INVESTIGATE THE EFFECTS OF INFORMATION SECURITY CLIMATE AND PSYCHOLOGICAL OWNERSHIP ON INFORMATION SECURITY POLICY COMPLIANCE

Sheng-Pao Shih, Department of Information Management, Tamkang University, Taiwan, R.O.C., sbao@mail.tku.edu.tw

Jia-Yin Liou, Department of Information Management, Tamkang University, Taiwan, R.O.C.

Abstract

Currently, information security policy compliance research mainly investigates information security compliant behaviors of employees from general deterrence theory or protection motivation theory. However, these studies focus on the discussions of security specifications in organization and the motivations of individuals' behaviors but omit the influences of contextual effects on employees' psychological states and employees' information security policy compliance. To fill this gap, we consider information security climate as background factors and psychological ownership as personal factors to investigate their impacts on information security policy compliance intentions. We will collect data from employees working in the high-tech industry in Taiwan to explore the relationships proposed in the research model. We conclude by explicating the implications of this research for academics and practitioners, along with compelling future research possibilities.

Keywords: Information security climate, psychological ownership, information security policy compliance intention.

1 INTRODUCTION

Information systems (IS) security has received a great deal of attention over the past 10 years. To reduce the risks from information security threats, managers have devoted energies to protect assets in organizations. In a security survey published in 2013, information security consulting services have increased fifteen percent in security evaluation on companies, compared with the year of 2012 (Forrester 2013). Although firms are devoting substantial resources to develop technologies and processes that can help safeguard the security of their computing assets (Boss et al. 2009; D'Arcy et al. 2009; Vance et al. 2013), increased attentions have been focused on the role that people play in maintaining an information security environment (Anderson & Agarwal 2010). Based on this anchor, numerous behavioral studies have been proposed to either improving employees' compliance with the organization security policies or explaining employees' IS misuse or abuse (Li & Siponen 2011). These behavioral approaches draw upon theories of Criminology and Psychology, such as Deterrence Theory (D'Arcy *et al.* 2009), Neutralization Techniques (Siponen & Vance 2010), Control-Reactance (Lowry & Moody 2014) and Socio-Cognitive (Myyry et al. 2009). Furthermore, due to the relatively human nature of adherence to security policies, organizations find enforcement of information security a critical challenge. Thus more recently, research in behavioral information security has started focusing on employee's intention and awareness to follow security policies (e.g. Bulgurcu et al. 2010; Herath & Rao 2009a). Specifically, some research has suggested that information security is an interplay between multidimensional disciplines (von Solms 2001). However, past studies have largely ignored contextual factors which may affect individuals' psychological states and security behaviors. This suggests the importance of understanding organizational environment such as climate (Chan et al. 2005). Past work safety studies have found a direct relationship between safety climate and safety behavior (e.g. Cooper & Phillips 2004; Glendon & Litherland 2001). We therefore argue that there is a need to study the organizational environment and develop a better understanding of the information security climate through theoretical arguments in the information security context. In addition, psychological ownership has emerged as important factors in the determination of social behavior in general, and health behaviors in several domains. Nevertheless, in information security settings, whether psychological ownership serves as a mediation variable in the relationship between information security climate and employees' security-related behaviors, for example, employees' intentions to comply with information security policy is still unknown. Managers have devoted lots of resources and facilities to enhance security level but may neglect human side of employees in organizations. Therefore, to fill the above mentioned research and practical gaps, and to understand the effects of context on psychological factors, drawing on the perspective of social-cognitive mediation process, we develop a research model that tries to investigate the effects of the work environment related to information security context (i.e. information security climate) and conceptualize information security climate as a higher order factor resulting from various organizational security practices. We attempt to fill the gap in the existing literature by providing a social influence process to psychological state to investigate how information security climate influence psychological ownership and in turn affect employees' information security policy compliance intention.

