Motivating IS security compliance: Insights from Habit and Protection Motivation Theory

Anthony Vance, Mikko Siponen, Seppo Pahnila

*Information Systems Department, Marriott School of Management, Brigham Young University, United States
+IS Security Research Center, Department of Information Processing Science, University of Oulu, Linnanmaa, P.O. Box 3000, FIN-90014 Oulu University, Finland

1. Introduction

Organizations typically encounter at least one breach of security due to an information security policy violation per year [1]. Furthermore, it has been estimated that over half of all IS security breaches are indirectly or directly caused by employee failure to comply with IS security procedures [19]. It is not surprising that a critical concern for organizations is the extent to which employees comply with information security policies [6,18]. A number of behavioral approaches have been proposed in the literature for either improving employees’ compliance with the security procedures of their organizations or to explain their reasons for computer abuse [16].

Many of behavioral approaches draw upon theories of Criminology and Psychology, such as Deterrence Theory [9], Neutralization Techniques [17] and socio-cognitive [11]. These, while valuable, have not resulted in examination of the influence of past compliance behavior on appraisals of information security threats and coping responses. This is an important omission, since Protection Motivation Theory (PMT) suggests that past behavior strongly influences the process of assessing threats and one's ability to cope with them.

To address this gap, we integrated the full PMT model with habit, a routinized form of past and automatic behavior [10]. Research on the theory of habit has highlighted the pervasive effect of habit on human behavior. This allowed us to examine the influence of routinized past IS security compliance behavior on the threat appraisal and coping mechanisms theorized in PMT.

To evaluate our model, we performed an empirical study in an organization in Finland (with a population of 210 employees). Our results offer relevant insights for both practitioners and researchers.

2. An overview of PMT and past applications in IS security

PMT explains how individuals are motivated to respond to warnings about threats or dangerous behaviors, termed fear appeals. In interpreting such messages, individuals use a cognitive process to weigh their response to the threat. PMT includes three factors that explain how threats are perceived, termed threat appraisal factors. These are rewards or benefits (any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior), severity (the magnitude of the threat), and vulnerability (the extent to which the individual is perceived to be susceptible to the threat).

PMT also includes three factors that explain an individual's ability to cope with the threat, termed coping appraisals. These are response efficacy (the belief in the perceived benefits of the coping action by removing the threat), response cost (to the individual in implementing the protective behavior), and self-efficacy (the degree that he or she believes it is possible to implement the protective behavior).
2.1. Previous IS security research using PMT

Because of its general nature, PMT has recently been applied to the domain of information security. Previous work in organizational context have focused on employees compliance with IS security procedures. However, no recent study has fully employed all of the coping and threat appraisals of PMT.

Of the four papers dealing with this [4,7,13,22] none discussed Antecedent sources of Information or Rewards. All dealt with Vulnerability and Severity, though Pahnila et al. combined them. All dealt with Response- and Self-Efficacy. Also response cost was only used in two studies: those by Herath and Rao and Pahnila et al.

In the context of IS security compliance, rewards are considered as only those for compliance, which presents an incomplete view of the cognitive mediating processes central to PMT. Furthermore, past behavior may be considered to be an important source of information influencing protection motivation. However, no studies have investigated sources of information antecedent to the PMT process. To overcome these two gaps, we extended the full PMT model to include habit as an antecedent effect.

3. Theoretical model

Our theoretical model employed habit theory and PMT. The original formulation of PMT explicitly suggested that “prior experience” was a preceding factor for PMT. Also it was noted that the PMT model assumed that both situational cues and habit had important effects on the decision-making process of PMT.

This view was also shared by investigators of the effect of habit, noting that many of the behaviors studied were repetitive, executed on a daily basis, and therefore possibly routine or habitual. We therefore theorized that habit was a determinant of the cognitive mediating process of protection motivation: our integrated model is shown in Fig. 1.

3.1. Protection Motivation Theory

PMT suggests that information about a threat causes a cognitive mediating process in individuals that appraises positive or negative responses. Thus employees' non-compliance with information security policies represents a maladaptive response, while compliance with them is an adaptive response. The maladaptive response invokes threat appraisal factors, which decrease the likelihood of maladaptive response, such as non-compliance with IS security policies.

One of the three threat appraisal factors is rewards (or benefits), which results in any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior which in our context is an employees' non-compliance with information security policies. Intrinsic and extrinsic rewards will increase the probability of a maladaptive response whereas perceptions of the severity and vulnerability to threats will decrease the probability of such a response. Rewards indicate physical or psychological pleasure or peer approval, which increase the probability of a maladaptive response. If an individual perceives that the reward for not adopting the coping response is higher than adopting it, then the individual will be less likely to adopt the coping response. In our context, we conceptualize rewards as saving time by not complying with the information security policy. Research on information security policy compliance shows that people see saving time as a benefit for non-compliance [21]. Vulnerability is to the probability that an unwanted incident will happen if no actions are taken to prevent it. In our study, vulnerability denotes employees' assessment of whether their...
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات