Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

The Role of Formal and Social Control in Information Security Behaviors

Yu Wen Hung
National Sun Yat-sen University, d004020004@student.nsysu.edu.tw

Jack Shih-Chieh Hsu
National Sun Yat-Sen University

Sheng-Pao Shih
Tamkang University

The role of formal and social control in information security behaviors

Yu Wen Hung[1]
Department of Information Management, National Sun Yat-Sen University,
Kaohsiung, Taiwan

Jack Shih-Chieh Hsu
Department of Information Management, National Sun Yat-Sen University,
Kaohsiung, Taiwan

Sheng-Pao Shih
Department of Information Management, Tamkang University,
Taipei, Taiwan

ABSTRACT

The purpose of this study is to explore the effect of formal and social control on in-role and extra-role security behaviors. Following past studies, we reexamine the effect of formal control on behaviors. Based on social control theory, we further hypothesize the effect of social control on security behaviors. Data collected from 259 members of IS departments confirmed our hypotheses that both formal control and social control generate effects on both in-role and extra-role security behaviors. Implications for academia and practitioners are also provided.

Keywords: Information security, formal control, social control, in-role and extra-role behavior

INTRODUCTION

The importance of information security has been emphasized by various studies (Boss et al. 2009; Herath and Rao 2009; Lee and Lee 2002; Lee et al. 2004). Organizations rely heavily on information systems amidst increasing threats from the Internet, making this issue even more salient. Recently, using the perspective of attitude-behavior oriented theories (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Ifinedo 2012; Zhang et al. 2009), academics and practitioners in the IS area have started focusing on understanding what drives IS department members to perform

[1] Corresponding author. d004020004@student.nsysu.edu.tw +886 7 5252000#4760

unethical behaviors. One of the most common conclusions is that a certain level of control is needed to reduce delinquent behaviors or increase precaution. Specifically, formal control mechanisms play a critical role in driving individuals to comply with organizational policy. The major drivers of compliance behaviors are formal control mechanisms including specifications, evaluations and rewards (Boss et al. 2009). However, organizational behavior literature indicates that, in addition to in-role behaviors, extra-role behavior has been highly valued by managers. In-role behavior refers to those behaviors that are indicated in security policies. Extra-role behavior refers to behaviors that are not listed but benefit the organization's information security (D'Arcy and Greene 2009). Better collaborative outcomes can be obtained when extra-role behaviors are also observed (Bedwell et al. 2012). Given that an organization is a social entity in which it may be hard to rely solely on formal control mechanisms, the purpose of this study is to examine the impact of both formal and social control on individuals' in-role and extra-role behaviors, based on social control theory.

By exploring the effect of formal and social controls on behaviors, we urge managers not to ignore the exercise of social control in addition to formal control. The paper proceeds as follows. Next, we review the literature applicable to the proposed problems and propose corresponding hypotheses. This is followed by a conceptual model, the research methodology and the field study used to test the proposed hypotheses. We then offer data analysis and discussions. The paper concludes with a summary of key points and contributions.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Formal Control

One important research stream in understanding employee behavior regards control. The goal of control is to motivate individuals to comply with the desired behavior (Das and Teng

1998; Eisenhardt 1985). In the IS area, control theory has been adopted to understand the extent to which the exercising of different control mechanisms, and their combinations, can effectively drive information system developers to perform effectively (e.g., Boss et al. 2009). The most common conclusion is that, with effective controls which drive individuals to perform desired behaviors or actions, acceptable project performance can be ensured. Viewed through this organizational control lens, one recent study built a model to explain individual information security precaution-taking behavior (Boss et al. 2009). The proposed formal information security control mechanism includes specification, evaluation and reward. Those control mechanisms are similar to the behavioral or outcome control proposed by Kirsch (1996).

Specification refers to formalized statements which articulate desired behaviors or outcomes and are typically codified as organizational policies and procedures. Specification provides employees with the direction of the desired goal, and ways to achieve this goal. *Evaluation* is a process of data collection and comparison to examine the extent to which an individual's behavior or performance meets the specification. With evaluation, managers can then determine adjustments required for any deviations. *Reward* refers to the implicit or explicit consequences of the violation of or compliance with a specified behavior. It sends a signal to employees that compliance with the specified behavior is desired. With specified procedures and a clearly expected outcome, managers can then determine the reward or punishment for individuals based on how well their behaviors meet expectations or the expected outcomes are observed. Boss et al. (2009) found that the acts of specifying policies and evaluating behaviors are effective in convincing individuals that security policies are mandatory; therefore, compliance behaviors are observed. Therefore, we hypothesized:

H1a: Formal control is positively associated with in-role security behavior.

