Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness

Jack Shih-Chieh Hsu, Sheng-Pao Shih, Yu Wen Hung, Paul Benjamin Lowry

Information Systems Research
Vol. 26, No. 2, June 2015, pp. 282–300
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)
http://dx.doi.org/10.1287/isre.2015.0569
© 2015 INFORMS

The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness

Jack Shih-Chieh Hsu
Department of Information Management, National Sun Yat-sen University,
Kaohsiung 80424, Taiwan, jackshsu@mis.nsysu.edu.tw

Sheng-Pao Shih
Department of Information Management, Tamkang University,
New Taipei City 25137, Taiwan, sbao@mail.tku.edu.tw

Yu Wen Hung
Department of Information Management, National Sun Yat-sen University,
Kaohsiung 80424, Taiwan, d004020004@student.nsysu.edu.tw

Paul Benjamin Lowry
Department of Information Systems, City University of Hong Kong,
Kowloon, Hong Kong, paul.lowry.phd@gmail.com

Although most behavioral security studies focus on organizational in-role behaviors such as information security policy (ISP) compliance, the role of organizational extra-role behaviors—security behaviors that benefit organizations but are not specified in ISPs—has long been overlooked. This study examines (1) the consequences of organizational in-role and extra-role security behaviors on the effectiveness of ISPs and (2) the role of formal and social controls in enhancing in-role and extra-role security behaviors in organizations. We propose that both in-role security behaviors and extra-role security behaviors contribute to ISP effectiveness. Furthermore, based on social control theory, we hypothesize that social control can boost both in- and extra-role security behaviors. Data collected from practitioners—including information systems (IS) managers and employees at many organizations—confirmed most of our hypotheses. Survey data from IS managers substantiated the importance of extra-role behaviors in improving ISP effectiveness. Paired data, collected from managers and employees in the same organizations, indicated that formal control and social control individually and interactively enhance both in- and extra-role security behaviors. We conclude by discussing the implications of this research for academics and practitioners, along with compelling future research possibilities.

Keywords: IS security; behavioral security; in-role behaviors; extra-role behaviors; social control theory; SCT; security management; information security policy; ISP; formal control; social control; organizations
History: Radhika Santhanam, Senior Editor; Jonathon Cummings, Associate Editor. This paper was received on January 23, 2014, and was with the authors 12 months for 3 revisions. Published online in *Articles in Advance* April 24, 2015.

1. Introduction

The importance of information security and supporting information security policies (ISPs) in organizations has been emphasized extensively in recent research (e.g., Boss et al. 2009, D'Arcy and Hovav 2009, Posey et al. 2013). Recent related research has highlighted the importance of the human component in increasing ISP effectiveness—i.e., the extent to which an ISP reaches its objectives and goals concerning the security and protection of an organization's information (Knapp et al. 2007, Posey et al. 2014). Consequently, previous studies have focused on increasing users' compliance (Bulgurcu et al. 2010a) and on precautionary behaviors (Boss et al. 2009), while decreasing their computer abuse (Lee et al. 2004, Lowry et al. 2014) and access policy violations (Vance et al. 2013), to name a few examples. (Appendix A reviews the definitions of the key security-related behaviors addressed in information systems (IS) research and provides example studies that address these behaviors.) The extant research focuses primarily on in-role behaviors, defined as behaviors specified by or associated with ISPs, including performing listed and expected behaviors directly or adapting working style to align with those expectations (Katz 1964, Pahnila et al. 2007).

Our study builds on two key points of this literature. First, in addition to in-role behaviors, we explore the influence of extra-role behaviors on ISP effectiveness. Extra-role behavior refers to security behaviors not specified in an ISP and not dependent on the use of rewards or punishments to encourage performance.

The Achilles' heel of ISPs is that it is virtually impossible (and likewise quixotic) to outline and control every possible security behavior. Organizational research shows that enhanced organizational outcomes can be achieved when employees help each other perform their duties well, rather than performing only their own duties myopically (Van Dyne et al. 1994, Van Dyne and LePine 1998). This research implies that extra-role behaviors should not be neglected, because improved organizational working outcomes can be obtained when extra-role behaviors are fostered. However, the lack of systematic research into the role of extra-role behaviors in behavioral security leaves this compelling possibility unexamined. Thus, *the first purpose of our study is to clarify and examine the importance of extra-role behaviors in organizational ISP effectiveness when the effect of in-role behaviors is controlled.*

Second, the major drivers of in-role behaviors are formal control mechanisms—including specification, evaluation, reward, and punishment (Boss et al. 2009). Still, as social entities, successful organizations are unlikely to rely solely on formal control mechanisms for effective coordination (Boss et al. 2009, Kirsch et al. 2010). Employee behaviors are influenced both by specified rules and social interactions and by the social climate at work. For example, compliant behavior is partially a function of the organizational security climate (Chan et al. 2005) and social influences, such as subjective norms and attachment (Cheng et al. 2013, Herath and Rao 2009b). Although ISPs cannot account for such social factors, they can strongly influence organizational security behaviors. Behavioral security researchers therefore need to consider the elements of social interaction when investigating the drivers of security behavior, in addition to formal control mechanisms. Thus, *the second purpose of this study is to examine the impact and interaction of formal and social controls on employees' in- and extra-role behaviors.*

To achieve these goals, we propose a model based on social control theory (SCT). We collected data from IS managers and employees at many organizations. The survey data from IS managers confirmed the importance of extra-role behaviors in improving ISP effectiveness. Paired data, collected from managers and employees in the same organizations, indicate that formal control and social control have a positive influence individually and interactively on both in- and extra-role security behaviors.

2. Literature Review and Theoretical Foundation

2.1. Employees' ISP Behaviors: In- and Extra-Role Activities

Research has widely concluded that to secure information within an organization, managers should pay attention to specifying appropriate ISPs and motivating employees to follow them (Boss et al. 2009, Bulgurcu et al. 2010a, Posey et al. 2013, Wall et al. 2013). Security activities specified in ISPs are often considered *in-role behaviors*, which are required or expected organizational behaviors that are the basis of regular and ongoing job performance evaluations and are linked to rewards and punishments (Katz 1964, Welbourne et al. 1998). A recent example of these for organizational security are the protection motivation behaviors specified by Posey et al. (2013).

In addition to in-role behaviors, the importance of positive or prosocial behaviors in a collaborative working environment has been investigated (Van Dyne and LePine 1998, Williams and Anderson 1991). For example, Griffin et al. (2007) adopted the role theory developed by Katz and Kahn (1978) to describe the need to emphasize positive behaviors in the context of interdependence. In a highly interdependent context, an individual's work outcomes might be influenced by the performance of coworkers. Thus, one member's failing to perform requested behaviors could make it more difficult for the unit to achieve collective security goals (Bachrach et al. 2006). As an illustration, leaking customer data can lead to low customer satisfaction or lawsuits. Even employees not responsible for an information leak can be affected by the damage it does; workloads might increase, bad publicity could ensue, and financial performance could be reduced. This scenario indicates that an employee's organizational environment can be harmed when a breach occurs—even when that employee is not directly responsible for the breach.

Accordingly, mindful employees should be motivated to pay attention to others' behaviors in an interdependent context and thus engage in extra-role behaviors such as performing altruistic behaviors to aid others (i.e., *helping*) and speaking up with the intent to improve organizational functioning (i.e., *voicing*). *Helping* is cooperative behavior that emphasizes small acts of consideration. For example, without help from others, employees who are unfamiliar with ISPs or with how to implement them may act inappropriately. Other employees can offer assistance by providing guidance pertaining to ISPs, identifying inappropriate conduct, or helping others learn the ISPs. In the daily working environment, employees can voluntarily take actions that help to prevent security violations. *Voicing* (i.e., expressing *voice*) is another positive organizational behavior. It involves offering comments intended to improve the current state rather than merely to criticize (Roberts et al. 2006, Van Dyne and LePine 1998). Voicing is crucial in the contemporary information security context because of emerging threats and frequent changes in technologies. Security committees need new ideas from stakeholders to facilitate the continuous improvement of

ISPs. Suggestions from employees may be able to enhance the content of ISPs and address blind spots. Despite the importance of helping and voicing, such general extra-role behaviors are typically not specified in ISPs.

2.2. Control in Information Security Research

The goal of control is to motivate employees to comply with a desired behavior (Eisenhardt 1985). Whereas *formal control* focuses on specifications, evaluations, and reward/punishment, *informal control* is related to methods based on social or people-related strategies (Eisenhardt 1985, Kirsch 1996). IS studies have demonstrated that exercising and/or combining different control mechanisms can inspire IS developers to perform effectively (e.g., Kirsch 1996, 2004). A key conclusion of these studies is that effective controls encourage employees to perform desired behaviors or actions and can result in better outcomes. Similar research results are found regarding ISP compliance, computer abuse, and unethical computer behaviors (D'Arcy and Herath 2011). Most studies in this area have adopted a deterrence theory and examined how the presence of sanctions drives employees to comply with expectations. A common area of focus is on the effects of *formal sanctions*, which are explicit penalties for certain forms of misconduct (Siponen et al. 2012), in encouraging desired behaviors and discouraging undesired behaviors. However, the results of these sanctions have been mixed in IS security research, especially when other factors, such as informal sanctions, are considered (D'Arcy and Herath 2011). For example, Siponen and Vance (2010) showed that neutralization techniques used to rationalize negative behaviors were stronger than the certainty and severity of informal sanctions meant to thwart such behaviors. Guo and Yuan (2012) demonstrated that informal sanctions mediate the effects of formal sanctions on compliance intention. Posey et al. (2011) found that excessively strong formal controls can create a sense of privacy invasion and injustice that actually increases computer abuse.

Accordingly, D'Arcy and Devaraj (2012) identified two informal sanctions: social desirability pressure as a social cost and moral belief as a self-imposed cost. Based on a deterrence perspective, they further empirically demonstrated the suppressing effects of these two costs, compared with formal sanctions, on intentions to misuse technology. In terms of social costs, social influence (or a social norm) is one determinant of behavioral intention (Fishbein and Ajzen 1975). Likewise, employees tend to adopt recommended security actions in ISPs when they are motivated to comply with the expectations of important referents, such as managers (Aurigemma and Panko 2012; Herath and Rao 2009a, b; Johnston and Warkentin 2010; Peace et al. 2003).

