and Heaven, C. (1997). The development of a training model to improve health professionals' skills, self-efficacy and outcome expectancies when communicating with cancer patients. Social Science and Medicine, 44(2), 231-240.

Pierce, J. L., Kostova, T., and Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. Academy of Management Review, 26(2), 298-310.

Pierce, J. L., Kostova, T., and Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. Review of general psychology, 7(1), 84.

Pierce, J. L., O'Driscoll, M. P., and Coghlan, A.M. (2004). Work environment structure and psychological ownership: The mediating effects of control. The Journal of Social Psychology, 144(5), 507-534.

Rhee, H. S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

Shih, S. P., and Liou, J. Y. (2015). Investigate the Effects of Information Security Climate and Psychological Ownership on Information Security Policy Compliance.Proc. 19th Pacific Asia Conference on Information Systems. Singapore.

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

Siponen, M., Pahnila, S., and Mahmood, A. (2006). Factors influencing protection motivation and is security policy compliance. Proc. Innovations in Information Technology. p. 1-5.

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

Van Dyne, L., and Pierce, J. L. (2004). Psychological ownership and feelings of possession: Three field studies predicting employee attitudes and organizational citizenship behavior. Journal of Organizational Behavior, 25(4), 439-459.

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

Williams, L. J., and Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. Journal of management, 17(3), 601-617.