In addition to its impact on in-role behavior, this study also attempts to build a link between formal control and extra-role behavior, such as helping others in the department learn about the security policy and speaking up with ideas for the security policy. Although the performing of behaviors not listed in the specification does not lead to direct reward, we argue that formal control still generates an effect on extra-role behaviors because of interdependence (Bachrach et al. 2006; Organ 1988; Podsakoff et al. 2000; Van der Vegt et al. 2003). Specifically, interdependence is the major driver of altruistic security behaviors and formal control serves as a critical facilitator. Under a highly interdependence context, individuals within the same units have to work jointly to achieve a common goal. It is understandable that the inability to protect critical information may lead to disaster, which affects the working condition and outcome of all individuals within the same unit. For example, the leaking of customer information leads to low customer satisfaction, complaints, or even legal problems. Although a specific individual may not necessarily be responsible for the outcome, the damage caused generates an impact on each individual in the organization. Workload is increased in the aftermath and extra effort must be spent on pulling the organization's operations back on track. This also decreases work efficiency or increases difficulties for others to perform their regular work. On the other hand, formal control serves as an educational tool which allows individuals to understand the consequences of inappropriate conduct. That is, since individuals are then more aware of such conduct, they are more capable to assist others, including introducing those rules to newcomers and providing suggestions to those conducting themselves inappropriately. For example, specification allows members to know the desired behaviors which lead to a secure system, or unwanted behaviors which may weaken the protection. Information security policies not only contain specific rules but also specify the possible consequences of inappropriate conduct. We argue that if people are

more aware of security threats and possible consequences, they are more likely to assist others to protect their computers in order to avoid possible interference with their own work. Therefore, we hypothesize:

H1b: Formal control is positively associated with extra-role behavior.

Informal Control: Social Control (Bond) Perspective

Different from formal control, informal control is related to methods that are based on social or people-related strategies (Eisenhardt 1985; Kirsch 1996). The aim of informal control is to ensure that individuals act in a way consistent with the desired objectives of the project and in a manner that is in line with the ideology of the work environment (Choudhury and Sabherwal 2003). Informal control includes *self control* and *clan control*. Self control largely relies on individuals themselves, and clan control is exercised by selecting members and socializing them into a set of norms and values shared by the whole organization. In an interdependent context, clan control can be adopted when task-related behaviors and outcomes are not pre-specified. Clan control generates its effect through allowing organization members to jointly determine the project goals and how those goals should be attained.

Social control theory, also known as social bond theory, is proposed by Travis Hirschi (1969) and has been widely applied in criminology. This theory attempts to explain causes of social behavior that does not conform to generally accepted social rules. It is based on the hypothesis that despite a person's natural inclination towards crime, strong social bonds deter him/her from committing criminal acts. The chances of a person being involved in a crime increase when social bonds become weaker. Later researchers indicated that the more a person is attached to his referent goals, the less likely the person will be to engage in delinquent behavior (Vardi and Wiener 1996). This theory indicates that individuals' behavior is affected by four

major bonds with their surroundings: commitment, attachment, involvement and belief. In the following, based on these four major bonds, we discuss the relationship between social control and behaviors.

Meyer and Allen (1991) classified *commitments* into three types: continuance, affective and normative. Continuance and normative commitments drive individuals to perform in-role behavior. Those with strong continuance commitment may do only what is required to keep their jobs, and those with strong normative commitment may exhibit behaviors which meet organizational goals because they believe it is the right and moral thing to do. *Attachment* highlights individuals' sensitivity toward those to whom they have strong relationship, and the importance of that attachment to inhibiting the performance of delinquent behaviors. Individuals tend to perform desired behaviors (or "comply") in order to avoid negative feedback from others. Individuals who are strongly attached to coworkers are sensitive to the judgment of these important people and tend not to disappoint them. As an outcome, compliance behavior is a function of the perceived security within the organization (Chan et al. 2005). Theory of Planned Behavior (TPB) (Ajzen and Fishbein 1980) highlights the importance of *belief* on behavioral intention. The theory argues that an employee's attitude towards performing a given behavior is related to his/her belief about behavior-related consequences. In fact, many studies have shown the effect of belief or attitude on behavioral intention (e.g. Lee et al. 2004). In social control theory, *involvement* refers to engagement in conventional activities. Participatory decision making theory indicates that employees are more like to accept a decision if they are involved in the decision making process (Irvin and Stansbury 2004). James (1996) also indicated that users are more accepting of information security measures when they are involved in the process and

contribute to the solutions of any identified issues. A study by Lee et al. (2004) shows that employees' participation in informal meetings is effective in reducing their computer abuse.