The most common self-imposed costs include shame, moral beliefs, and commitment. Shame is considered a deterrent of negative behavior (Nagin and Paternoster 1993) in addition to formal and informal sanctions (Paternoster and Simpson 1996). Shame has been shown to inhibit the intention to commit software piracy (Siponen et al. 2012), but also to have no inhibitory effect on the intention to violate ISPs (Siponen and Vance 2010). The importance of moral beliefs or personal norms has been identified in several studies, and it applies to compliance intentions in a security context (e.g., Li et al. 2010, Siponen et al. 2012). Some studies have also shown that employees' commitment to their organizations (Herath and Rao 2009b) or to organizational security (Aurigemma and Panko 2012) improves security-related behaviors.

Although some security studies have considered informal social controls, most studies have focused only on negative or deviant behaviors, including piracy (Siponen et al. 2012), ISP violations (Siponen and Vance 2010), and misuse (D'Arcy and Devaraj 2012). Only a few have investigated the intention to adopt security recommendations (e.g., Johnston and Warkentin 2010, Lee and Larsen 2009). Fewer still have considered broader protection motivation behaviors (Posey et al. 2013). To the best of our knowledge, we are not aware of any study that has considered positive in-role and extra-role behaviors. Addressing this issue, we view an organization as a social unit and argue that SCT can provide a sound theoretical basis, from a social perspective, to account for informal controls improving IS compliance. By incorporating extra-role behaviors as dependent variables, we also contribute to SCT by extending its scope.

2.3. The Social Control (Bond) Perspective from Social Control Theory

SCT, proposed by Hirschi (1969), has been widely applied in criminology research. SCT identifies causes of social behaviors that do not conform to generally accepted social rules or norms, such as delinquent behaviors. SCT is also known as *social bond theory*, because it proposes that despite some natural inclinations toward crime, strong social bonds deter individuals from committing criminal acts. In contrast, the possibility of a person's involvement in a crime increases as his or her social bonds become weaker (Vardi and Wiener 1996). Hirschi (1969) classified the inhibitors of unwanted behaviors into four types: commitment, attachment, belief, and involvement.

First, *commitment* in SCT traditionally refers to one's identification with and dedication to one's role in society. Social control theorists view commitment from a cognitive perspective. For example, "to the person committed to conventional lines of action, risking one to 10 years in prison for a 10-dollar holdup is stupidity because to the committed person the costs and risks obviously exceed 10 dollars in value" (Hirschi 1969, p. 20). Because our context is organizational security, we naturally modified the context of commitment from one's role in society to one's role in an organization—that is, to one's organizational commitment. In other words, the more committed people are to their organizations, the more they calculate the costs of higher losses in committing delinquent behaviors within their organizations.

Second, *attachment* refers to employees' associations with others around them. Attachment is viewed as one type of internal control, based on social links. Individuals may take or avoid taking some actions when they are highly attached to others—including peers, parents, and other people they consider important. For example, attachment is negatively associated with delinquent behaviors, because performing such behaviors can disappoint those to whom the actors are attached (Hirschi 1969). In an organizational context, coworkers represent the most relevant attachment targets for employees.

Third, *belief* refers to the extent to which individuals think that performing certain behaviors is ethically correct. SCT assumes that a society has shared norms and values. When people internalize those norms or values, the individuals are motivated to perform behaviors that conform to the shared norms or to avoid conduct that violates them. For example, deviant behaviors are more likely to be observed in individuals who do not have an attitude of respect toward the rules of society (Hirschi 1969). Our study considers employees' beliefs about ISPs as a major driver of both in- and extra-role security behaviors.

Fourth, in traditional SCT contexts, *involvement* refers to the time and energy one spends on conventional societal actions. According to Hirschi (1969), because time and energy are limited for each individual, the more one spends on "regular" activities, the less one can spend on deviant activities. However, whereas previous criminology studies have focused on exploring ways to prevent delinquent behaviors, our research goals involve the drivers of in- and extra-role behaviors, which are positive organizational behaviors, not negative ones. The original assumption, therefore, does not hold well in our organizational context. Although Lee et al. (2004) define involvement as the amount of time and energy spent on conventional activities that reinforce relationships, the definition of involvement needs to be modified according to the form of behavior under investigation. We thus define *involvement* as the extent to which employees engage in the ISP-formation process and are aware of ISPs.

Outside of criminological research, only a few studies have attempted to apply SCT in a security context, although they have made promising indications regarding its applicability. For example, Lee and Lee (2002) explored the effectiveness of SCT in the context of computer crime in organizations. They proposed a combined model of SCT and general deterrence theory to investigate and address employees' misuse of IS. Ifinedo (2014) integrated SCT with the theory of planned behavior (TPB) to explore compliance intentions toward ISPs. Cheng et al. (2013) explored the impact of social bonds on ISP violation intentions. Their findings confirm the importance of social bonds in deterring potential criminal acts and encouraging ISP compliance.

In this study, we adapt SCT to our context of motivating employees to perform positive in- and extra-role behaviors. Departing from studies that used SCT to identify ways to prevent delinquency, we investigate whether social control can boost in- and extra-role behaviors. In addition, by incorporating social and formal controls into a single model and examining their effects on in- and extra-role behaviors, we can explore the influence generated by each control mechanism and the relative importance of each mechanism regarding each behavior.

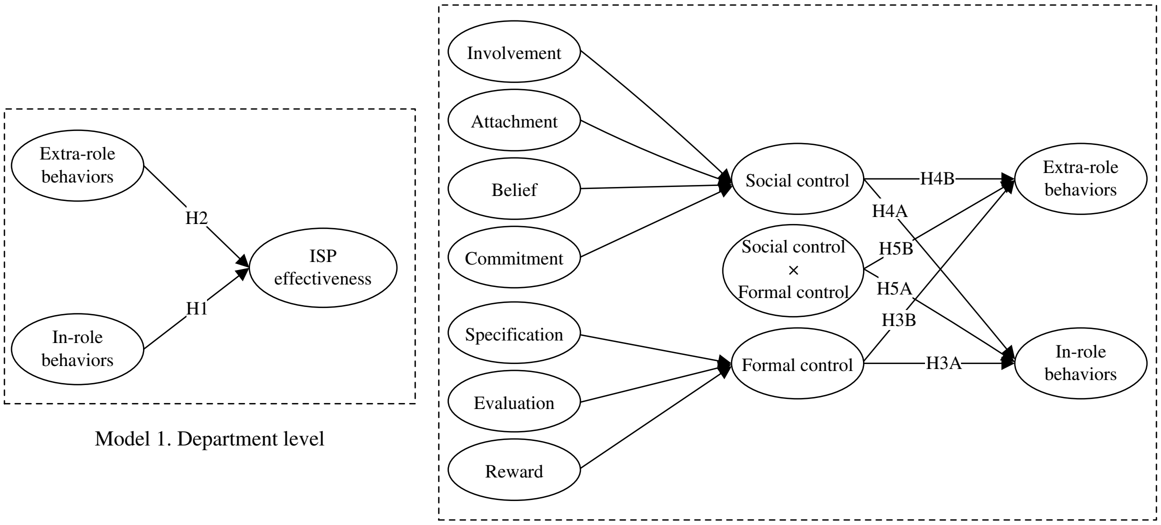
3. Research Model

As shown in Figure 1, our research model is separated into two distinct models. Model 1 aims to achieve our first goal: to discover the importance of extra-role behaviors in addition to in-role behaviors. Because ISP effectiveness is an organization-level construct, two independent constructs represent the extent to which in- and extra-role behaviors are observed in IS departments in general. The purpose of Model 2 is to examine the effects of perceived formal and social control on both extra-role and in-role behaviors; thus, this model applies to the individual level. In addition, formal control contains three subcomponents, and social control contains four. Although it is possible to consider the effects of each subcomponent on dependent variables, for the sake of theoretical parsimony, we use these two as second-order formative constructs (Law et al. 1998). Furthermore, we treat these two constructs as formative because internal consistency is not necessary for the subcomponents in each control (e.g., whereas one respondent may perceive high evaluation and high specification, another may sense high evaluation and low specification in his or her company).

3.1. Model 1: In- and Extra-Role Behaviors and ISP Effectiveness

The goal of ISPs is to improve organizational information security, and thus a surrogate of their effectiveness is the extent to which information is secured. We argue that the effectiveness of information security within an organization relies on the employees

Figure 1 Research Models (Department Level and Individual Level)



Model 1. Department level

Model 2. Individual level

who perform in-role security behaviors (Guo 2013). For example, information leakage frequently occurs when employees fail to log out after accessing their email accounts on public computers. Of course, information still might not be secured if the ISPs cannot cover all emerging threats. The likelihood that information cannot be secured is even higher when some employees fail to follow ISPs. Significant harm can be caused by careless behaviors performed by employees even when their intentions are not malicious (Guo et al. 2011). Therefore, we hypothesize the following:

Hypothesis 1 (H1). *In-role organizational security behaviors are positively associated with ISP effectiveness.*

In an information security context, the extra-role behavior of *helping* is important to ISP effectiveness, because an organization's performance is determined by the amalgamation of each employee's efforts. It is likely that some employees in any organization will fail to perform specified ISP behaviors because of low ISP awareness, poor abilities, low self-efficacy, or carelessness. Employees must therefore help each other adhere to ISPs; otherwise, the "weakest links" will undermine their organizations' security. For example, employees can enhance ISP effectiveness by introducing new employees to ISPs, reminding others to log out of a system after accessing information, and assisting those who do not know how to perform security behaviors.

Employees may also perform *voicing* behaviors, such as making innovative suggestions related to ISP content with the intention of improving information security. Effective ISPs cannot be fully developed and improved if employees do not actively make recommendations, communicate their concerns to others, or even encourage other employees to get involved. Without input from employees, ISP committees are more prone to make decisions disconnected from employees' experiences. This disconnection is a serious issue, because recent research has found a large divide between employees and security experts in understanding and addressing ISPs (Posey et al. 2014). Consequently, a lack of voice can undermine ISP effectiveness. In summary:

Hypothesis 2 (H2). *Extra-role organizational security behaviors (e.g., helping and voicing) are positively associated with ISP effectiveness.*

3.2. Model 2: Controls and Behaviors

In this study, we argue that both formal and informal (social) controls should be exercised to boost in- and extra-role behaviors. We now explain how both types of control influence in-role and extra-role behaviors.

