Information & Management 51 (2014) 217–224

Contents lists available at ScienceDirect

Information & Management

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

Employees' adherence to information security policies: An exploratory field study

Mikko Siponen [a], M. Adam Mahmood [b,*], Seppo Pahnila [c]

[a] Department of Computer and Information Systems, University of Jyväskylä, Finland
[b] Department of Accounting and Information Systems, University of Texas at El Paso, United States
[c] Department of Information Processing Science, The University of Oulu, Finland

ARTICLE INFO

Article history:
Received 21 August 2009
Received in revised form 19 March 2013
Accepted 15 August 2013
Available online 21 December 2013

Keywords:
Information security
Information security policy compliance
Protection Motivation Theory
Cognitive Evaluation Theory
Theory of Reasoned Action
Threat appraisal
Self-efficacy
Response efficacy
Attitude
Normative beliefs
Rewards
Moderating effect
Work experience
Information systems security
Information systems security policies
Employees' compliance of information systems security policies
Multi-theory based model to explain employees' adherence to information security policies
SEM-based analysis of the model

ABSTRACT

The key threat to information security comes from employees who do not comply with information security policies. We developed a new multi-theory based model that explained employees' adherence to security policies. The paradigm combines elements from the Protection Motivation Theory, the Theory of Reasoned Action, and the Cognitive Evaluation Theory. We validated the model by using a sample of 669 responses from four corporations in Finland. The SEM-based results showed that perceived severity of potential information security threats, employees' belief as to whether they can apply and adhere to information security policies, perceived vulnerability to potential security threats, employees' attitude toward complying with information security policies, and social norms toward complying with these policies had a significant and positive effect on the employees' intention to comply with information security policies. Intention to comply with information security policies also had a significant impact on actual compliance with these policies. High level managers must warn employees of the importance of information security and why it is necessary to carry out these policies. In addition, employees should be provided with security education and hands on training.

1. Introduction

Information security incidents have increased significantly in the last decade. In order to cope with increased threats, not only technical solutions, but IS security policies have been proposed. Employees, however, seldom comply with these policies, placing their organizations' assets and businesses at risk. In order to address this concern, several information security policies compliance approaches have been proposed. We have decided to build a new multi-theory based model using the Protection Motivation Theory (PMT), the Theory of Reasoned Action (TRA), and the Cognitive Evaluation Theory (CET) and then to validate it empirically using a large sample of practitioners from Finland ($N = 669$).

2. Previous work on information security policy compliance

Recent research studies on the topic of security policy compliance have been divided into three categories: (1) conceptual principles with no underlying theory or empirical evidence; (2) theoretical models with no empirical evidence; and (3) empirical work grounded in theory.

* Corresponding author at: Department of Accounting and Information Systems, University of Texas at El Paso, El Paso, TX 79968, United States.
Tel.: +1 915 747 7748; fax: +1 915 747 5126.
E-mail addresses: mikko.t.siponen@jyu.fi (M. Siponen), mmahmood@utep.edu (M. Adam Mahmood), seppo.pahnila@oulu.fi (S. Pahnila).

0378-7206/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.im.2013.08.006

Studies in the conceptual principles area only present practical guidelines and suggestions for improving employees' compliance with information security policies as well as allow users to learn of information security countermeasures that can reduce the resulting problems.

Theoretical models without empirical evidence include studies that provide *theory-based* insights into how employees' policy compliance can be enhanced. These, however, do not offer any evidence to support the insights. These models suggest that both social and technical solutions can be used to reduce computer abuse. Karjalainen and Siponen [8] claimed that that IS security training had some unique characteristics and, therefore, needed its own theory, which, according to the authors, must satisfy four pedagogical requirements: (a) a group oriented approach of teaching and learning, (b) teaching contents based on collective experiences of learners' contents, (c) collaborative learning based teaching methods that produce collective knowledge, and (d) evaluation of learning needs to emphasize experiential and communication-based methods. They concluded by showing how an IS security training approach can be designed that satisfy these requirements.

Empirical studies grounded in theories present studies that are both theory-based and empirically validated. Aytes and Connolly [1] used the rational choice model to explain why university students engage in risky computing behavior such as opening email attachments without checking for viruses, failing to back up files, and disclosing passwords. Using a sample of 167 students, they found that respondents continued to practice unsafe computing even when they were fairly knowledgeable in safe computing practices. They suggested that providing additional information may not necessarily result in safe behavior and concluded by suggesting that organizations may have to force participants to comply.