2 LITERATURE REVIEW

2.1 Information Security Policy Compliance

Similar to other organizational policies, security policy is a foundational tool that translates the expectations of security management into clear, specific, and measureable objectives and mandates (Goel & Chengalur-Smith 2010). The purpose of information security policy is to influence and drive actions and behaviors of employees that are consistent with the information systems security requirements in organizations. Goel and Chengalur-Smith (2010) suggest that security policy should be carefully drafted to attain desired goals and objectives by bring breath, clarity, and brevity of

security contents when drafting a security policy because all members in the organization are subjects to comply with security policy. Past information security policy compliance studies have adopted various theories to investigate this issue, such as general deterrence theory (Herath & Rao 2009a; Pahnila et al. 2007), protection motivation theory (Herath & Rao 2009b; Ifinedo 2012; Posey et al. 2013; Siponen et al. 2014; Vance et al. 2012), theory of planned behaviour (Bulgurcu *et al.* 2010; Hu et al. 2012), and theory of reasoned action (Pahnila *et al.* 2007; Siponen & Vance 2010). Recent studies started to investigate the effect of security climate on employee compliant behavior (Chan *et al.* 2005; Goo et al. 2013). However, Goo et al. (2013) only considers the effect of information security climate on organizational commitment but neglects the effect of information security climate on psychological ownership. We claim that security climate can enhance the possession feelings of employees because of safety information technology working atmosphere and, consequently, influence the intentions to comply information security policies.

2.2 Psychological Ownership

Some psychological factors, such as information security awareness, normative beliefs, self-efficacy, have been discussed in information security research (e.g. Bulgurcu *et al.* 2010). The psychological ownership is different from these psychological factors, because its main focus is the feelings of possessiveness and being psychologically tied to an object (Pierce et al. 2001: 299). Psychological ownership refers to the relationship between an individual and an object in which the object is experienced as connected with the self (Blau & Caspi 2009: 49). Feeling of psychological ownership draws upon the concepts of territoriality, which means an individual possess feelings for the target. Thus, psychological ownership can be described as psychological possession feelings of ownership. Psychological ownership can have positive or negative orientation toward changes, and is dependent on the types of change involved (Van Dyne & Pierce 2004). In this study, we define psychological ownership as an employee who has the feeling of a strong sense of ownership toward the particular information systems in organizations handled by an individual.

2.3 Information Security Climate

From social information view, organizational environment such as organizational climate may affect individual behaviors (James & James 1989). Organizational climate is defined as a set of attributes that are known as key predictors of individual behaviour in organizations. Such climate mediates the relationship between objective characteristics of working conditions (organizational policies, practices. and procedures) and an individual's working behavior (Campbell, 1971). In other words, climate is considered to be a perceptual medium through which the effects of the organizational context are translated into an employee's behavior. Similarly, the concept of information security climate is especially useful in this study since information security can be considered as a form of safety in the organization, and information security climate emphasizes employees' compliance with policies or regulations organizations present as well. Recently, Chan et al. (2005) conceptualized information security climate and empirically analysed the relationship between information security climate and compliant behavior. While extant studies views security climate as organizational members' perceptions emanated from various "observable" security policies, practices and procedures as a whole (e.g., Chan et al. 2005), they conceptualized the security climate as a unidimensional one. We believe that information security climate is a high-order factor composed of some organizational security practices. Following Griffin & Neal (2000) and Goo et al. (2013), we take the information security climate as a second-order factor composed of specific first order factors under the information security context.

3 RESEARCH MODEL

In this section, the review of related literature and theories are provided. We begin with a brief overview of the research model of this study. We then argue the socio-cognitive mediation process to

explain employees' information security policy compliance behaviors through the information security climate and employees' psychological ownership.

Typically, organizations view security behaviors as employee compliance with information security routines and specifications. These behaviors comprise computer security activities that are part of the formal work role and procedures, such as using personal information protective procedures correctly, properly performing lock-out screen when temporary absent, applying appropriate work practices to reduce exposure to potential hazards and attacks from the Internet, and following regular password changing policies and requirements. Furthermore, information security behaviors can be understood as the result of the socio-cognitive mediation process (Herath & Rao 2009b; Vance *et al.* 2012). Specifying the causal order of variables is critical to making inferences about mediational relationships (Mathieu & Taylor 2006). In this study, information security policy compliance behavior is influenced by socially constructed shared perceptions among employees of an organization with regard to information security specifications, procedures, and practices. Employees judge the value that organization attaches to information security through the information security statements and policies. Employees' psychological feelings and belongings are proximal antecedents to security behaviors and may also influence the motivation to perform security behaviors. In an organization, antecedents for employee to perform security behaviors are related to the way individuals perceive the value of security in their organizations. If individuals perceive that their organizations are concerned about the security, they will develop positive attitudes and commit to carry out behaviors that benefit the organization to meet security standards. Information security climate provides the atmosphere and invisible norms in the environment with an overall security practices to motivate employees to perform security behaviors, i.e. complying information security policy. Therefore, information security climate acts as an antecedent for individual psychological feelings since the socio-cognitive mediation explain such psychological process. Accordingly, this study proposes a sequential mediation process between information security climate and information security policy compliance behavior that aims to enhance our knowledge about the antecedents and determinants of security behaviors. From the logic discussed above, the research model is depicted graphically in Figure 1. Besides, in order to control the effects of deterrence that often adopted by organizations, we also include general deterrence variables as control variables according to prior information security policy compliance studies (D'Arcy & Herath 2011).