3.2.1. Effect of Formal Control on In-Role Behaviors. One study developed a model to explain individual information security precaution-taking behavior on the basis of formal control (Boss et al. 2009). The authors hypothesized that individuals pay more attention to precautionary behavior when certain formal control mechanisms exist, including specification, evaluation, and reward. Those control mechanisms are, indeed, very similar to the formal control concept proposed by Kirsch (1996). *Specification* refers to formalized statements that articulate desired behavioral outcomes and that are typically codified as organizational policies and procedures. Specification provides employees with direction regarding the desired goal and ways to achieve it. *Evaluation* is a process of data collection and comparison to examine how well an individual's behavior or performance meets the specification. With evaluation, managers can determine the adjustments required for any deviations. *Reward* refers to the implicit or explicit consequences of violating or complying with the specified behavior. Rewards send a signal to employees that compliance with the specified behavior is desired. With specified procedures and expected outcomes, managers can determine the reward or punishment for employees, based on how well the employees' behaviors meet expectations or whether the expected outcomes are observed. Boss et al. (2009) found that specifying ISPs and evaluating behaviors are effective in convincing employees that ISPs are mandatory and thus result in compliant behaviors. Hence, we hypothesize the following:

Hypothesis 3A (H3A). *Formal control related to organizational security is positively associated with in-role organizational security behaviors.*

3.2.2. Effect of Formal Control on Extra-Role Behaviors. Although performing certain behaviors not specified in the ISP does not necessarily lead to a certain reward, we expect that formal control can still influence extra-role behaviors, because ISPs may serve as educational tools, especially regarding specification. Specification clarifies which behaviors enhance system security and which weaken it. Effective rules also specify the possible consequences of inappropriate conduct. We argue that if employees are more aware of security threats and possible consequences, they are better able to assist others to protect their computers and avoid interference with their own work (Bulgurcu et al. 2010a, D'Arcy and Hovav 2009). In this fashion, formal control also serves as an educational tool that allows employees to understand inappropriate conduct and its possible outcomes. Therefore, we hypothesize the following:

Hypothesis 3B (H3B). *Formal control related to organizational security is positively associated with extra-role organizational security behaviors.*

3.2.3. Effect of Social Control Effect on In-Role Behaviors. As noted, we adapt to our context the four mechanisms of SCT that influence social control: commitment, attachment, belief, and involvement.

Commitment. Commitment acts as a driver that pushes employees to serve organizational goals. Highly committed employees are willing to dedicate themselves to their roles, because they identify themselves as members of the organization. As an outcome, the relationship between commitment and desired action can be observed (Wiener 1982). Empirical studies have confirmed the relationship between commitment and compliance. For example, Bulgurcu et al. (2010b) showed that organizational commitment positively affects an employee's ISP compliance attitude, and Stanton et al. (2005) illustrated the importance of organizational commitment to security behavior. In sum, commitment drives employees to perform in-role behaviors, and highly committed employees believe it is important or ethically imperative to perform such organizational behaviors (Malhotra and Galletta 2005).

Attachment. According to Hirschi (1969), people who live in the same social settings often share moral beliefs. They may adhere to such values as sharing, sensitivity to the rights of others, and respect for rules. Accordingly, within social units, it is often desirable for members to perform behaviors that adhere to commonly held beliefs. Employees tend to perform desired behaviors (or be compliant) to avoid negative social consequences, such as disdain from others. When employees are strongly tied to important referents (e.g., coworkers), they are more sensitive to judgments from those referents and try not to disappoint them. Therefore, employees are less likely to violate organizational norms when they have a strong attachment to their job and the organization (Cheng et al. 2013). If employees believe their managers or peers expect them to comply with ISPs, they are more likely to undertake security actions (Herath and Rao 2009b, Pahnila et al. 2007). Hence, attachment increases compliant behaviors, and highly attached employees are more likely to engage in in-role security behaviors.

Belief. Ajzen and Fishbein (1980) developed TPB to explain an individual's intention to perform a given behavior. TPB posits that people's attitudes toward performing a given behavior are related to their *beliefs* about behavior-related consequences. TPB further postulates that behavior can be explained by behavioral beliefs, normative beliefs, and self-efficacy. In addition, empirical security-related studies have shown the positive effects of beliefs and attitudes on behavioral intentions (e.g., Pahnila et al. 2007). In a social unit in which shared norms, values, and goals are developed, internalization is a major driver of acceptable behaviors (Lee et al. 2004, O'Reilly and Chatman 1986). In sum, employees who have strong beliefs that agree with the shared norms and goals of their organizations are more likely to generate favorable attitudes toward in-role behaviors and engage in them than those with weaker beliefs.

Involvement. To explain the impact of involvement on in-role behavior, we adopt the participatory decision-making theory. This theory indicates that employees are more likely to accept a decision if they are involved in the decision-making process (Irvin and Stansbury 2004). James (1996) indicated that users are more accepting of information security measures when they are involved in the planning process and contribute to the solutions of any identified issues. Albrechtsen (2007) also found that users' active participation in an information security workshop was the key to successfully influencing their behaviors and that it helped to improve their information security knowledge and awareness. Moreover, Theoharidou et al. (2005) suggested that organizations should encourage employee participation in informal meetings and should motivate employees by involving them in all phases of security design and implementation. A study by Lee et al. (2004) showed that employee participation in informal meetings effectively reduces computer abuse. We therefore expect that employees are more willing to comply with ISPs when those employees are involved in the process of planning them.

Considering these four major forms of social control in relation to in-role behaviors, we predict the following:

Hypothesis 4A (H4A). *Social control related to organizational security (via commitment, attachment, belief, and involvement) is positively associated with in-role organizational security behaviors.*

3.2.4. Effect of Social Control on Extra-Role Behaviors.

Commitment. The relationship between commitment and organizational citizenship behavior (OCB) has been theoretically articulated by Scholl (1981) and Wiener (1982). Others argue that commitment drives employees to perform altruistic behaviors by promoting their identification with the organization (Organ and Ryan 1995). Employees with a strong commitment identify with, are involved in, and enjoy membership in the organization. They are therefore likely to exert great effort on behalf of the organization (Mowday et al. 1979). Furthermore, highly committed employees tend to believe that they are a part of an organization and are willing to perform activities outside of their normal in-role behaviors, including prosocial activities that benefit the organization (Wiener 1982). Empirical studies have also supported the benefits of positive commitment in both Western (e.g., O'Reilly and Chatman 1986) and Eastern cultures (e.g., Van Dyne and Ang 1998). We thus expect that employees with a high commitment are more likely to engage in extra-role behaviors.

Attachment. SCT posits that individuals with a strong sense of attachment to colleagues tend not to perform delinquent behaviors, to avoid disappointing or receiving criticism from colleagues. We likewise argue that attachment can lead employees to perform altruistic behaviors, outside of in-role behaviors, because such behaviors are potentially pleasing to those to whom they are attached. Because people are more sensitive to others when they are attached to them, receiving positive feedback from others is likely important. Although engaging in extra-role behaviors is not recognized by formal reward systems, employees may receive informal appreciation or recognition from supervisors or colleagues (Organ 1988). Thus, employees with a higher attachment are more likely to engage in extra-role behaviors.

Belief. Workplace values represent another driver of extra-role behavior (Van Dyne et al. 1994). When employees internalize shared workplace values and goals, the employees are more likely to help others reach the shared goals. As noted, social control takes place in societies with shared norms and values. This implies that when securing organizational systems is a goal or value shared by employees in an organization, such employees are more likely to adhere to ISPs and assist others to do so.

Involvement. Employees who are involved in policymaking processes are more eager to see the policies succeed (Irvin and Stansbury 2004). Employees have a higher level of ownership of and commitment to policy content when they help develop it (Allen and Meyer 1990). Such employees tend to devote extra effort to and take actions in support of the policies' success. Furthermore, participatory decision making generally leads to higher satisfaction (Black and Gregersen 1997, Cotton et al. 1988), and satisfaction is a major driver of citizenship behaviors such as helping. It is thus reasonable to assume that in addition to performing the behaviors specified in ISPs, employees involved in the ISP formation process will tend to support others to ensure the security of the system or information.

Considering these four major forms of social control in relation to extra-role behaviors, we predict the following:

Hypothesis 4B (H4B). *Social control related to organizational security (via commitment, attachment, belief, and involvement) is positively associated with extra-role organizational security behaviors.*

3.2.5. The Interaction Effect of Social Control and Formal Control on In-Role Behaviors.

In this section, we propose that formal control has a stronger effect on in-role behaviors when social control is also present. We expect that employees who are aware of formal control mechanisms and have a strong connection with other employees or the organization will perform more in- and extra-role behaviors. As suggested by SCT, the presence of social control increases individuals' motivation to perform in-role behaviors because they believe information should be secured, they commit to the success of ISPs, they are willing to put in effort to help the company, and the failure to perform expected behaviors may disappoint the people important to them (Hirschi 1969). Therefore, they tend to adapt to the rules and execute them more effectively. Thus, we expect more in-role behaviors when levels of both formal and social control are high, because employees are motivated to perform expected behaviors by both external drivers (e.g., rewards) and internal drivers (e.g., not disappointing others).

In addition, employees tend to perform limited in-role behaviors when either formal or social control is low. When social control is the only driving force, individuals do not know what to do (low specification), are not afraid of being caught for bad behaviors (low evaluation), and are not motivated to act (low reward). Conversely, when formal control is the only driving force, the possibility that employees will perform only minimal behaviors is high, because they are not concerned with disappointing others or compromising their relationships with them. We therefore expect that employees with either low social or low perceived formal control will perform fewer in-role behaviors compared with those who have strong social bonds and a strong sense of formal control. Thus, we hypothesize the following:

Hypothesis 5A (H5A). *The interaction between social and formal control related to organizational security is positively associated with in-role organizational security behaviors.*

3.2.6. The Interaction Effect of Social Control and Formal Control on Extra-Role Behaviors. We also argue that employees who are strongly bonded with coworkers tend to perform more extra-role behaviors when they are aware of formal control. By viewing social control as the major motivation for employees to perform specific extra-role behaviors and formal control as the procedural guideline or performance standard for performing those behaviors (Cheng et al. 2013, Lee et al. 2004), we propose that these two control mechanisms can generate a stronger effect jointly than they can independently. Extra-role behaviors are more likely when employees have a strong motivation to help others, and more helping behavior can be expected when employees know exactly how to help others.