H2a: Social control is positively associated with in-role behavior.

Among the three components of organizational *commitment*, extra-role behavior is more affected by the affective and normative components. Employees with a strong affective commitment are those strongly committed individuals who identify with, are involved in, and enjoy membership in the organization. They are therefore believed to be willing to exert great effort on behalf of the organization (Mowday et al. 1979). Normative commitment drives individuals to believe that they are part of the organization and that the performing of prosocial behaviors can benefit the organization and are therefore their responsibility (Wiener 1982). For *attachment* to colleagues, social control theory argues that the performing of delinquent behaviors is due to a lack of attachment which leads individuals to ignore opinions and expectations from others. Since one is sensitive to others when he/she is attached to them, receiving positive feedback from others is important as well. Although engaging in extra-role behaviors is not recognized by the formal reward systems, individuals may receive informal appreciation or recognition from supervisors or colleagues (Organ 1988). For *involvement* in the policies' related activities, participatory decision making also indicates that employees are more eager to see the policies succeed if they are involved in the policy-making process (Irvin and Stansbury 2004). Therefore, they tend to spend extra effort and take possible actions to increase the possibility of success. Lastly, for *belief*, organizational behavior literature indicates that one driver of extra-role behavior is workplace values (Van Dyne et al. 1994). When there are shared values and goals in the workplace, and those values and goals are internalized by individual members, the likelihood that individuals spend extra effort to reach those goals is increased. This

implies that when securing the system or information is accepted by individuals and serves as a shared goal or value within the organization, in addition to performing what is specified in the policies, individuals tend to assist others to perform the desired behavior in order to ensure the system or information is secured.

H2b: Social control is positively associated with extra-role behavior.

RESEARCH METHOD

Constructs and Item Development

The measurement items of the constructs were obtained based on existing scales in extant literature; otherwise, we developed new measure closely our definition of constructs such as commitment, attachment, belief, and involvement. All constructs were measured with multiple items on five-point Likert scales. Since we collected required data in Taiwan, a translation-back translation action was performed to ensure translation quality (Brislin 1980). To ensure content validity, the survey questionnaire was reviewed by two professors and seven Ph.D. students majoring in MIS. Minor modifications were made based on the feedback to increase the quality of the items. *Commitment* was assessed with items adapted to reflect an individual's willingness to put out effort to benefit his/her organization (Meyer and Herscovitch 2001). *Involvement* was measured with items which focused on an individual's experience of participating in formal and informal activities and meetings. *Attachment* was assessed with items adapted to reflect an individual's emotional relationship with other members of the department and shared norms and values (Chiu et al. 2006; Hoegl and Gemuenden 2001). *Belief* was measured with items to measure both an individual's belief that the behavior leads to certain outcomes and his/her evaluation of these outcomes (Ajzen and Fishbein 1980). The items to measure *formal control* were adapted from Boss et al. (2009). *Specification* measured individual employees' familiarity

with organizational security policies which are clear and formalized statements. *Evaluation* focused on the assessment of an individual employee's compliance with or violation of security policies. *Reward* measured the implicit or explicit consequences of the compliance with or violation of specified behavior. The items adapted from Griffin et al (2007) were used to capture *in-role behavior* which refers to the extent to which individuals perform specified security behaviors proficiently. *Extra-role behavior* was measured with items to capture to the extent to which individuals perform altruistic behaviors not specified in security policies.

Sample and Data Collection

Based on our research purpose, individuals working in the IS department were preferred in this study. Data collection ran from April to June, 2012. A total of 259 respondents replied to the survey. Of the 259 respondents, 69% were male, and 85.3% were in the 26 to 40 age range. About 76% of respondents held specialist positions such as programmer, system analyst and database administrator. In order to detect the potential bias resulting from sampling, a comparison of the early and late respondents on all variables was conducted (Armstrong and Overton 1977). The results show no significant differences between these two groups in all constructs. Therefore, we believe that the credibility of the following analysis is not undermined by non-response bias.

DATA ANALYSES AND DISCUSSION

The SmartPLS was used to test the measurement and the structural models. The reliability of all constructs is well above 0.7 and factor loadings of each measurement item are above 0.5 as well. Through reliability testing, this questionnaire can be assumed to be reliable. The item-total correlation (ITC), composite reliability (CR), and average variance extracted (AVE) values indicate high convergent validity (Fornell and Lareker 1981). Discriminant

validity is also assured because the correlations coefficients among variables are less than 0.90 and the square root of AVE for each variable is greater than the inter-construct correlation coefficients (Fornell and Lareker 1981).

