December 2007

Out of Fear or Desire: Why do Employees Follow Information Systems Security Policies?

Jai-Yeol Son
University of British Columbia

Hyeun-Suk Rhee

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation
http://aisel.aisnet.org/amcis2007/268

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
OUT OF FEAR OR DESIRE: WHY DO EMPLOYEES FOLLOW INFORMATION SYSTEMS SECURITY POLICIES?

Jai-Yeol Son  
Sauder School of Business  
University of British Columbia  
jai.son@sauder.ubc.ca

Hyeun-Suk Rhee  
School of Management  
University of Texas at Dallas  
suerhee@utdallas.edu

Abstract

Two well-grounded motivational models—command-and-control and self-regulation, which are viewed as competing explanations of why individuals follow rules (Tyler and Blader 2005)—are used as conceptual lenses through which to view employees’ adherence to information systems security policy (ISSP). Specifically, we aim to identify specific factors drawn from each of the two competing approaches that determine the level of employees’ adherence to their organization’s ISSP, and to develop and empirically test a conceptual model based on the two groups of determinants to be identified. Further, we will compare the relative efficacy of the two approaches to predict each of the two types of ISSP adherence behaviors. Our conceptual arguments will be tested with data to be collected via a survey in large-scale field studies. When completed, the results of this proposed study should contribute to the literature of corporate security management by advancing our knowledge of the central determinants of employees’ adherence to ISSP. Gaining such an understanding will also be managerially important because organizations can design more effective security training and education programs to promote their employees’ adherence behaviors related to ISSP.

Keywords: Corporate security management, information systems security policies, security compliance behavior, command-and-control and self-regulation

Introduction

Security breaches can result in irrevocable damage to firms in terms of reputation, monetary damages, and financial performance. For example, the announcement of a security breach at a firm has been found to result in a negative abnormal return on the firm’s market value (Cavusoglu et al. 2004). To reduce their risk of exposure to a security breach and its subsequent consequences, firms invest in various protective measures. Most of these measures are technological. However, people who interact with the information assets of an organization are “truly security’s weakest link” (p. 4, Mitnick and Simon 2002). That is, an organization’s employees constitute one of its most significant security risks. One critical task of organizational security management is how to deal with employees effectively (Dhillon and Backhouse 2000). For example, to improve security performance, organizations need to require their employees to take precautionary measures such as updating security patches and running virus scans (Shropshire et al. 2006).

Despite the high degree of risk posed by employees, most organizations develop their corporate security programs without coming to grips with the human aspect of their exposure (Parker 1981; Straub and Welke 1998). Many organizations underestimate the importance of managing human functions and instead are heavily dependent on technological solutions for enhancing their security performance (Whitman 2003). Similarly, little research attention has been paid to the effective management of human functions to improve security performance within organizations. More research attention needs to be devoted to advancing our knowledge of how to effectively manage human functions to improve the security performance of an organization. We posit that one reason for failure to confront the risk posed by employees may be the paucity of research in this area.
The proposed research is a first step toward closing this knowledge gap by offering theoretical explanations for why employees follow (or don’t follow) their organization’s information systems security policy (ISSP). Two well-grounded motivational models—command-and-control and self-regulation, which are viewed as competing explanations of why individuals follow rules (Tyler and Blader 2005)—are used as conceptual lenses through which to view employees’ adherence to ISSP. In particular, two salient factors are identified from each model: deterrence certainty and deterrence severity from the command-and-control approach, and perceived legitimacy and perceived value congruence from the self-regulatory approach. They are proposed as the major determinants of two specific forms—compliance and deference—of employees’ rule-following behaviors with respect to IT security.

Particular attention will be paid to the comparison of the two approaches in explaining the two rule-following behaviors related to IT security. To date, IS researchers have predominantly focused on the command-and-control approach, such as general deterrence theory (Cook 1982; Ehrlich 1973), as the theoretical foundation to explain why employees adhere (or do not adhere) to an ISSP (Kankanhalli et al. 2003; Straub 1990). Little attention has been paid to understanding employees’ ISSP adherence behaviors from the self-regulatory approach. However, given the findings from a recent study (Tyler and Blader 2005), the emphasis on the command-and-control approach over the self-regulatory approach warrants close re-examination. Tyler and Blader (2005) found that the self-regulatory approach is better than the command-and-control approach in predicting employees’ rule-following behavior in general. Therefore, it will be stimulating to examine whether this particular context yields the same result. That is, do employees adhere to an ISSP mainly out of fear (i.e., the command-and-control model) or desire (i.e., the self-regulatory model)? This proposed research will systematically compare the relative efficacy of the two approaches and report the result.

