Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory

*Princely Ifinedo**

Shannon School of Business, Cape Breton University, P.O. Box 5300, Sydney, Nova Scotia B1P 6L2, Canada

ARTICLE INFO

Article history:
Received 5 August 2011
Received in revised form
23 September 2011
Accepted 31 October 2011

Keywords:
Information systems security policy
Behavioral intentions
Compliance
Theory of planned behavior
Protection motivation theory

ABSTRACT

This research investigated information systems security policy (ISSP) compliance by drawing upon two relevant theories i.e. the theory of planned behavior (TPB) and the protection motivation theory (PMT). A research model that fused constituents of the aforementioned theories was proposed and validated. Relevant hypotheses were developed to test the research conceptualization. Data analysis was performed using the partial least squares (PLS) technique. Using a survey of 124 business managers and IS professionals, this study showed that factors such as self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence ISSP behavioral compliance intentions of employees. The data analysis did not support perceived severity and response cost as being predictors of ISSP behavioral compliance intentions. The study's implications for research and practice are discussed.

1. Introduction

Modern organizations rely on information systems (IS) for their survival; this is because such systems often hold valuable organizational data resources (Cavusoglu et al., 2004; Richardson, 2011; Ifinedo, 2009, 2011). To safeguard the critical IS assets held in such systems from misuse, abuse and destruction; organizations often utilize a variety of tools and measures such as installing firewalls, updating anti-virus software, backing up their systems, maintaining and restricting access controls, using encryption keys, using surge protectors, and using comprehensive monitoring systems (Ryan, 2004; Workman et al., 2008; Lee and Larsen, 2009). However, the aforementioned tools and measures offer a technological or technical solution to the problem, and are rarely sufficient in providing total protection of IS organizational resources (Rhodes, 2001; Sasse et al., 2004; Stanton et al., 2005; Herath and Rao, 2009a).

Researchers including Vroom and von Solms (2004), Stanton et al. (2005), and Pahnila et al. (2007) have noted that organizations that pay attention to technical as well as non-technical means of protecting their IS assets and resources are likely to be more successful in their attempts to protect their key IS assets. The onus is therefore on organizations to utilize multi-perspective approaches for protecting their IS assets and resources (Herath and Rao, 2009b). Indeed, several researchers have indicated that socio-organizational imperatives are equally considered important to organizations with desires to safeguard their IS resources (Vroom and von Solms, 2004; Stanton et al., 2005; Pahnila et al., 2007; Bulgurcu et al., 2010). In fact, it has been reported that one of the reasons why IS security

* Tel.: +1 902 563 1227; fax: +1 902 563 1941.
E-mail addresses: pifinedo@gmail.com, princely_ifinedo@cbu.ca.
0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.10.007

incidents and abuses continue to plague organizations is that organizational employees are the weakest link in ensuring IS security; they constitute an insider threat to their organizations (Vroom and von Solms, 2004; Stanton et al., 2005; Post and Kagan, 2007; Warkentin and Willison, 2009; Richardson, 2011). For instance, a study that evaluated the tradeoffs between computer security protection and accessibility concluded that employees are more likely to bypass security measures in order to complete a task (Post and Kagan, 2007). Against such a backdrop, it would be a beneficial approach for organizations to focus on their own employees' intentions and behaviors.

Recently, studies have emerged to signify the pertinence of employees' compliance with organizational rules, guidelines, and requirements laid out in their information systems security policy (ISSP) as a useful mechanism for shaping or influencing the behaviors of their employees with respect to how organizational IS resource are used (Cavusoglu et al., 2004; Knapp and Marshall, 2006; Pahnila et al., 2007; Post and Kagan, 2007; LaRose et al., 2008; Bulgurcu et al., 2010; Ifinedo, 2009, 2011). The same stream of literature also suggests that where such ISSPs are in place to help safeguard against misuse, abuse, and destruction of IS assets, employees often do not readily comply with such documents (Pahnila et al., 2007; Siponen and Vance, 2010). Thus, studies designed to increase of knowledge of the sorts of issues that may be inhibiting or encouraging the compliance of ISSP in organizations will be welcoming to the extant literature. Insights in this area of study have started to surface in the relevant literature (Cavusoglu et al., 2004; Vroom and von Solms, 2004; Siponen and Willison, 2009; Bulgurcu et al., 2010; Anderson and Agarwal, 2010). This current research is designed to complement the growing body of knowledge in the area.

Two relevant theories i.e. theory of planed behavior (TPB) (Ajzen, 1991) and the protection motivation theory (PMT) (Rogers, 1983) will be integrated to increase our knowledge of ISSP compliance by employees in modern organizations. Previous works have used research frameworks that integrated PMT and TPB with other theories (e.g. Bulgurcu et al., 2010; Pahnila et al., 2007; Herath and Rao, 2009a,b; Lee and Kozar, 2005; Lee and Larsen, 2009). To the best of knowledge, no prior research has used both theories in a single study. Anderson and Agarwal's (2010) review of the literature in this area indicated that the two foregoing theories have been used by ISSP compliance research.

With respect to the PMT, which emphasizes the fear appeal perspective, Siponen and Vance (2010) asserted that ISSP compliance research using fear appeal theories often do not always explicate noncompliance behaviors. Others (e.g. Herath and Rao, 2009b) provided support for the view espoused by Siponen and Vance (2010). Thus, by incorporating the PMT with the TPB, an enduring behavior-intention theory, this research aims at engendering our knowledge in the area. Further to this, compliance, being a complex concept, should be studied from differing perspectives to enhance knowledge (Aronson et al., 2010).

The remainder of the paper is organized as follows: First, information about the study's theoretical foundations is presented. Second, the research model and hypotheses then follows Third, the research methodology is presented. Next, information about the analyses and results are presented. The paper concludes by discussing its findings, implications, limitations and avenues for further research.

2. Theoretical background

2.1. *Protection motivation theory*

Protection Motivation Theory (PMT), which developed by Rogers (1983) expanded the health-related belief model in the social psychology and health domains (Rippetoe and Rogers, 1987; Milne et al., 2000). Drawing from the expectancy-value theories and the cognitive processing theories, PMT was developed to help clarify fear appeals. PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson and Agarwal, 2010). In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event (Rogers, 1983; Woon et al., 2005). It is composed of the following two items:

(i) Perceived vulnerability i.e. an individual's assessment of the probability of threatening events. In this study, threats resulting from noncompliance with ISSP.
(ii) Perceived severity i.e. the severity of the consequences of the event. In this instance, imminent threats to the security of one's organization's information arising from noncompliance with ISSP.

The coping appraisal aspect of PMT refers to an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et al., 2005). Coping appraisals are made up of three sub-constituents:

(i) Self-efficacy – this factor emphasizes the individual's ability or judgment regarding his or her capabilities to cope with or perform the recommended behavior. In the context of this research, it refers to the sorts of skills and measures needed to protect the information in one's organizational IS (Bandura, 1977, 1991; Woon et al. 2005; Pahnila et al., 2007).
(ii) Response efficacy – this factor relates to the belief about the perceived benefits of the action taken by the individual (Rogers, 1983). Here, it refers to the compliance with ISSP as being an effective mechanism for detecting a threat to one's organizational IS assets.
(iii) Response cost – this factor emphasizes the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behavior, in this instance complying ISSP.

Previous research that have used PMT found it useful in predicting behaviors related to individual's computer security behaviors both at home and in organizations (Lee and Larsen, 2009; Ng et al., 2009; Anderson and Agarwal, 2010) and ISSP compliance (Herath and Rao, 2009a,b; Pahnila et al., 2007).