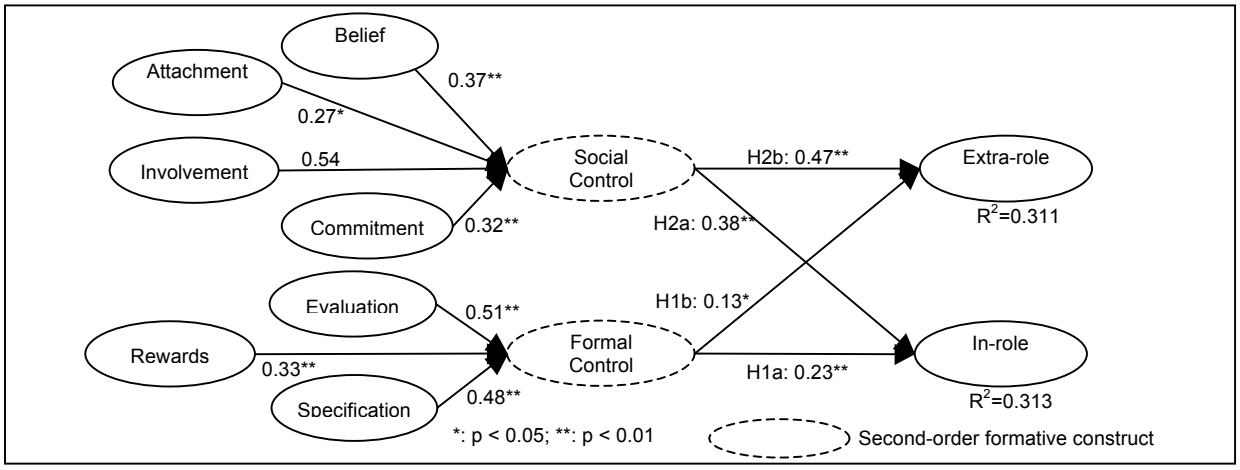

Figure 1. Structural Model and Path Coefficients

The result is shown in Figure 1. The proposed four hypotheses were all found to be supported. In addition, two types of control explain 31.1% of the variance of extra-role behaviors and 31.3% of the variance of in-role behaviors.

For information security studies, we contribute to this research area by showing the importance of extra-role behaviors to security effectiveness. Although researchers have started to pay attention to the impact of human factors on security effectiveness, past studies largely focused on reducing delinquent behavior or promoting compliant behavior (Boss et al. 2009; Herath and Rao 2009). We also contribute to control theory research by introducing social control as one type of informal control. Clan control is exercised through selecting members and socializing them into a social unit. For clan control to generate effects, shared norms and values play a critical role. However, clan control literature does not pay much attention to those parts in addition to shared norms, the receiving of rewards and avoidance of punishment. Our study fills in this gap. We successfully showed that individuals perform desired behaviors for the following

reasons: they do not want to disappoint those to whom they are attached, they internalize those norms and believe that performing those behaviors is correct, they are committed to the organization affectively and normatively, and they are involved in the consensus forming process. Lastly, this study also contributes to social control theory. Originating from criminology, social control research largely focused on its effect on reducing delinquent behaviors. In this study, we extended the scope of its application by proposing that social control (social bond) also has an effect on both in-role and extra-role behaviors.

For practitioners, the strong weight of specification implies that individuals' awareness of formal control can ensure that those individuals will actually perform the specified behaviors. Therefore, in addition to specifying expected behavior explicitly, managers should also try to make sure that employees fully understand the requests, how their behavior is evaluated, and the rewards that may be obtained from performing the specified behaviors. This can be done through effective training or education. On the other hand, for social control, involvement has the greatest weight. There are several opportunities for employees to get involved in the policy-forming or training process. For example, once the guideline for information security has been made, managers should invite employees to engage in the policy formation meeting. A bottom-up approach gives employees a better chance to understand the guideline and provide their input in forming the most suitable and doable policies. In addition, after the policies have been determined, having employees engage in the training program can also assist employees to be alert to potential security threats. Since employees are more committed to those policies, the possibility that they can perform adequate actions or assist others increases. A better result can therefore be achieved.

REFERENCES

Ajzen, I., and Fishbein, M. 1980. "Understanding Attitudes and Predicting Social Behavior," EnglewoodCliffs, NY: Prentice-Hall.

Armstrong, J., and Overton, T. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.

Bachrach, D.G., Powell, B.C., Bendoly, E., and Richey, R.G. 2006. "Organizational Citizenship Behavior and Performance Evaluations: Exploring the Impact of Task Interdependence," *Journal of Applied Psychology* (91:1), pp. 193-201.