Specifically, our objectives in this proposed research are threefold.

First, we intend to identify specific factors drawn from each of the two competing approaches that determine the level of employees’ adherence to their organization’s ISSP. To accomplish this objective, the determinants of the employees’ ISSP adherence behavior will be investigated in detail, guided by the framework of the two previously mentioned models.

Second, based on the two groups of determinants that will be identified, we intend to develop and empirically test a conceptual model to explain two types of employees’ ISSP adherence behaviors: compliance and deference. By incorporating these two competing approaches into a single framework, we anticipate that we will gain a more comprehensive understanding of the key motivations of employees’ ISSP adherence behavior.

Third, we will attempt to compare the relative efficacy of the two approaches as predictors of the two types of ISSP adherence behaviors. Such an understanding will enable us to guide organizations in designing more effective IT security management programs for their employees.

Conceptual Development

Development of a valid ISSP is a prerequisite to an effective security management program in organizations (Straub and Welke 1998). One important element of ISSP is to set guidelines for employees about what is allowed and is not allowed in the use of their organization’s IT resources. We view employees’ adherence behaviors related to their organization’s ISSP as a specific case of rule-following behavior, and therefore, turn our attention to the literature of rule-following behavior to understand why employees adhere (or do not adhere) to their organization’s ISSP.

Two distinct forms—compliance and deference—of rule-following behaviors are chosen for examination in this proposed study. The distinction between these two forms of behavior is well-documented in the literature (Tyler and Blader 2005). Deference refers to voluntary acceptance of rules (Tyler 1990). On the other hand, compliance refers to acquiescence to a particular kind of request when a target recognizes that he or she is being urged to respond in a desired way (Cialdini and Goldstein 2004).

The literature on rule-following behavior suggests two well-grounded approaches—command-and-control and self-regulatory models—that govern individuals’ decisions to follow or to break rules (Tyler and Blader 2005). The two approaches provide us with seemingly competing interpretations of an individual’s rule-following behavior (Tyler and Blader 2005). These two approaches are rooted in two contrasting perspectives of the motivation that directs human behavior (Ryan and Deci 2000). While the first is built on extrinsic motivational models of human behavior, the latter is on intrinsic motivational models (Tyler and Blader 2005). Extrinsic motivation suggests that individuals’ expectations about external contingencies (e.g., rewards, punishments, etc.) are a driving force that directs human behavior. On the other hand, the intrinsic motivation model suggests that individuals undertake a certain action for its own sake without regard for the contingencies they may face.

The command-and-control approach, built on extrinsic motivational models of human behavior, has been used as a dominant paradigm in understanding employees’ rule-following behavior (Tyler and Blader 2005). Organizations appear to
rely on the command-and-control approach to promote their employees’ rule-following behavior related to ISSP. An ISSP typically specifies enforcement of the policy. It often states that noncompliance may be subject to certain disciplinary actions that include termination of employment. This assumes that potential violators of ISSP are responsive to amenable to threats of sanctions.

In particular, general deterrence theory serves as a useful framework within the command-and-control approach as a way to understand organizational efforts to regulate their employees’ behavior as it relates to IT security. General deterrence theory was originally developed by Ehrlich (1973) to explain how to prevent people from engaging in illegal and/or undesirable activities. The main premise of the theory is that sanctions, punishments, or disincentives can effectively deter people from committing a deviant activity (Straub 1990). Several studies on IT security management theory have successfully applied the theory to explain the level of security performance within organizations (Kankanhalli et al. 2003; Straub 1990). For example, Straub (1990) demonstrated that organizational investments in deterrent administrative procedures are negatively associated with the level of computer abuse by employees in organizations.

The two central tenets of general deterrence theory are the certainty of sanctions and the severity of sanctions (Straub 1990; Straub and Welke 1998). These two central tenets—deterrence certainty and deterrence severity—appear to be closely related to the enforcement of ISSP. Deterrence certainty refers to the high likelihood of sanctions for violation of policy or rules; and deterrence severity refers to the harshness of the sanctions. By formally establishing an ISSP, an organization endeavors to explicitly communicate to its employees that sanctions will follow when they do not comply with the ISSP (i.e., deterrence certainty). An ISSP generally states potential sanctions, up to termination of employment, for violation of the ISSP (i.e., deterrence severity). We therefore develop the following research hypotheses regarding the effects of the factors rooted in the command-and-control approach:

\[ H1(a): \text{Deterrence certainty will have a positive impact on employees' compliance with ISSP.} \]
\[ H1(b): \text{Deterrence certainty will have a positive impact on employees' deference to ISSP.} \]
\[ H2(a): \text{Deterrence severity will have a positive impact on employees' compliance with ISSP.} \]
\[ H2(b): \text{Deterrence severity will have a positive impact on employees' deference to ISSP.} \]