However, we expect fewer extra-role behaviors when either perceived formal or perceived social control is low. Although employees who are strongly bonded with others are willing to perform altruistic behaviors, a lack of knowledge or behavioral criteria with respect to these behaviors reduces the possibility that employees will actually perform them. Therefore, even though extra-role behaviors can still be expected, the amount or frequency of the behaviors should be lower. Conversely, although certain extra-role behaviors can be expected when employees know exactly what to do, a lack of strong motivation limits the occurrence of such behaviors. The ideal conditions for promoting extra-role behaviors consist of a high degree of both perceived formal and social control. Therefore, we hypothesize the following:

Hypothesis 5B (H5B). *The interaction between social and formal control related to organizational security is positively associated with extra-role organizational security behaviors.*

4. Research Methods

4.1. Study Design

Given the different goals and study levels of Models 1 and 2, distinct data sets from managers and employees were used to test the models. We gathered both data sets via surveys in actual organizations in Taiwan. Because managers of IS departments are more familiar with ISP effectiveness than employees are, feedback from managers was used to examine Model 1. The constructs in Model 2 include employees' perceptions of formal control and their social bonds with the organization or other employees. Thus, for Model 2, we solicited opinions from employees in the same organizations.

4.2. Data Collection

We sent a survey package (one survey for the manager and five surveys for the IS employees) to 200 managers of IS departments in different companies in Taiwan. IS managers were asked to deliver up to five individual-level surveys to their subordinates. The survey for the managers included a series of questions pertaining to ISP effectiveness, general extra- and in-role behaviors in their departments, and extra- and in-role behaviors for each of their five selected employees. The survey for the employees included questions on their perceptions of formal control from the organization and informal control from the organization or colleagues. Of the 200 surveys for managers, 78 were completed and usable for data analysis, and of the 1,000 employee surveys, 260 were returned. Among the returned surveys from employees, 43 were deleted because they were incomplete. The final valid response rate was 39% for managers and 21.7% for employees; these rates are strong for organization-level research. Tables 1–3 provide detailed demographics for employees, managers, and organizations, respectively.

To ensure that the selected employees were representative of the larger department, we compared the managers' rated in-role and extra-role behavior scores of their departments and the scores of the employees they selected to participate in the survey. No significant difference was found (the averaged difference is 0.04 for in-role and 0.05 for extra-role behaviors), thus providing assurance of the representativeness of the selected participants.

Table 1 **Demographic Information: Employees** ($N = 217$)

Measure	Categories	No.	%
Gender	Male	138	63.6
	Female	76	35.0
	Missing	3	1.4
Age	25 and under	8	3.7
	26–30	59	27.2
	31–35	70	32.3
	36–40	49	22.6
	41 and above	28	12.9
	Missing	3	1.4
Tenure (years)	1–3	92	42.4
	4–6	49	22.6
	7–10	51	23.5
	11 and above	21	9.6
	Missing	4	1.8
Education	Doctoral	1	0.5
	Masters	73	33.6
	Bachelors and less	140	64.5
	Missing	3	1.4
Position	Programmer	140	64.5
	System analyst	14	6.5
	Network engineer	7	3.2
	Database administrator	6	2.8
	Maintenance employees	11	5.1
	Other professionals	36	16.6
	Missing	3	1.4
Department	IT	83	38.2
	Service support	14	6.5
	Systems	7	3.2
	R&D	55	25.3
	Applications	32	14.7
	Others	26	12.0
Industry type	Manufacturing	64	29.5
	IT	72	33.2
	Retailing/service	26	12.0
	Medical	14	6.5
	Finance	33	15.2
	Others	3	1.4
	Missing	5	2.3

Notes. IT, Information technology; R&D, research and development.

4.3. Ensuring Cross-Cultural Equivalence

Because the survey was conducted in Taiwan and most of the items were adopted from papers published in international English language journals, we performed several steps to ensure translation quality, per Brislin (1980), and cross-cultural equivalence, per Lowry et al. (2011). First, we collected English language items from published papers and translated them into Mandarin Chinese. To ensure content validity, the Chinese versions of the surveys were pretested by two IS researchers and two practitioners. Seven Ph.D. students were then asked to perform card sorting of all items. To increase the items' quality and validity, a few items with ambiguous terms were modified based on feedback. Finally, a translator with no connection to the study translated all of the items back into English. More importantly, the comparison between the initial and back-translated English versions of the surveys showed no significant semantic differences, suggesting translation quality and cross-cultural equivalence.

Table 2 **Demographic Information: Managers** ($N = 78$)

Measure	Categories	No.	%
Gender	Male	60	76.9
	Female	14	17.9
	Missing	4	5.1
Age	26–35	23	29.5
	36–45	42	53.8
	46 and above	11	14.1
	Missing	2	2.6
Tenure (years)	1–3	21	26.9
	4–6	23	29.5
	7–10	18	23.1
	11 and above	14	17.9
	Missing	2	2.6
Education	Doctoral	2	2.6
	Masters	53	67.9
	Bachelors and under	21	26.9
	Missing	2	2.6
Department	IT	18	23.1
	Service support	9	11.5
	Systems	5	6.4
	R&D	22	28.2
	Applications	12	15.4
	Others	12	15.5

Notes. IT, Information technology; R&D, research and development.

4.4. Constructs and Measurement

Social control includes four components. In this study, social control is considered a second-order formative construct containing four reflective constructs. *Commitment* was assessed with three items adapted from Meyer and Herscovitch (2001). Those items reflect employees' willingness to make an effort to benefit

Table 3 **Demographic Information: Organizations** ($N = 78$)

Measure	Categories	No.	%
Industry type	Manufacturing	19	24.4
	IT	32	41.0
	Retailing/service	5	6.4
	Finance	12	15.4
	Transportation	1	1.3
	Others	8	10.3
	Missing	1	1.3
Number of employees (in organization)	100 and under	23	29.5
	101–999	23	29.4
	1,000 and above	32	41.0
Number of employees (in department)	1–10	34	43.6
	11–20	16	20.5
	21 and above	27	34.6
	Missing	1	1.3
Information security management team?	Yes	50	64.1
	No	25	32.1
	Missing	3	3.8
Specialist in charge of information security?	Yes	64	82.1
	No	12	15.4
	Missing	2	2.6

Note. IT, Information technology.

their organizations. *Involvement* was measured with five items developed by the authors, but guided by SCT literature. The measures focused on capturing an individual's experience of participating in formal and informal activities and meetings (Lee et al. 2004). *Attachment* was assessed with three items adapted from Chiu et al. (2006) and Hoegl and Gemuenden (2001). Those items reflect an individual's emotional attachment to other employees in the same department. *Belief* was measured with three items adapted from Ajzen and Fishbein (1980). The items measured both the individual's beliefs that the behavior leads to certain outcomes and his or her evaluation of these outcomes.

Formal control includes three components. Twelve items (four items for each component) adopted from Boss et al. (2009) were used to assess those components. *Specification* captures how familiar employees are with ISPs that are clear and formalized statements. *Evaluation* focuses on the assessment of individual employees' ISP violation or compliance. *Reward* measures the implicit or explicit consequences of ISP violation or compliance.

Behaviors include both in- and extra-role behaviors. Six items adapted from Griffin et al. (2007) were used to capture in-role behavior, or how well employees adapt to the new security requirements and perform specified security behaviors proficiently. Another six items adapted from Van Dyne and LePine (1998) were used to measure extra-role behaviors—that is, how well employees perform altruistic behaviors not specified in ISPs and how well they voice their opinions or suggestions to benefit their work group.

Five items adapted from Knapp (2005) were used to measure *ISP effectiveness*, which refers to how well an organization's ISP supports its overall security.

4.5. Validity and Reliability

As shown in Appendix B, Table B.1, all item loadings are above 0.7, and item-total correlations (ITCs) are higher than 0.3. The composite reliability of all constructs is higher than 0.7, and the average variance extracted (AVE) values are all greater than 0.5, indicating convergent validity. Moreover, the results in Table B.2 show that the square root of the AVE is greater than all of the ITCs, indicating discriminant validity. We treated formal and social control as second-order formative constructs that contain three and four first-order constructs, respectively. This approach is appropriate, because the inclusion of these components is supported by the literature, and all weights of the first-order constructs are significant. In addition, low to moderate (not high) correlations between paired first-order variables can be observed, which implies that they should not be modeled as reflective constructs. Last, problems with collinearity are not likely, because the variance inflation factor values (between 1.0 and 1.8) are all lower than the conservative cutoff value (3.3). Also, to address the critical issue of unobserved heterogeneousness, we used the finite mixture partial least squares (FIMIX-PLS) function provided in SmartPLS to test whether the aggregate analysis is affected by heterogeneous data structures (Posey et al. 2013). The results show that our data are not influenced by the unobserved heterogeneous issue, because no significant difference was found in a two-segment analysis.

4.6. Common Method Bias and Nonresponse Bias

Because the data were self-reported, common method bias (CMB) was a potential concern in Model 1, which we address statistically in this section. First, the Harman's single-factor test was conducted. The results showed that five factors were present, and the variance explained by the first factor was 43.2% (Harman 1976). We also followed the approach recommended by Liang et al. (2007), which includes a common method factor linking to all single-indicator constructs. The results showed that most method factor loadings were not significant. In addition, the ratio of substantive variance to method variance was approximately 34:1. However, both of these approaches are limited and have their critics. We thus followed the guidelines by Pavlou et al. (2007) to conclude that CMB is highly unlikely, because the correlations between our latent constructs were moderate to low (CMB causes high correlations). CMB, therefore, should not be a serious concern for this study.

