Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies

Jai-Yeol Son *

School of Business, Yonsei University, 50 Yonsei-ro, Seodaemun-gu, Seoul, 120-749, South Korea

ABSTRACT

Given the significant role of people in the management of security, attention has recently been paid to the issue of how to motivate employees to improve security performance of organizations. However, past work has been dependent on deterrence theory rooted in an *extrinsic motivation model* to help understand why employees do or do not follow security rules in their organization. We postulated that we could better explain employees' security-related rule-following behavior with an approach rooted in an *intrinsic motivation model*. We therefore developed a model of employees' motivation to comply with IS security policies which incorporated both extrinsic and intrinsic models of human behavior. It was tested with data collected through a survey of 602 employees in the United States. We found that variables rooted in the *intrinsic* motivation model contributed significantly more to the explained variance of employees' compliance than did those rooted in the *extrinsic* motivation model.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

Security incidents can have a negative impact on the market value of a firm. Goel and Shawky [3] found that firms experienced a 1% decrease of market share after the announcement of a security breach. Surprisingly, many incidents are perpetrated by organizational members (inside the firewall). In this sense, employees at all levels are the weakest link in information security. Employees can be a threat because they can be involved in intentional abuse (e.g., data theft, data destruction, etc.) or unintentional or accidental events (e.g., forgetting to change a password, forgetting to log off, etc.). Such acts are often referred to as IS security non-compliance behavior [13]. As they have direct access to the network of the organization, employees often become the target of thieves or hackers who attempt to use social engineering techniques to gain access to an organization's information. Nonetheless, many organizations underestimate the importance of managing human functions and rely heavily on technological solutions to their IS security. Most organizations develop their security programs without first considering the human aspect of their exposure to security breaches.

As pointed out by Siponen and Vance [9], studies in this area have relied heavily on general deterrence theory (GDT) as a theoretical basis for understanding why employees follow (or do not follow) an organization's IS security policy (ISSP) (e.g., [1,4,6]).

Thus deterrent certainty and deterrent severity of GDT have been touted as effective strategies in preventing employees from misusing the information assets of their organizations. However, the efficacy of this theoretical solution has been questioned because studies have reported mixed results about the impacts of them as effective regulators of employees' conduct.

Studies in organizational behavior that are drawn from the social psychology literature on human motivation have often explained employees' rule-following behavior with two motivation models of human behavior [12]: one is an *extrinsic motivation model* (focusing on the perceived consequences, such as punishment or reward, of breaking the rules) and the other is an *intrinsic motivation model* (holding that employees follow the rules because of their innate desire to follow the rules). Past research found that the intrinsic motivation model better explained employees' rule-following but the current research stream has been built on GDT and therefore is closely linked to the extrinsic motivation model. Despite its potential to explain employees' security-related behavior, the intrinsic motivation model has not received due attention in the literature. We argued that we could improve our ability to explain employees' violations of security-related rules with the intrinsic motivation model.

Our study, by focusing on the both the extrinsic and intrinsic models, was constructed to offer a theoretical explanation for why employees do or do not follow their organization's ISSP. In particular, two salient variables were identified for each model: perceived deterrent certainty and deterrent severity for the extrinsic model, and perceived legitimacy and value congruence from the intrinsic model. They were assumed to be the determinants of employees'

* Tel.: +82 2 2123 5456; fax: +82 2 2123 8639.
E-mail address: json@yousei.ac.kr.

behavior. The study also examined the relative contributions of the two models in understanding employees' ISSP compliance behavior. Thus our stimulating question was: Do employees comply with an ISSP mainly out of fear (the extrinsic motivation), desire (the intrinsic model), or both?

2. Theoretical foundation and hypotheses

Development of a valid ISSP is a prerequisite to an effective security management program in an organization. It is a written statement that defines the goals and objectives of the policy, requirements for the organization's security management, workers' roles and responsibilities, and penalties and countermeasures for violations. One important element of an ISSP is to define rules for appropriate use of the organization's IT resources by employees. Organizations often follow best practices provided by guidelines such as BS7799 and GASPP (Generally Accepted Systems Security Principles) to design ISSP which their employees must follow [10]. In addition, ISSP generally defines penalties for non-compliance.

We view employees' compliance with ISSP as a specific case of employees' rule-following behavior and therefore looked at the literature of rule-following behavior to understand why employees do or do not comply with their organization's ISSP. This has suggested two models explaining employees' rule-following behavior the extrinsic motivation model (a command-and-control approach) and the intrinsic motivation model (a self-regulatory approach). The extrinsic model has traditionally been used as a dominant paradigm in understanding employees' rule-following behavior. Indeed, organizations appear to focus on the extrinsic model with security policies that state that non-compliance results in disciplinary actions that include termination of employment. To this end, general deterrence theory has been used as the dominant way to explain organizational efforts to regulate their employees' behavior.