Bedwell, W.L., Wildman, J.L., DiazGranados, D., Salazar, M., Kramer, W.S., and Salas, E. 2012. "Collaboration at Work: An Integrative Multilevel Conceptualization," *Human Resource Management Review* (22:2), pp. 128-145.

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), pp. 151-164.

Brislin, R.W. (ed.) 1980. *Translation and Content Analysis of Oral and Written Material*. Boston: Allyn & Bacon.

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), pp. 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), pp. 18-41.

Chiu, C.M., Hsu, M.H., and Wang, E.T.G. 2006. "Understanding Knowledge Sharing in Virtual Communities: An Integration of Social Capital and Social Cognitive Theories," *Decision Support Systems* (42:3), pp. 1872-1888.

Choudhury, V., and Sabherwal, R. 2003. "Portfolios of Control in Outsourced Software Development Projects," *Information Systems Research* (14:3), pp. 291-314.

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.

D'Arcy, J., and Greene, G. 2009. "The Multifaceted Nature of Security Culture and Its Influence on End User Behavior," *IFIP TC8 International Workshop on Information Systems Security Research*, Cape Town, South Africa, May 29-30, pp. 145-157.

Das, T.K., and Teng, B.S. 1998. "Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances," *Academy of Management Review* (23:3), pp. 491-512.

Eisenhardt, K.M. 1985. "Control: Organizational and Economic Approaches," *Management Science* (31:2), pp. 134-149.

Fornell, C., and Lareker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:3), pp. 39-50.

Griffin, M.A., Neal, A., and Parker, S.K. 2007. "A New Model of Work Role Performance: Positive Behavior in Uncertain and Interdependent Contexts," *Academy of Management Journal* (50:2), pp. 327-347.

Herath, T., and Rao, H. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Hirschi, T. 1969. *Causes of Delinquency*. Berkeley, CA: University of California Press.
Hoegl, M., and Gemuenden, H.G. 2001. "Teamwork Quality and the Success of Innovative Projects: A Theoretical Concept and Empirical Evidence," *Organization Science* (12:4), pp. 435-449.
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.
Irvin, R.A., and Stansbury, J. 2004. "Citizen Participation in Decision Making: Is It Worth the Effort?," *Public Administration Review* (64:1), pp. 55-65.
James, H.L. 1996. "Managing Information Systems Security: A Soft Approach," *Information Systems Conference of New Zealand*, New Zealand, Oct. 30-31, IEEE, pp. 10-20.
Kirsch, L.J. 1996. "The Management of Complex Tasks in Organizations: Controlling the Systems Development Process," *Organization Science* (7:1), pp. 1-21.
Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security* (10:2), pp. 57-63.
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), pp. 707-718.
Meyer, J.P., and Allen, N.J. 1991. "A Three-Components Conceptualization of Orgnizational Commitment," *Human Resource Management Review* (1:1), pp. 61-89.
Meyer, J.P., and Herscovitch, L. 2001. "Commitment in the Workplace: Toward a General Model," *Human Resource Management Review* (11:3), pp. 299-326.
Mowday, R.T., Steers, R.M., and Porter, L.W. 1979. "The Measurement of Organizational Commitment," *Journal of Vocational Behavior* (14:2), pp. 224-247.
Organ, D.W. 1988. *Organizational Citizenship Behavior: The Good Soldier Syndrome*. Lexington, MA: Lexington Books.
Podsakoff, P.M., MacKenzie, S.B., Paine, J.B., and Bachrach, D.G. 2000. "Organizational Citizenship Behaviors: A Critical Review of the Theoretical and Empirical Literature and Suggestions for Future Research," *Journal of Management* (26:3), pp. 513-563.
Van der Vegt, G.S., Van de Vliert, E., and Oosterhof, A. 2003. "Informational Dissimilarity and Organizational Citizenship Behavior: The Role of Intrateam Interdependence and Team Identification," *Academy of Management Journal* (46:6), pp. 715-727.
Van Dyne, L., Graham, J.W., and Dienesch, R.M. 1994. "Organizational Citizenship Behavior: Construct Redefinition, Measurement, and Validation," *Academy of Management Journal* (37:4), pp. 765-802.
Vardi, Y., and Wiener, Y. 1996. "Misbehavior in Organizations: A Motivational Framework," *Organization Science* (7:2), pp. 151-165.
Wiener, Y. 1982. "Commitment in Organizations: A Normative View," *Academy of Management Review* (7:31), pp. 418-428.
Zhang, J., Reithel, B.J., and Li, H. 2009. "Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security* (17:4), pp. 330-340.