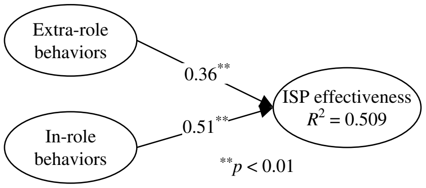
Moreover, to assess the potential for nonresponse bias, surveys returned in the first two weeks were compared with those returned in the final two weeks. The results revealed no differences between these two waves. To further detect the possibility of nonresponse bias, we followed best practices and conducted a post hoc qualitative approach suggested by Sivo et al. (2006). We contacted five managers who did not return the survey and five managers who returned the survey. However, we found no significant evidence in the differences between these groups in terms of in- and extra-role behaviors (between those who did and did not return the surveys) that would suggest nonresponse bias.

5. Analysis and Results

5.1. Hypotheses Testing

Following the latest partial least squares (PLS) standards by Lowry and Gaskin (2014), we used PLS to test the proposed hypotheses. PLS, a components-based structural equation-modeling tool, was selected for the following reasons. First, the goal of this study was to incorporate theories to explore the impacts

Figure 2 **Results of Model 1**

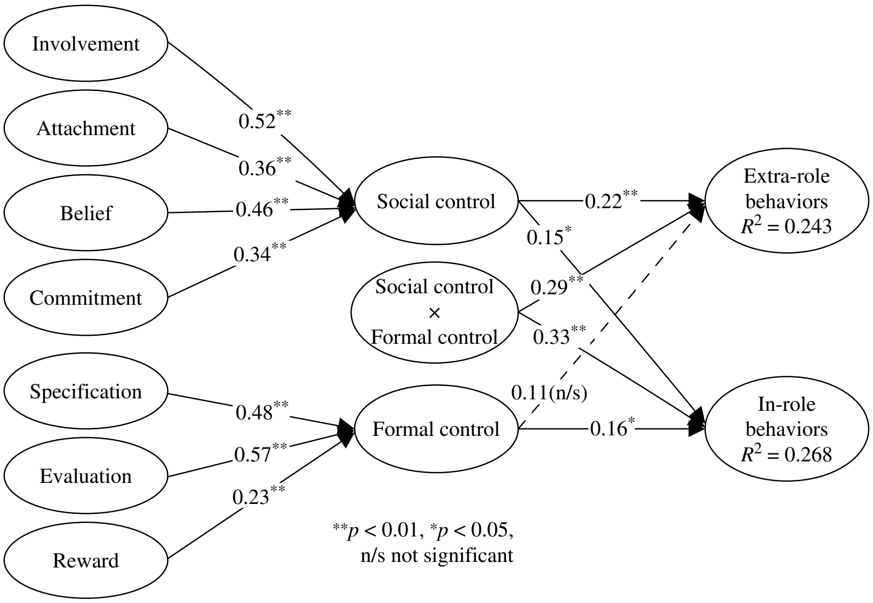


of different control mechanisms on both in- and extra-role behaviors, and PLS is considered appropriate for such an extension of existing structural theories, because this tool is useful for theory construction rather than confirmation (Hair et al. 2011, Lowry and Gaskin 2014). In contrast, covariance-based methods are more appropriate for testing established theories and consequently providing fit statistics, which do not apply with PLS (Lowry and Gaskin 2014). Second, we operationalized controls as formative second-order constructs. Even though formative constructs theoretically can be realized in covariance-based structural equation modeling (SEM), such an application is complex, limited, and rarely conducted, because covariance-based SEM usually cannot process the large matrices needed to realize these formative constructs (Diamantopoulos 2011, Hair et al. 2011). Specifically, we used SmartPLS 2.0 (Ringle et al. 2005) with bootstrapping as a resampling technique (500 random samples) to test the structural model and the significance levels of the paths. Path coefficients, their significance levels, and the R^2 values were used jointly to evaluate the model. In addition, to generate the interaction terms for Model 2, we followed the standardized product indicator approach suggested by Chin et al. (2003), which has been broadly adopted by previous studies (e.g., Tiwana and Keil 2009) and is built directly into SmartPLS.

Model 1 tests the effect of extra-role and in-role behaviors on ISP effectiveness. As shown in Figure 2, both extra-role ($\beta = 0.36$; $t = 2.81$) and in-role ($\beta = 0.51$; $t = 3.59$) behaviors positively affect ISP effectiveness. These results indicate that ISP effectiveness is high when employees perform activities specified in ISPs or help others perform those activities. In addition, in-role behavior is likely more helpful in our context, because the coefficient is higher. Last, these two behaviors explain almost 51% of the variance of ISP effectiveness.

Model 2 examines the effects of formal and social control on in- and extra-role behaviors, as shown in Figure 3. We operationalized social control and formal control as second-order formative constructs. Based on our hypotheses, we tested the individual and joint impacts of extra-role and in-role behaviors. Formal control was found to affect in-role behavior ($\beta = 0.16$; $t = 2.34$) but not extra-role behavior ($\beta = 0.11$; $t = 1.62$). Social control was positively associated with both in-role ($\beta = 0.15$; $t = 2.29$) and extra-role ($\beta = 0.22$; $t = 2.93$) behaviors. Hence, with the exception of H3B, all proposed hypotheses were supported. Furthermore, the combined variance explained by social and formal control was 24.3% for extra-role behavior and 26.8% for in-role behavior. In addition, the interaction term (social control × formal control) had a significant positive influence on extra-role behavior ($\beta = 0.29$, $t = 4.71$) and in-role behavior ($\beta = 0.33$, $t = 5.26$). Thus, H5A and H5B are fully supported.

Figure 3 **Results of Model 2**



5.2. Summary of Results

For Model 1, both in-role (H1) and extra-role (H2A) security behaviors were found to improve ISP effectiveness. The variance of effectiveness explained by the two types of behaviors indicates that these behaviors have strong predictive capabilities. For Model 2, with the exception of the link from formal control to extra-role organizational security behaviors (H3B), the direct effects from formal control to in-role organizational security behaviors (H3A) and from social control to in-role (H4A) and extra-role (H4B) organizational security behaviors, as well as the interaction effects (H5A and H5B), were supported.

6. Discussion

In this study, we examined the importance of organizational in-role and extra-role security behaviors on the effectiveness of ISPs and examined the impact of formal control and social control on both types of security behaviors. The results confirmed our expectation that in addition to in-role behaviors, extra-role behaviors play a critical role—although in-role behaviors have a relatively stronger effect. For the drivers of behaviors, we further compared the weights of each first-order construct to understand its contribution toward the overall construct. For formal control, the weights of evaluation (0.57) and specification (0.48) were more than double that of rewards (0.23). This result aligns with that of Boss et al. (2009), who showed that rewards have a limited effect on the degree to which an ISP is perceived to be mandatory. For social control, the strong weight of involvement (0.52) represents its critical role in forming the second-order construct, compared with the other three components (0.46 for belief, 0.36 for attachment, and 0.34 for commitment). This result highlights the importance of employee involvement in ISP formation, especially because involvement is the most critical component of social control within an organization. Moreover, the weight of belief was slightly stronger than those of attachment and commitment. This pattern also aligns with past studies. For example, Lee et al. (2004) found that, followed by norms and belief, involvement is better at reducing the intention to abuse a computer.

Another interesting finding is the level of impact exerted by different control mechanisms on each type of behavior. For in-role behavior, the effects of both types of control were significant, and the levels of effect were similar. The result indicates that both types of control mechanisms likely generate equal effect sizes with respect to in-role behavior. The positive coefficient of the interaction term further suggests that better effects can be achieved when both types of control are present; that is, they have a positive multiplying effect when they appear together.

For extra-role behavior, contrary to our expectations, we discovered that formal control has a limited effect. We had argued that outcome interdependence drives employees to perform extra-role behaviors and that formal control can be viewed as an educational tool that allows employees to learn what behaviors may be performed to enhance information security. Yet formal control was found to affect extra-role behavior positively and significantly when social control and the interaction between the two control mechanisms were not included. However, the effect of formal control on extra-role behaviors became insignificant when the social control mechanism was included.

To explain this finding, we argue that knowing what security actions should be performed may boost extra-role behaviors in an interdependent contemporary work environment. However, the insignificant direct effects of formal controls imply that formal control is not as crucial as social control in inspiring extra-role behaviors. More extra-role behaviors can be expected when employees are attached to their coworkers, are involved in IS creation activities, share security beliefs, and are highly committed to their organizations. Although employees driven by formal control might perform extra-role behaviors, the scope of their behavior is more likely to be limited to interdependent tasks.

6.1. Contributions to Research and Theory

Although researchers have begun to investigate the impact of human factors on ISP effectiveness, studies have largely focused on reducing misuse behavior or promoting compliance with formal policies. Extra-role behaviors have been largely overlooked. We contribute to behavioral security research by showing the importance of extra-role behaviors to ISP effectiveness, in addition to the importance of in-role behaviors. Although the influence of extra-role behaviors was slightly lower than that of in-role behaviors in our study, they are nonetheless crucial for improving organizational ISP effectiveness.

We contribute not only to the information security research stream but also to control theory research by introducing social control as a compelling form of informal control. We suggest that social control, through SCT, can be used to extend or complement the concepts of informal control. For example, intrinsic motivation and shared norms and values play a critical role in informal control. Individuals who are self-regulated or driven by social pressure from others in the same group tend to perform desired behaviors to receive rewards or avoid punishment. However, past control literature has not paid much attention to processes other than the fostering of self-regulation, formation of shared norms, receiving of rewards, and avoidance of punishment. Although SCT emphasizes the importance of shared norms, values, and goals, it also emphasizes the need to take other factors—attachment, commitment, belief, and involvement—

into consideration. According to SCT, individuals perform desired behaviors because (1) they do not want to disappoint those to whom they are attached (i.e., attachment), (2) they pledge themselves to their roles within an organization (i.e., commitment), (3) they internalize organizational norms and believe that performing those behaviors is correct (i.e., belief), and (4) they are involved in the consensus-forming process (i.e., involvement).

This study also contributes to SCT. Originating from criminology, SCT research has focused largely on how social bonds reduce delinquent behaviors. Past studies have maintained that individuals tend to avoid performing delinquent behaviors when they are strongly bonded with their environment. We extended the scope and applicability of SCT by proposing that social control (i.e., social bonds) increases positive behaviors, such as in-role and extra-role behaviors. We demonstrate that social bonds can also drive individuals to perform specified and desired behaviors, because individuals want to perform such behaviors to avoid disappointing others. We also show that social bonds lead employees to perform altruistic behaviors. Extra-role behaviors represent activities in which employees help others to perform their duties well and in which they voice ideas and strategies for the organization. We showed that employees tend to perform extra-role behaviors when they are strongly connected with others.