In contrast to the command-and-control approach, the self-regulatory approach, as an alternative explanation of why individuals exhibit certain rule-following behaviors, focuses on individuals’ innate desires to follow rules regardless of the contingencies they expect to encounter (Tyler and Blader 2005). The approach is built on intrinsic motivation models of human behavior (Ryan and Deci 2000) and holds that the intrinsic desire to follow rules is more of a determinant of behavior than fear of the certainty or severity of prescribed sanctions. The efficacy of this approach as an explanation of employees’ rule-following behaviors in an organizational setting has been demonstrated in the prior studies (King and Lenox 2000; Suchman 1995; Tyler and Blader 2005).

Scholars have identified several sources of employees’ intrinsic motivation to follow rules instituted by their organization. Drawing upon Tyler and Blader (2005), we will focus on two sources of intrinsic motivation—perceived legitimacy and perceived value congruence—that are rooted in employees’ assessment of the social value of their organizations. Perceived legitimacy refers to an individual’s judgment that “the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs and definitions” (p. 574, Suchman 1995). For example, employees will view ISSP as legitimate when the importance of following ISSP in their work organization is successfully communicated. On the other hand, perceived value congruence refers to an individual’s judgment about congruence between his or her moral values and the rules instituted by the organization (Tyler and Blader 2005). Based on these two explanations for the origins of the intrinsic motivation for employees to follow rules instituted by their organizations, we expect that an employee’s adherence to his or her organization’s ISSP will be largely influenced by the employee’s opinion of the legitimacy of the ISSP and by the congruence between his or her moral values and the ISSP.

\[ H3(a): \text{Perceived legitimacy will have a positive impact on employees' compliance with ISSP.} \]
\[ H3(b): \text{Perceived legitimacy will have a positive impact on employees' deference to ISSP.} \]
\[ H4(a): \text{Perceived value congruence will have a positive impact on employees' compliance with ISSP.} \]
\[ H4(b): \text{Perceived value congruence will have a positive impact on employees' deference to ISSP.} \]

The command-and-control approach (e.g., general deterrence theory) has traditionally been a dominant theoretical model to understand why employees engage (or, do not engage) in adherence to an ISSP instituted by their organization (Kankanhalli et al. 2003; Straub 1990). Little attention has been paid to understanding employees’ ISSP adherence behaviors from the distant self-regulatory approach. However, interestingly, a recent study in the management area found that the self-regulatory approach provides a more explanatory power than the command-and-control approach for predicting employees’ rule-following behavior in general. We view employees’ adherence behaviors related to their organization’s ISSP as a specific case of rule-following behavior. Therefore, we expect that the result will hold in this particular rule-following behavior context: employees’ adherence to an ISSP.
**H5(a):** The self-regulatory approach will provide a more explanatory power than the command-and-control approach for predicting employees’ compliance with ISSP.

**H5(b):** The self-regulatory approach will provide a more explanatory power than the command-and-control approach for predicting employees’ deference to ISSP.

Figure 1 shows our conceptual model based on the preceding discussion.

**Proposed Methodology**
We will test our research hypotheses with data collected from a cross-sectional survey of full-time employees of organizations. As a first step, we have already begun the instrument development process through previous studies that contain measures of the constructs included in our research model. We will modify these measures, as appropriate, to make them conform better to the context of this study. Where existing scales are not applicable, we will carefully develop the items based on the descriptions in the prior studies.

For the main survey, we are considering a national panel drawn from the database of a market research firm. A web-based survey will be used to collect data. We plan to send email invitations to approximately 2,000 individuals employed by organizations with at least 20 employees and expect to achieve a sample size of at least 500.

After the data are collected from the final survey, the instrument will be tested for various psychometric properties by employing a confirmatory factor analysis approach. Structural equation modeling using Lisrel (or AMOS) will be used to test the research model. We will use a chi-square difference test to statistically compare the strengths of path coefficients from the control-and-command approach and from the self-regulatory approach. In the test, the original research model (i.e., unconstrained model) will be compared with a constrained model in which the two paths of interest were set to be equal. This chi-square difference test is considered most appropriate when path estimates are compared within the framework of structural equation modeling (Bollen 1989) and in fact, the technique has been widely used for similar comparative analyses in information systems and other research domains (Hoskisson et al. 2002; Kim and Prabhakar 2004).

**Reference**