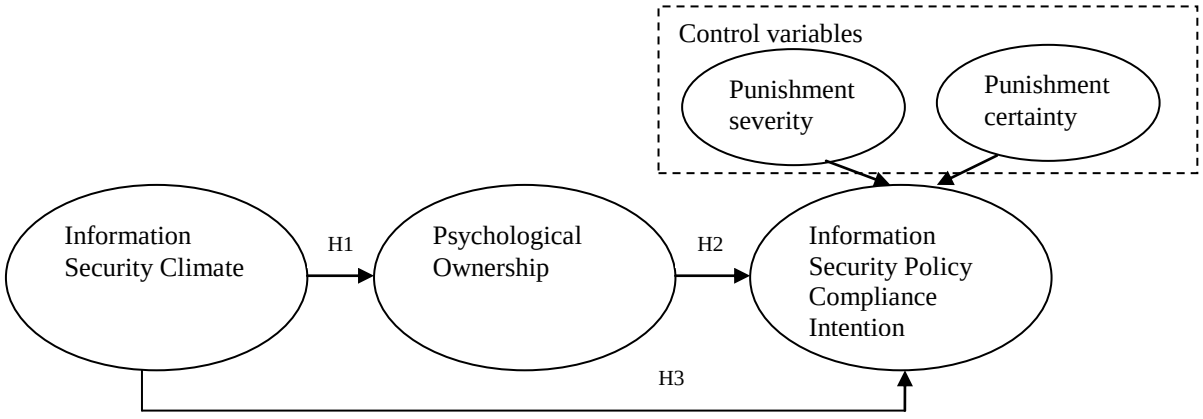

Figure 1. Research Model

3.1 Information Security Climate and Psychological Ownership

Information security climate is defined as individual perceptions of safety-related specifications, practices, and procedures that affect the information security in organizations. An information security climate reflects environments where security information is formally communicated through training and meetings, and informally through discussion and dialogue in teams, where security events are quickly solved, regardless of the cost, and where there is a vast investment in security training. A positive information security climate is expected to lead to the development of positive security

feelings in individuals through principles of social exchange. In this sense, security climate provides employees the context with security guard and atmosphere to affect their feelings of possession or ownership of the systems they handled in the organization (Pierce et al., 2001). Thus, the following is hypothesized:

H1: Information security climate is positively associated with psychological ownership.

3.2 Psychological Ownership and Information Security Policy Compliance Intention

Psychologists consider ownership as a prime motivator of human behavior. Researchers propose that psychological ownership may produce positive actions such as in-role behaviors (Van Dyne & Pierce 2004). Information security policy can be an in-role behavior because individual performs information security requirements that are specified in security policies. Van Dyne & Pierce (2004) found a significant positive relationship between psychological ownership and employee performance. Therefore, we expect that psychological ownership would encourage employees to perform a higher level of security performance which includes the compliance with information security policy. We propose the following:

H2: Psychological ownership is positively associated with information security policy compliance intention.

3.3 Information Security Climate and Information Security Policy Compliance Intention

Safety climate makes an obvious safty goal from employees' perceptions(Campbell, 1971). Traditional safety research indicated that safety climate positively affects safety behaviors (Cooper & Phillips 2004; Johnson 2007; Zohar & Luria 2004), such as complying safety work practices (Neal & Griffin 2006). Extending this logic to the information security context, Goo et al. (2013) indicated that information security climate can be formed by top management attention, security enforcement, security policy, and security awareness program. Improving the information security climate through great security attentions from management, security specifications to enforce security working habit, or security training to strengthen information security awareness, employee would be more likely to have the intentions to comply information security polies. For example, regular password changing increases security level of users, and in the meantime, raises the possibilities for employees to exhibit compliant behaviors. We propose:

H3: Information security climate is positively associated with information security policy compliance intention.

