Chapter 11
Unethical Information Security Behavior and Organizational Commitment

Toshihiko Takemura
Saga University, Japan

ABSTRACT

In this chapter, the authors investigate the relationships between unethical behaviors from the viewpoint of information security and organizational commitment by analyzing micro data collected from a survey the author conducted in March 2012. As a result, at first, it is found that heightening the degree of Organizational Commitment (OC) does not exclusively deter all unethical behaviors, but that at least OC deters the intention to access non-work-related Websites in the workplace. In addition, it is confirmed that the effects of OC toward the intention of the non-work-related Website access in the workplace according to the organizational attributes are different. In the organizations whose non-work-related Website access in the workplace is prohibited as a rule, heightening the degree of OC is able to reduce the respondents who access non-work-related Websites in their workplace. It is found that based on TPB and TRA, the attitude and risk assessment toward the intention of unethical behaviors have an influence on the behaviors.

INTRODUCTION

In most organizations, for the purpose of hedging security accidents, various kinds of technical measures and/or managements are introduced and operated, and they achieve a certain amount of effect. Unfortunately, however, they sometime result in deterioration in employee’s productivity and morale (Albrechtsen, 2007; Albrechtsen & Hovden, 2009). Besides, regardless of implementing them, there are cases that some security accidents occur. Then, we cannot necessarily say that the reason is that organizational measures are inadequacy, and the number of incident ac-
Unethical Information Security Behavior and Organizational Commitment

Incidents caused by that employee who unethically behaves is not negligible. For example, though the organizational rule works on deterring employee’s unethical behaviors to a certain degree, some employees may sometime violate the rule if the rule is too strict or difficult to comply with originally. For the purpose of deterring such a behavior, the various programs such as security education and training are developed (Thomson & von Solms, 1998; Puhakainen & Siponen, 2010; Albrechtsen & Hovden, 2010), and the programs make the employees understood the need and importance of information security and heightened their security awareness. On the other hand, even if they recognize the importance of information security, in practice some employees do not comply with the rules and they would become vulnerability of the organizations. Therefore, employees need to have self-enforceable security awareness toward the ethical behavior. If it is feasible, it is expected that the organizational measures would become workable well.

If there is a method that not only improves productivity of employees’ original daily-tasks, but also are also able to improve their security awareness, the method would be ideal for the organization. As one of the methods, heightening employees’ organizational commitment (OC) is thinkable. It seems that this fact holds true for the unethical security behaviors and the behavioral intentions according to various previous works. Especially, from the viewpoint of information security measures, it is expected that employees have their self-enforceable security awareness toward the ethical behavior by heightening OC.

There are some related works with regard to relationships between OC and information security measures discussed from practical viewpoints (Siponen, 2000; Siponen, 2001; Trompeter & Eloff, 2001). On the other hand, there are few empirical studies still now.

We investigate the relationships between unethical behaviors from the viewpoint of information security and OC by analyzing micro data collected from a survey for Japanese workers that the author conducted at March 2012.

BACKGROUND

Organizational Commitment

The study of OC is important because organizational commitment can influence employees’ creativity, innovativeness, adaptation, and reduces unethical behaviors. For a long time, OC is defined as the subject’s perceptions concerning his loyalty toward the organization, his willingness to exert a great deal of effort to achieve organizational goals, and his acceptance of the organization’s values (Porter et al., 1974). In the other words, OC is an attitude that influences employee behavior beneficial to the organization (Riketta, 2002).

OC is the more attractive for practicians and researchers in work commitment; job involvement, career commitment and OC. There are some reasons. For example, employees’ turnover or retire predicted by OC would be more accurate rather than by the other commitments and job satisfaction (Williams & Hazer, 1986; Mathiew & Zajac, 1990; Riketta, 2002), or the heightening of OC is related with improving their performance or productivity, or reducing their work absence and lateness (Morris & Sherman, 1981; Bateman & Strasser, 1984).

Information Security Behaviors

For the purpose of protecting organization’s assets from misuse, abuse and the other cheating, many organizations utilize a various tools and measures such as installing firewalls, backing up their systems, restricting access controls and using comprehensive monitoring systems. However, these technical tools and measures are not necessarily sufficient because the measures relate