Finally, this study also contributes to research on extra-role behaviors. We illustrated that social control is a critical antecedent of employees' extra-role behaviors. Previous studies have classified personal characteristic-related antecedents of extra-role behaviors into different types, such as attitude, dispositional variables, role perception, demographic variables, and ability. Although some components of social control have been identified in the literature (e.g., commitment), this is the first study to view control as an important antecedent of extra-role or citizenship behaviors. Furthermore, the positive coefficient of the interaction effect of formal and informal control on extra-role behavior suggests that although formal control itself has a limited effect on promoting extra-role behavior, social control can generate a greater effect when formal control is present—creating a powerful interaction effect.

6.2. Contributions to and Implications for Practice

Again, the "weakest link" in a department or organization can harm all employees. This study has interesting implications for practitioners seeking to improve the security of organizations by addressing "weak links." First, as shown in Model 1, both in- and extra-role behaviors are crucial to ISP effectiveness. This result implies that at the departmental level, managers cannot focus only on encouraging in-role behaviors of ISP compliance; they must also encourage employees to perform extra-role behaviors related to security. Encouraging extra-role behaviors is crucial to addressing organizational "weak links," regardless of whether such employees are acting carelessly, maliciously, unobservantly, without self-efficacy, or simply without knowledge of ISPs. Performing extra-role behaviors can help employees monitor and report bad behavior and/or help less capable employees work more effectively.

The results of Model 2 indicate some ways to promote desired behaviors in individuals. Formal control and social control were shown to be equally important for driving employees to perform in-role behaviors. However, social control was more important in driving extra-role behavior. To improve formal control, in addition to specifying the expected behavior explicitly, managers should ensure that employees fully understand what behaviors are expected, how their behaviors will be evaluated, and what rewards they may be granted by performing these behaviors. This knowledge can be shared through effective security, education, training, and awareness (SETA) initiatives. Because threats from the Internet are continually evolving, training and policies must be continually adapted and delivered on a regular basis. To enhance employee awareness, managers can also post ISP-related practices in places easily accessible to employees or even provide system modifications with job-aware reminders for specific organizational activities in certain job functions (e.g., audits, quarterly statements, field sales, warehouse control). In addition, organizations should make greater efforts to evaluate and reward desired security behaviors as part of periodic raise and performance reviews. Nevertheless, these efforts alone will fail to secure organizations fully from internal threats. Social control is pivotal.

To improve social control, given the importance of altruistic behavior to ISP effectiveness, organizations should promote extra-role behavior by building social bonds among employees and by encouraging managers to lead by example. Our model and results suggest that antisocial employees who lack a connection to others in an organization may be inherent security risks. Managers must act as leaders who enhance employees' psychological attachment to their colleagues and the organization, increase their commitment to the organization, strengthen their beliefs regarding in- and extra-role behaviors, and allow them to participate in (even lead) the ISP-formation process. Formal or informal mechanisms can be provided to enhance interaction among employees. Frequent interaction is the basis for forming interpersonal rapport and psychological attachment. Managers should pay attention to employees with low commitment, because those employees are less likely to perform their jobs well and are relatively unwilling to help others. Managers should also pay attention to the employee recruiting process to select employees who enjoy working with others. Soft skills and leadership may be the crucial missing links to many insider security issues. Hence, efforts such as company picnics, 360-degree feedback, department lunches, work retreats, anonymous feedback mechanisms, celebrating success, recognizing outstanding employees, team-building exercises, job rotation, open-door policies, and even after-hours trips to the local bar might not only increase employee morale but also help build a hard-to-penetrate "social firewall" that improves insider security behaviors.

Moreover, of the four first-order constructs, involvement has the highest weight and might be the easiest to implement. Managers can capitalize on several opportunities to involve employees in ISP formation and training. For example, after the guidelines for information security have been established, managers can invite employees to make recommendations at an ISP-formation meeting. A bottom-up approach gives employees a better chance to understand the guidelines and provide their input into forming the most suitable and achievable ISPs. Our research thus calls into question the common practice of using security experts as the primary source of ISPs, especially because there are serious perceptual gaps between these experts and employees (e.g., Posey et al. 2014). Moreover, after ISPs have been determined, engaging employees in SETA-based training programs can improve their awareness of potential security threats. Because employees are more committed to ISPs they helped write and implement, they are more likely to perform adequate actions or assist others. Employees could also help run SETA-based training programs on a rotating basis.

Last, the findings from our investigations on what contributes to ISP effectiveness indicate that managerial attention is required to motivate employees to pay greater attention to in-role behaviors while not ignoring extra-role behaviors. In addition, the coefficients of in-role (0.51) and extra-role (0.36) behavior imply that managers should pay more attention to in-role behaviors. We believe attention is especially necessary when employees are not strongly bonded with each other or when ISPs are well known and understood. Extra-role behaviors are driven mainly by social bonds and therefore are difficult to observe when employees are not strongly bonded with their organizations or coworkers. Because in-role behavior is a function of both types of control, ISP effectiveness has to rely on in-role behaviors driven by formal control. When employees are familiar with the ISPs, they better know what to do and are therefore more likely to perform in-role behaviors. In this condition, ISP effectiveness may rely on in-role behaviors driven by formal control.

By contrast, extra-role behaviors may be emphasized when an ISP is not clearly written, is newly introduced, or is unfamiliar to employees. In-role behavior driven by formal control is less likely when ISPs are not clearly written or are "above and beyond" employees' job requirements. As indicated in Figure 3, the weights of the first-order formative components indicate that specification and evaluation have higher contributions, which further indicates that formal control is low in the absence of a clear ISP specification or evaluating approach. Under these circumstances, ISP effectiveness can rely only on the force of social control to drive employees to perform required actions and help others to do so.

6.3. Limitations and Future Research

Several limitations of this study point to exciting research possibilities. First, although we collected data from both managers and employees to avoid CMB and to improve generalizability, the data are cross-sectional. It is quite likely, however, that performing extra-role behaviors enhances social bonds; longitudinal data are required to explore this type of recursive relationship.

Second, we used a subjective evaluation of ISP effectiveness. Objective data, such as the number of actual ISP violations, would be useful to verify and build on our findings. These kinds of data are particularly challenging to gather in organizational settings, however, because organizations generally do not want to disclose ISP violations. Overcoming this barrier would be a meaningful breakthrough.

Third, some of the extra-role behaviors proposed by researchers are not easily measured (Van Dyne and LePine 1998). In this study, only helping and voicing (i.e., providing suggestions or opinions) behaviors were included. It would thus be beneficial for future research to explore the effects of other types of extra-role behaviors, such as championship, sportsmanship, initiative, and civic virtues. Furthermore, it was suggested recently that the distinction between in- and extra-role behaviors is contingent and that altruistic behaviors may be considered in-role behaviors in certain contexts (Vey and Campbell 2004). For example, helping others may result in intangible or tangible rewards in some companies with 360-degree evaluations. Executives would also be expected to engage in many extra-role behaviors because they should lead by example. Careful considerations should be made before applying our results to organizations that consider helping an in-role behavior.

Finally, this study focuses only on IS employees because we believed they were more likely to encounter and understand various information security threats than employees in other departments. Moreover, our data were gathered in Taiwan, which is considered a strongly collectivistic society compared to the United States, which is considered strongly individualistic. Taiwan is also much stronger in terms of uncertainty avoidance. Individual- and national-level differences between Chinese and American cultures have been found in technology-based decision making (Zhang et al. 2007), trust formation (Lowry et al. 2010), privacy evaluations (Lowry et al. 2011), and even in the propensity toward computer abuse (Lowry et al. 2014). A given culture contains specific social norms that apply differently from those in other cultures (Lowry et al. 2011). Consequently, it is possible that SCT applies differently to IS security compliance in Chinese, American, and cross-cultural organizational cultures (e.g., multinational firms in Hong Kong, New York, and London). Organizations themselves also have distinct cultures that give rise to unique sets of accepted norms (e.g., employees at Walmart have different organizational norms than those at HSBC). Therefore, particular care should be taken when generalizing our results to a new cultural or organizational context. We encourage researchers to collect data from employees in departments outside of IS and from companies outside of Taiwan to build on our results cross-culturally.

7. Conclusion

We examine the influence of in-role and extra-role security behaviors on ISP effectiveness and, based on social control theory, explore the role of formal and social controls in enhancing these behaviors. Data collected from 78 IS managers demonstrate the importance of both in-role and extra-role behaviors in improving ISP effectiveness, and paired data collected from managers and 217 employees in the same organizations indicate that formal control and social control individually and interactively enhance both in- and extra-role security behaviors. The findings suggest that managers should encourage extra-role security behaviors to improve security and enhance employees' connections with their organizations.

Acknowledgments

The authors are grateful to the senior editor, associate editor, and anonymous reviewers for their constructive comments on this paper. This paper was supported by the Ministry of Science and Technology (Taiwan) under project number [NSC 101-2410-H-032-014] and partially supported by the Aim for the Top University Plan of the National Sun Yat-sen University and Ministry of Education of Taiwan. The second author serves as the corresponding author.