GDT was originally developed to explain how to prevent people from engaging in undesirable activities. The theory has been predominantly used as a theoretical foundation in the study of deviant behavior. The theory posits that individuals are less likely to commit a deviant activity when the risks of getting caught and the severity of punishment increases. These two central tenets, deterrent certainty and deterrent severity, are closely related to the enforcement of ISSP. Deterrent certainty refers to the high likelihood of sanctions for violation of policy or rules; and deterrent severity refers to the harshness of the sanctions.

However, deterrence effects may be better explained by *perceived* levels of sanction certainty and severity than their *actual* or objective level. For instance, prior studies have reported that perceived levels of sanction certainty and severity are highly correlated with the level of deterrence for behaviors such as marijuana use, shoplifting, petty theft, and speeding in automobiles. Our study therefore used perceived levels of deterrent certainty and severity. Such perceptions can result from both direct and indirect experience with punishment and punishment avoidance. That is, people develop their perception of deterrent certainty and severity by experiencing punishment or punishment avoidance subsequent to committing a deviant behavior; the perceptions can be developed by observing how others have been treated after committing a deviant behavior. Similarly, we assumed that employees would develop their perceptions on deterrent certainty and severity due to both personal and observed experience of punishment and punishment avoidance due to ISSP non-compliance actions.

Kankanhalli et al. [5] found that deterrent severity was not a strong predictor of IS security effectiveness in organizations. More recently, D'Arcy et al. [1] found that only deterrent severity

reduced IS misuse by employees. On the other hand, Herath and Rao [4] found that deterrent certainty positively affected employees' security policy compliance intention, but they reported a negative effect of deterrent severity on employees' security policy compliance intention. In spite of these mixed findings, we followed the reasoning of GDT described and made two hypotheses:

H1. Deterrent certainty is positively associated with employees' compliance with ISSP

H2. Deterrent severity is positively associated with employees' compliance with ISSP

The intrinsic motivation model of human behavior holds that innate desires and preferences outweigh expected outcomes, such as rewards and sanctions. Several reasons are advanced to explain why employees will exhibit varying levels of intrinsic motivation to follow rules of their organization, including differences in personal norms and moral beliefs. D'Arcy et al. recently offered empirical evidence that employees' moral commitment has a strong deterrent effect on IS misuse. Also, employees' assessment of their employer may be important sources of intrinsic motivation to follow workplace rules. Drawing upon Tyler and Blader [12], we focus on two specific workplace judgments: perceived value congruence and perceived legitimacy; these are particularly important to managers because, unlike other sources of intrinsic motivation that originate from individual differences in personal norms and moral beliefs, employees' judgments of their employer can be shaped through their interactions.

In line with the conceptualization of perceived legitimacy [11], in our study we defined it as the extent to which employees view the ISSP as appropriate, desirable, and just. Employees will view it as legitimate when the importance of following it is successfully communicated. When an organization attempts to influence the behavior of its members, it is critical to achieve legitimacy in the eyes of its members. However, its possession and use of power is not always enough to ensure that the members will act on its requests. For instance, individuals' perceptions of the legitimacy of a law have been found to be a strong deterrent to minor offenses, such as traffic violations. Similarly, prior work has shown that an employer's rules perceived as legitimate were likely to be followed.

Perceived value congruence was defined as an employee's assessment of the extent to which he or she and his or her employer share the same value set. People generally tend to interact with others sharing similar beliefs because this interaction verifies and reinforces their own beliefs. Similarly, they tend to be satisfied with their job, are committed to their organization, and desire to continue their employment relationship for a long time [2]. In the employee rule-following literature, strong empirical evidence exist that employees' perceptions of value congruence with their employer increase the likelihood that they will follow the rules instituted by the employer. We therefore formulated the following two hypotheses:

H3. Perceived legitimacy is positively associated with employees' compliance with ISSP

H4. Perceived value congruence is positively associated with employees' compliance with ISSP

Based on our review of the literature on individuals' rule-following behavior, we posit that the intrinsic motivation model as well as the extrinsic motivation model can play important roles in predicting employees' ISSP compliance. We formally tested this assertion by developing the following hypothesis:

H5. Variables drawn from both the extrinsic and intrinsic motivation models will explain significantly more employees' ISSP