D'Arcy, Hovav, and Galletta [3] stated that insider misuse of IS resources was a significant threat to organizations. They used an extended version of the deterrence theory to investigate whether perceived certainty and severity of organizational sanctions were affected by user awareness of IS security countermeasures. They found, using a sample of 269 employees from eight companies, that computer users were aware of the: security policies through the training programs; and observation of computer misuse. They further found that perceived severity of sanctions was more effective in reducing IS misuse than actual sanctions.

Johnston and Warkentin [7] investigated the effect of fear-inducing arguments (e.g., fear appeals) on end users' compliance with information security policies. The authors postulated, based on an extension of the Protection Motivation Theory (PMT), that response efficacy, self-efficacy, and social influence would have a positive effect on employees' intention to adopt anti-spyware software tools. They hypothesized that the perception of threat severity would negatively affect response efficacy and self-efficacy and also that the perception of threat susceptibility would negatively influence the efficacies. They found support, using a sample of 275 participants, for all hypothesized relationships with the exception of perceptions of threat susceptibility to response efficacy and perceptions of threat susceptibility to self-efficacy.

A recent study by Hovav and D'Arcy [5] used the deterrence theory in an experiment conducted across cultures. Using a sample of 366 MBA and industry respondents from the United States and 360 from South Korea, the authors found that perceived certainty (PC) of sanctions had a stronger influence on IS misuse intention for the Korean sample whereas the influence of perceived severity (PS) of sanctions was stronger for the U.S. sample. Technical counter measures (TCM) had a significant relationship with perceived certainty of measures but not perceived severity for the Korean sample whereas, for the U.S. sample, TCM had a significant relationship with both PC and PS. Age had a significant relationship with IS misuse intention (INT) for the U.S. sample whereas, the Korean sample showed that age was positively associated with INT. The authors surmised, based on their findings, that deterrence theory was not culturally neutral.

Jai-Yeol [6] questioned the efficacy of the results obtained by previous research studies in IS security policy compliance using a general deterrence theory-based model that was embedded in extrinsic motivation. The author postulated that an intrinsic motivation-grounded model could do a better job than an extrinsic motivation-based model. The author used a model that included both extrinsic and intrinsic characteristics of human behavior. Using a PLS-based approach to data analysis on a sample of 602 employees, the author found that constructs in the intrinsic motivation paradigm contributed significantly more to the employees' security policy compliance variability than constructs embedded in the extrinsic motivation paradigm.

Siponen and Vance [12] felt that IS security researchers had used deterrence theory to examine the violations of IS security policies, whereas neutralization theory could provide a better explanation of IS security violations. They postulated that neutralization positively affect intention to violate IS security policies. The authors also theorized that formal sanctions, informal sanctions, and shame negatively affected intention to violate IS security policies. They found, using a sample of 395 employees from different organizations, that neutralization was a good predictor of employees' intention to violate IS security policies. The effect of informal sanctions on intention, in the presence of neutralization was not, however, significant. Also, in the presence of neutralization, formal sanctions did not predict IS security violations.

Most recent studies used only one theory. Some authors used a rational choice model to study the risky computing behavior of university students while others used PMT. Combining different theories is termed *theory integration*; it entails fusing several theories. The hope is that an integrated model will provide more explanatory power than one derived from a single theory. With the exception of Herath and Rao [4], none of the prior studies were based on multiple theories.

3. The research model and hypotheses

3.1. Theories and the research model

Protection Motivation Theory (PMT), is considered to be the leading theory in the area of health behavior motivation. It involves the appraisal of its two components: threat and coping. *Threat appraisal* is concerned with the process of evaluating a fear that occurs due to an individual's perception of how threatened he or she feels due to some situation. There are two threat appraisal factors: *perceived vulnerability* (how an individual feels that a negative event will take place if no measures are taken to counter the problem) and *perceived severity* (the degree of physical and psychological harm an illness may seem to cause). In the context of our research, these are measures of how susceptible the employee's organization is to information security breaches and the potential harms (e.g., financial loss) that may occur because of the breaches. *Coping appraisals* consists of two dimensions: self-efficacy (individuals' ability or judgment of their capabilities to carry out the coping response actions) and response efficacy (the effectiveness of the recommended coping response in reducing threat to an individual). Self-efficacy is the most powerful predictor of intention to comply with a behavior and, in the context of our study, refers to employees' belief that they can apply and adhere to information security policies and procedures.