IS Security Policy Violations: 
A Rational Choice Perspective

Anthony Vance, Brigham Young University, USA
Mikko Siponen, University of Oulu, Finland

ABSTRACT

Employee violations of IS security policies are reported as a key concern for organizations. Although behavioral research on IS security has received increasing attention from IS scholars, little empirical research has examined this problem. To address this research gap, the authors test a model based on Rational Choice Theory (RCT)—a prominent criminological theory not yet applied in IS—which explains, in terms of a utilitarian calculation, an individual’s decision to commit a violation. Empirical results show that the effects of informal sanctions, moral beliefs, and perceived benefits convincingly explain employee IS security policy violations, while the effect of formal sanctions is insignificant. Based on these findings, the authors discuss several implications for research and practice.

Encouraging employees to comply with IS security policies is a major challenge for organizations. This is because no IS security practice or technique, no matter how effective, can be ultimately successful if improperly implemented by its users (Aytes & Conolly, 2004; Ernst & Young, 2008; Puhakainen, 2006). Employees who are aware of their organization’s IS security policies and yet willfully disregard or violate them pose a particular challenge, given that the existence of IS security policies and security awareness programs have little effect on these employees (Siponen, 2000; Stanton, Stam, Mastrangelo, & Jolton, 2005). Despite the clear need to understand and respond to this problem, little IS research has investigated employee violations of IS security policies.

Although IS scholars have examined IS security-related behavioral issues such as computer “abuse” and “misuse” (D’Arcy, Hovav, & Galletta, 2009; Lee, Lee, & Yoo, 2004; Straub, 1990), this body of research is not explicitly designed to measure the factors affecting intentional violations of IS security policies. For this reason, an understanding of computer abuse might not help to clarify a situation in which employees are aware of their organization’s IS security policies, yet willfully choose to violate them.

Furthermore, IS research on computer abuse in particular has focused on the cost of a utilitarian deterrence approach: formal sanctions. In turn, the perceived benefits of norm

DOI: 10.4018/joeuc.2012010102
breaking, informal sanctions, and moral evaluations have received little or no attention from IS security scholars, even though recent studies in the field of Criminology have highlighted the important roles these constructs play in decisions to violate. More importantly, these perceived benefits have received no attention in the study of employee IS security policy violations. As a result, there is a need for studies that apply (a) informal sanctions, (b) moral evaluations, and (c) benefits in the area of IS security policy violation.

To address this need, we believe that Rational Choice Theory (RCT)—a prominent criminological theory that has not yet been applied to IS—is especially useful for studying employee IS security policy violations. This theory can be seen as a modern extension of classical deterrence theory, which holds that violations can be reduced by imposing sanctions that are certain and severe. However, RCT goes beyond deterrence theory by incorporating individuals’ perceptions of benefits of violations and informal sanctions as well as espoused moral beliefs. According to RCT, individuals perform a mental utilitarian calculation involving each of these factors when making a decision to commit a violation. An empirical test given in two organizations strongly supports our model, showing that perceived benefits, moral beliefs, and informal sanctions have a significant impact on employees’ intentions to violate IS security policies. However, contrary to the findings of several studies examining computer abuse, the effect of formal sanctions is not significant, suggesting that the contexts of computer abuse on the one hand and intentional violations of IS security policies on the other may be appreciably different.

The remainder of this paper is organized as follows: the second section contrasts previous work on IS security behavior in general with the specific problem of IS security policy violations. The third section develops our theoretical model and hypotheses, and the fourth section presents the empirical results. The fifth section discusses the implications of these findings for research and practice. Finally, the conclusion summarizes the key findings and contributions of the paper.

**Previous Research on IS Security Behavior and Compliance**

Previous research in the area of IS security behavior in an organizational context can be divided into three areas: (1) IS security awareness and training, (2) computer abuse, and (3) information security policy violations. In this section, we show below that while many contributions have been made in the first two areas, comparatively little research has directly addressed the problem of intentional violations of IS security policies. Next, we show that although the first two streams of research have made important contributions to IS security research, they have addressed distinctly different research questions than those examining factors that lead to deliberate violations of IS security policies.

**IS Security Awareness and Training**

Research on IS security awareness and training programs (Lafleur, 1992; McLean, 1992; Puhakainen, 2006; Siponen, 2000; Telders, 1991; Thomson & von Solms, 1998; Vroom & von Solms, 2002) offers important insights into how employees’ awareness of IS security policies and guidelines can be increased (Lafleur, 1992; McLean, 1992; Thomson & von Solms, 1998; Vroom & von Solms, 2002). Such research also offers insights into how employees can be motivated to comply with such policies (Puhakainen, 2006; Siponen & Iivari, 2006). Contributions to this research stream generally comprise conceptual frameworks (Lafleur, 1992; McLean, 1992; Siponen, 2000; Telders, 1991; Thomson & von Solms, 1998; Vroom & von Solms, 2002) and qualitative studies on the effect of IS security education on employees’ IS
Users as Developers: A Field Study of Call Centre Knowledge Work
[www.igi-global.com/chapter/users-developers-field-study-call/18648?camid=4v1a](www.igi-global.com/chapter/users-developers-field-study-call/18648?camid=4v1a)

Semantic Composition of Web Portal Components
[www.igi-global.com/chapter/semantic-composition-web-portal-components/18158?camid=4v1a](www.igi-global.com/chapter/semantic-composition-web-portal-components/18158?camid=4v1a)