Appendix A. Key Security-Related Behaviors from IS Research

Behaviors	Definitions	References
Access policy violation behaviors	Occur when employees access sensitive information in a way that is contrary to the policies of their organizations	Vance et al. (2013)
Compliant behaviors	Employees protect the information and technology resources from potential security breaches and follow the ISP of the organization	Bulgurcu et al. (2010a), Herath and Rao (2009b)
Computer abuse	"The unauthorized and deliberate misuse of assets of the local organization information system by individuals" (p. 257)	Straub (1990)
Delinquent behaviors	Intentional and deliberate use of information, such as stealing, revealing, and selling confidential information to outsiders	Siponen and Vance (2010)
Misuse behaviors	Intentional misuse of IS resources including behaviors that are unethical or inappropriate (e.g., personal use of company email account) and those that are illegal (e.g., accessing confidential company information)	D'Arcy et al. (2009)
Noncompliant behaviors	Employees knowingly and intentionally violate ISPs of their organizations, regardless of the behavior and the reason	Lowry and Moody (2014)
Precaution behaviors	Individuals take proactive measures or actions to secure their computers and deal with information security in accordance with prescribed corporate ISPs	Boss et al. (2009)
Protection-motivated behaviors	"Volitional behaviors enacted by organization insiders to protect (1) organizationally relevant information and (2) the computer-based information systems in which the information is stored, collected, disseminated, and/or manipulated from information security threat" (p. 1189)	Posey et al. (2013)
Reactance behaviors	Employees knowingly and intentionally violate ISPs of their organizations—and even do the opposite of what is required—in response to perceived organizational injustice or threats to their individual sense of freedom	Lowry and Moody (2014), Posey et al. (2011)
Unethical behaviors	Refers to misuse or the inappropriate use of IS, such as illegal copying of software and data or recklessly posting confidential data onto unsecured servers or websites	Banerjee et al. (1998), Leonard and Cronan (2001)

Appendix B. Measurement Items, Validity Support, and Reliability Support

Table B.1 Measurement Validity and Reliability

Constructs	Item	Loading	ITC
	Extra-role behaviors: By manager, on the department level "*Employees of this department…*"		
Extra-role behaviors—Department ($\alpha = 0.92$; CR = 0.94; AVE = 0.71)	…volunteer to do security policy-related behaviors for the work group.	0.86	0.78
	…help each other in the group learn about the security policies.	0.75	0.64
	…help orient new employees to the security policies in this group.	0.70	0.55
	…develop and make recommendations concerning information security policies that affect the organization.	0.83	0.74
	…speak up and encourage others in the organization to get involved in information security policies that affect the organization.	0.82	0.73
	…speak up in the organization with ideas for new strategies or changes in information security policies.	0.81	0.74
	In-role behaviors: By manager, on the department level "*Employees of this department…*"		
In-role behaviors—Department ($\alpha = 0.86$; CR = 0.80; AVE = 0.51)	…always adapt well to changes in core security requirements.	0.70	0.69
	…always cope with security requirement changes to the way they have to do the core tasks.	0.66	0.67
	…always learn new skills to adapt to changes resulting from security requirement changes.	0.75	0.71
	…always carry out the core parts of security requirements well.	0.82	0.59
	…usually complete core security requirements well using the standard procedures.	0.82	0.54
	…ensure core security requirements are completed properly.	0.83	0.66
	ISP effectiveness: By manager, in department		
ISP effectiveness ($\alpha = 0.86$; CR = 0.89; AVE = 0.72)	The information security policy achieves most of its goals.	0.81	0.70
	The information security policy accomplishes its most important objectives.	0.85	0.75
	Generally speaking, information in the organization is sufficiently protected.	0.87	0.79
	Overall, the information security policy is effective.	0.86	0.79
	The information security program (policy) has kept security losses to a minimum.	0.84	0.75
	Extra-role behaviors of individual employees: By manager, on the individual level		
Extra-role behaviors—Employee ($\alpha = 0.88$; CR = 0.91; AVE = 0.64)	(*Name of employee*) volunteers to do "security policies"-related behaviors for the work group.	0.78	0.75
	___ helps others in the work group learn about the work related to security policies.	0.82	0.71
	___ helps orient new employees in this work group to the security policies.	0.79	0.60
	___ develops and makes recommendations concerning information security policies that affect the work group or organization.	0.88	0.76
	___ speaks up and encourages others in the work group to get involved in information security policies that affect the work group or organization.	0.87	0.78
	___ speaks up in the work group (or organization) with ideas for new strategies or changes in information security policies.	0.89	0.75
	In-role behaviors of individual employees: By manager, on the individual level		
In-role behaviors—Employee ($\alpha = 0.86$; CR = 0.89; AVE = 0.59)	(*Name of employee*) always adapts well to changes in core security requirements.	0.89	0.66
	___ always copes with security requirement changes to the way he/she has to do the core tasks.	0.82	0.71
	___ always learns new skills to adapt to changes resulting from security requirement changes.	0.79	0.70
	___ always carries out the core parts of security requirements well.	0.86	0.70
	___ usually completes core security requirements well using the standard procedures.	0.84	0.71
	___ ensures core security requirements are completed properly.	0.83	0.75
	Social control: By employee, on the individual level		
Belief ($\alpha = 0.90$; CR = 0.93; AVE = 0.83)	Following IS security policies is one of my beliefs.	0.89	0.76
	Following IS security policies is what I should do.	0.93	0.84
	Following IS security policies is the right thing to do.	0.90	0.77
Attachment ($\alpha = 0.92$; CR = 0.95; AVE = 0.86)	At work, I depend on my colleagues.	0.89	0.80
	At work, I am very close to my colleagues.	0.96	0.90
	At work, I am attached to my colleagues completely.	0.93	0.83
Involvement ($\alpha = 0.92$; CR = 0.94; AVE = 0.76)	I often attend meetings related to organizational security regulations.	0.88	0.80
	I am involved in organizational security activities.	0.88	0.81
	I am involved in organizational security decisions.	0.83	0.75
	I often participate in organizational security training-related activities.	0.89	0.81
	I attend many organizational security training courses.	0.88	0.81
Commitment ($\alpha = 0.86$; CR = 0.92; AVE = 0.78)	Overall, I am willing to put effort into this organization.	0.87	0.71
	Overall, I am willing to put effort into my work.	0.91	0.79
	Overall, I am willing to put effort into making the organization better.	0.87	0.70

Table B.1 (Continued)

Constructs	Item	Loading	ITC
	Formal control: By employee, on the individual level		
Specification ($\alpha = 0.90$; CR = 0.93; AVE = 0.77)	I am familiar with the organization's IT security policies, procedures, and guidelines.	0.88	0.77
	I am required to know a lot of existing written procedures and general practices to secure my computer system.	0.82	0.69
	There are written rules regarding security policies and procedures at the organization.	0.89	0.79
	The organization's existing policies and guidelines cover how to protect my computer system.	0.91	0.83
Evaluation ($\alpha = 0.96$; CR = 0.97; AVE = 0.88)	Managers in my department frequently evaluate my security behaviors.	0.93	0.88
	Managers regularly examine data relating to how well I follow security policies and procedures.	0.92	0.87
	Managers formally evaluate me and my colleagues regarding compliance with security policies.	0.95	0.92
	Managers assess whether or not I follow organizational security procedures and guidelines.	0.95	0.91
Reward ($\alpha = 0.96$; CR = 0.97; AVE = 0.90)	My pay raises and/or promotions depend on whether I follow documented security policies and procedures.	0.94	0.91
	I will receive a personal mention in oral or written reports if I comply with security policies and procedures at this organization.	0.93	0.86
	I will be given monetary or nonmonetary rewards for following security policies and procedures.	0.97	0.94
	Tangible rewards are tied to whether I follow the organization's IT security policies, procedures, and guidelines.	0.95	0.92

Notes. CR, Composite reliability; IT, information technology.

Table B.2 Measurement Model Statistics

Latent construct	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12
(1) *Belief*	4.14	0.52	**0.911**											
(2) *Involvement*	2.57	0.83	0.125	**0.872**										
(3) *Commitment*	4.00	0.45	0.261	0.219	**0.883**									
(4) *Attachment*	3.56	0.64	0.119	0.077	0.351	**0.927**								
(5) *Evaluation*	3.22	0.79	0.318	0.434	0.185	0.207	**0.938**							
(6) *Reward*	2.27	0.78	0.036	0.285	0.130	0.008	0.344	**0.949**						
(7) *Specification*	3.54	0.68	0.341	0.489	0.287	0.211	0.529	0.063	**0.877**					
(8) *Extra-role behaviors*	3.16	0.85	0.137	0.405	0.115	0.174	0.400	0.040	0.263	**0.800**				
(9) *In-role behaviors*	3.80	0.76	0.183	0.330	0.065	0.060	0.431	0.075	0.357	0.536	**0.768**			
(10) *Extra-role behaviors* (higher level)	3.21	0.88	—	—	—	—	—	—	—	—	—	**0.843**		
(11) *In-role behaviors* (higher level)	3.84	0.69	—	—	—	—	—	—	—	—	—	0.507	**0.714**	
(12) *ISP effectiveness* (higher level)	3.87	0.75	—	—	—	—	—	—	—	—	—	0.501	0.780	**0.849**

Notes. The diagonal (bold) line represents the square root of AVE. SD, standard deviation.

References

Ajzen I, Fishbein M (1980) *Understanding Attitudes and Predicting Social Behavior* (Prentice-Hall, Englewood Cliffs, NJ).

Albrechtsen E (2007) A qualitative study of users' view on information security. *Comput. Security* 26(4):276–289.

Allen NJ, Meyer JP (1990) The measurement and antecedents of affective, continuance and normative commitment to the organization. *J. Occupational Psych.* 63(1):1–18.

Aurigemma S, Panko R (2012) A composite framework for behavioral compliance with information security policies. Sprague RH Jr, ed. *Proc. 45th Hawaii Internat. Conf. Systems Sci.* (IEEE, Los Alamitos, CA), 3248–3257.

Bachrach DG, Powell BC, Collins BJ, Richey RG (2006) Effects of task interdependence on the relationship between helping behavior and group performance. *J. Appl. Psych.* 91(6): 1396–1405.

Banerjee D, Cronan TP, Jones TW (1998) Modeling IT ethics: A study in situational ethics. *MIS Quart.* 22(1):31–60.

Black JS, Gregersen HB (1997) Participative decision-making: An integration of multiple dimensions. *Human Relations* 50(7): 859–878.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *Eur. J. Inform. Systems* 18(2):151–164.

Brislin RW (1980) Translation and content analysis of oral and written material. Triandis HC, Berry JW, eds. *Handbook of Cross-Cultural Psychology* (Allyn & Bacon, Boston), 389–444.

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

Bulgurcu B, Cavusoglu H, Benbasat I (2010b) The role of information security policy fairness and organizational commitment in managing information security. *5th Pre-ICIS AIS SIGSEC Workshop Inform. Security and Privacy* (AIS, Atlanta).

Chan M, Woon I, Kankanhalli A (2005) Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *J. Inform. Privacy Security* 1(3):18–41.

Cheng L, Li Y, Li W, Holm E, Zhai Q (2013) Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Comput. Security* 39(B):447–459.