4 RESEARCH METHODS AND ANALYSIS

A cross-sectional survey will be conducted to collect required data to examine our proposed model. The key informants of our study are the employees work in corporations. The target sampling frame of this survey will be the employees working in the companies selected from "CommonWealth" magazine, a considerably well-known and credible practical magazine in Taiwan. The study will focus on top 500 high-tech industry because they are more conscious of information security issues. We believe our sampling frame is capable of representing the information security viewpoints from high-tech industry. We will contact the managers in the identified organization from the survey list to obtain their willingness to join our study. Follow-up questionnaires will be sent again and phone calls will be made to those firms who don't reply back at the first stage. After the survey returns, this study will do statistic analysis with SmartPLS (Ringle et al. 2005) to test related validity and reliability issues. All the hypotheses testing can be done by examining the significant level of coefficients between corresponding research variables in the proposed model.

5 EXPECTED CONTRIBUTIONS

The study will clarify the relationships between the information security climate, psychological ownership and their impacts on information security policy compliance intentions. Overall, the study will provide the following contributions. First, this study conceptualized information security climate as a multidimensional concept and operationalized it as a second-order construct composed of dimensional components. Second, we found no empirical studies that have explored the relationships between information security climate and psychological ownership in the context of information security. Other than numerous past security studies focus on the deterrence effects to enhance employees' compliance behavior, we consider deterrence as control variables and contribute to the information security management literature from the social-cognitive mediation process perspective, the viewpoints from information security climate and psychological ownership, to understand the informal positive influences on employee's information security compliance intentions.

References

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

Blau, I., and Caspi, A. (2009). What type of collaboration helps? Psychological ownership, perceived learning and outcome quality of collaboration using google docs. Proceedings of the Chais Conference on Instructional Technologies Research：Learning in the Technological Area. pp. 48-55.

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.

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 & Security, 1(3), 18-41.

Cooper, M. D., and Phillips, R. A. (2004). Exploratory analysis of the safety climate and safety behavior relationship. Journal of Safety Research, 35(5), 497-512.

D'Arcy, J., and Herath, T. (2011). A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.

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.

Forrester, R., (2013) The forrester wave: Information security consulting services, In: Forrester Research.

Glendon, A. I., and Litherland, D. K. (2001). Safety climate factors, group differences and safety behaviour in road construction. Safety Science, 39(3), 157-188.

Goel, S., and Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. The Journal of Strategic Information Systems, 19(4), 281-295.

Goo, J., Yim, M.-S., and Kim, D. J. (2013). A path way to successful management of individual intention to security compliance: A role of organizational security climate. Rochester, pp. 1-24.

Griffin, M. A., and Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation. Journal of Occupational Health Psychology, 5(3), 347-358.

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.
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.
James, L. A., and James, L. R. (1989). Integrating work environment perceptions: Explorations into the measurement of meaning. Journal of Applied Psychology, 74(5), 739-751.
Johnson, S. E. (2007). The predictive validity of safety climate. Journal of Safety Research, 38(5), 511-521.
Li, Y., and Siponen, M. (2011). A call for research on home users' information security behavior. Proc. Proceedings of the 15th Pacific Asia Conference on Information Systems. Brisbane, pp. 1-11.
Lowry, P. B., and Moody, G. D. (2014). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, forthcoming
Mathieu, J. E., and Taylor, S. R. (2006). Clarifying conditions and decision points for mediational type inferences in organizational behavior. Journal of Organizational Behavior, 27(8), 1031-1056.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), 126-139.
Neal, A., and Griffin, M. A. (2006). A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels. Journal of Applied Psychology, 91(4), 946-953.
Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behavior towards is security policy compliance. *Proc. 40th Hawaii International Conference on System Sciences (HICSS 2007). Hawaii, USA*, 156b-156b.
Pierce, J. L., Kostova, T., and Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. Academy of Management, 26(2), 298-310.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quarterly, 37(4), 1189-1210.
Ringle, C. M., Wende, S., and Will, A., (2005) Smartpls 2.0 (beta).
Siponen, M., Adam Mahmood, M., and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.
Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.
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., Lowry, P., and Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of management information systems, 29(4), 263-289.
Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. Information and Management, 49(3-4), 190-198.
von Solms, B. (2001). Information security — a multidimensional discipline. Computers & Security, 20(6), 504-508.
Zohar, D., and Luria, G. (2004). Climate as a social-cognitive construction of supervisory safety practices: Scripts as proxy of behavior patterns. Journal of Applied Psychology, 89(2), 322-333.