Chin WW, Marcolin BL, Newsted PR (2003) A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inform. Systems Res.* 14(2):189–218.

Chiu CM, Hsu MH, Wang ETG (2006) Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems* 42(3):1872–1888.

Cotton JL, Vollrath DA, Froggatt KL, Lengnick-Hall ML, Jennings KR (1988) Employee participation: Diverse forms and different outcomes. *Acad. Management Rev.* 13(1):8–22.

D'Arcy J, Devaraj S (2012) Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sci.* 43(6):1091–1124.

D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *Eur. J. Inform. Systems* 20(6):643–658.

D'Arcy J, Hovav A (2009) Does one size fit all? Examining the differential effects of IS security countermeasures. *J. Bus. Ethics* 89(1):59–71.

D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inform. Systems Res.* 20(1):79–98.

Diamantopoulos A (2011) Incorporating formative measures into covariance-based structural equation models. *MIS Quart.* 35(2):335–358.

Eisenhardt KM (1985) Control: Organizational and economic approaches. *Management Sci.* 31(2):134–149.

Fishbein M, Ajzen I (1975) *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research* (Addison-Wesley, Reading, MA).

Griffin MA, Neal A, Parker SK (2007) A new model of work role performance: Positive behavior in uncertain and interdependent contexts. *Acad. Management J.* 50(2):327–347.

Guo KH (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. *Comput. Security* 32(1):242–251.

Guo KH, Yuan Y (2012) The effects of multilevel sanctions on information security violations: A mediating model. *Inform. Management* 49(6):320–326.

Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *J. Management Inform. Systems* 28(2): 203–236.

Hair JF, Ringle CM, Sarstedt M (2011) PLS-SEM: Indeed a silver bullet. *J. Marketing Theory Practice* 19(2):139–152.

Harman HH (1976) *Modern Factor Analysis* (University of Chicago Press, Chicago).

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

Herath T, Rao HR (2009b) Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inform. Systems* 18(2):106–125.

Hirschi T (1969) *Causes of Delinquency* (University of California Press, Berkeley, CA).

Hoegl M, Gemuenden HG (2001) Teamwork quality and the success of innovative projects: A theoretical concept and empirical evidence. *Organ. Sci.* 12(4):435–449.

Ifinedo P (2014) Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inform. Management* 51(1):69–79.

Irvin RA, Stansbury J (2004) Citizen participation in decision making: Is it worth the effort? *Public Admin. Rev.* 64(1):55–65.

James HL (1996) Managing information systems security: A soft approach. Sipple RS, ed. *Proc. Inform. Systems Conf. New Zealand* (IEEE, Los Alamitos, CA), 10–20.

Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quart.* 34(3): 549–566.

Katz D (1964) The motivational basis of organizational behavior. *Behav. Sci.* 9(2):131–146.

Katz D, Kahn RL (1978) *The Social Psychology of Organizations* (Wiley, New York).

Kirsch LJ (1996) The management of complex tasks in organizations: Controlling the systems development process. *Organ. Sci.* 7(1):1–21.

Kirsch LJ (2004) Deploying common systems globally: The dynamics of control. *Inform. Systems Res.* 15(4):374–395.

Kirsch LJ, Ko DG, Haney MH (2010) Investigating the antecedents of team-based clan control: Adding social capital as a predictor. *Organ. Sci.* 21(2):469–489.

Knapp KJ (2005) A model of managerial effectiveness in information security: From grounded theory to empirical test. Unpublished doctoral dissertation, Department of Management, Auburn University, Auburn, AL.

Knapp KJ, Marshall TE, Rainer RK Jr, Ford FN (2007) Information security effectiveness: Conceptualization and validation of a theory. *Internat. J. Inform. Security Privacy* 1(2):37–60.

Law KS, Wong CS, Mobley WM (1998) Toward a taxonomy of multidimensional constructs. *Acad. Management Rev.* 23(4):741–755.

Lee J, Lee Y (2002) A holistic model of computer abuse within organizations. *Inform. Management Comput. Security* 10(2):57–63.

Lee SM, Lee SG, Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Inform. Management* 41(6):707–718.

Lee Y, Larsen KR (2009) Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inform. Systems* 18(2):177–187.

Leonard LN, Cronan TP (2001) Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *J. Assoc. Inform. Systems* 1(12):1–31.

Li H, Zhang J, Sarathy R (2010) Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems* 48(4):635–645.

Liang H, Saraf N, Hu Q, Xue Y (2007) Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quart.* 31(1):59–87.

Lowry P, Cao J, Everard A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Management Inform. Systems* 27(4):163–200.

Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Trans. Prof. Commun.* 57(2):123–146.

Lowry PB, Moody GD (2014) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Inform. Systems J.*, ePub ahead of print July 8, http://dx.doi.org/10.1111/isj.12043.

Lowry PB, Posey C, Roberts TL, Bennett RJ (2014) Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *J. Bus. Ethics* 121(3):385–401.

Lowry PB, Zhang D, Zhou L, Fu X (2010) Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Inform. Systems J.* 20(3): 297–315.

Malhotra Y, Galletta D (2005) A multidimensional commitment model of volitional systems adoption and usage behavior. *J. Management Inform. Systems* 22(1):117–151.

Meyer JP, Herscovitch L (2001) Commitment in the workplace: Toward a general model. *Human Resource Management Rev.* 11(3):299–326.

Mowday RT, Steers RM, Porter LW (1979) The measurement of organizational commitment. *J. Vocational Behav.* 14(2):224–247.

Nagin DS, Paternoster R (1993) Enduring individual differences and rational choice theories of crime. *Law Soc. Rev.* 27(3): 467–496.

O'Reilly CA, Chatman J (1986) Organizational commitment and psychological attachment: The effects of compliance, identification, and internalization on prosocial behavior. *J. Appl. Psych.* 71(3):492–499.

Organ DW (1988) *Organizational Citizenship Behavior: The Good Soldier Syndrome* (Lexington Books, Lexington, MA).

Organ DW, Ryan K (1995) A meta-analytic review of attitudinal and dispositional predictors of organizational citizenship behavior. *Prospect. Psych.* 48(4):775–802.

Pahnila S, Siponen M, Mahmood A (2007) Employees' behavior towards IS security policy compliance. Sprague RH Jr, ed. *Proc. 40th Hawaii Internat. Conf. System Sci. (HICSS 2007)* (IEEE, Los Alamitos, CA), 156b.

Paternoster R, Simpson S (1996) Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law Soc. Rev.* 30(3):549–583.

Pavlou PA, Liang H, Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quart.* 31(1):105–136.

Peace AG, Galletta DF, Thong JYL (2003) Software piracy in the workplace: A model and empirical test. *J. Management Inform. Systems* 20(1):153–177.

Posey C, Bennett RJ, Roberts TL, Lowry PB (2011) When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *J. Inform. Systems Security* 7(1):24–47.

Posey C, Roberts TL, Lowry PB, Hightower RT (2014) Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inform. Management* 51(5):551–567.

Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney JF (2013) Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quart.* 37(4): 1189–1210.

Ringle CM, Wende S, Will A (2005) SmartPLS 2.0. Accessed October 1, 2013. http://www.smartpls.de.

Roberts TL, Lowry PB, Sweeney PD (2006) An evaluation of the impact of social presence through group size and the use of collaborative software on group member "voice" in face-to-face and computer-mediated task groups. *IEEE Trans. Prof. Commun.* 49(1):28–43.

Scholl RW (1981) Differentiating organizational commitment from expectancy as a motivating force. *Acad. Management Rev.* 6(4):589–599.

Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quart.* 34(3):487–502.

Siponen M, Vance A, Willison R (2012) New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Inform. Management* 49(7):334–341.

Sivo SA, Saunders C, Chang Q, Jiang JJ (2006) How low should you go? Low response rates and the validity of inference in IS questionnaire research. *J. Assoc. Inform. Systems* 7(6):351–414.

Stanton JM, Stam KR, Mastrangelo P, Jolton J (2005) Analysis of end user security behaviors. *Comput. Security* 24(2): 124–133.

Straub DW (1990) Effective IS security. *Inform. Systems Res.* 1(3): 255–276.

Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. *Comput. Security* 24(6):472–484.

Tiwana A, Keil M (2009) Control in internal and outsourced software projects. *J. Management Inform. Systems* 26(3):9–44.

Van Dyne L, Ang S (1998) Organizational citizenship behavior of contingent workers in Singapore. *Acad. Management J.* 41(6):692–703.

Van Dyne L, LePine JA (1998) Helping and voice extra-role behaviors: Evidence of construct and predictive validity. *Acad. Management J.* 41(1):108–119.

Van Dyne L, Graham JW, Dienesch RM (1994) Organizational citizenship behavior: Construct redefinition, measurement, and validation. *Acad. Management J.* 37(4):765–802.

Vance A, Lowry PB, Eggett D (2013) Using accountability to reduce access policy violations in information systems. *J. Management Inform. Systems* 29(4):263–289.

Vardi Y, Wiener Y (1996) Misbehavior in organizations: A motivational framework. *Organ. Sci.* 7(2):151–165.

Vey MA, Campbell JP (2004) In-role or extra-role organizational citizenship behavior: Which are we measuring? *Human Perform.* 17(1):119–135.

Wall JD, Palvia P, Lowry PB (2013) Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *J. Inform. Privacy Security* 9(4):52–79.

Welbourne TM, Johnson DE, Erez A (1998) The role-based performance scale: Validity analysis of a theory-based measure. *Acad. Management J.* 41(5):540–555.

Wiener Y (1982) Commitment in organizations: A normative view. *Acad. Management Rev.* 7(31):418–428.

Williams LJ, Anderson SE (1991) Job satisfaction and organizational commitment as predictors of organizational citizenship and inrole behaviors. *J. Management* 17(3):601–617.

Zhang D, Lowry PB, Zhou L, Fu X (2007) The impact of individualism—Collectivism, social presence, and group diversity on group decision making under majority influence. *J. Management Inform. Systems* 23(4):53–80.

CORRECTION

In this article, "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness" by Jack Shih-Chieh Hsu, Sheng-Pao Shih, Yu Wen Hung, and Paul Benjamin Lowry (first published in *Articles in Advance*, April 24, 2015, *Information Systems Research*, DOI:10.1287/isre.2015.0569), the Acknowledgments was updated.