Information Security Training Customized by Risk Profile

Submission Type: Emergent Research Forum Paper

Shuting Xu
Georgia Gwinnett College
sxu@ggc.edu

Peter Meso
Georgia Gwinnett College
pmeso@ggc.edu

Yi Ding
Georgia Gwinnett College
yding1@ggc.edu

Abstract

To ensure the employees follow companies' information security procedures and policies, information security training is adopted as a common approach to improving employees' security behavior. In this paper we study the efficacy of information security training customized by risk profile. Firstly, we will examine the efficacy of security training customized by risk profile on security risk assessment. Secondly, we will evaluate the effect between risk assessment and security behavior.

Keywords

Information security training, risk profile, risk assessment.

Introduction

To ensure the employees follow companies' information security procedures and policies, information security training is adopted as a common approach to improve employees' security behavior (Karjalainen and Siponen 2011). Currently, information security education and training are provided in a variety of avenues, such as traditional lectures, hands-on exercises, real world simulations, online training, emails on security tips and updates, etc. For a specific trainee, what is the training method that can effectively improve his or her security behavior?

To improve the efficacy of information security training, we propose to implement a Learner Profile Based Information Security Learning (LPBISL) Recommendation System based on several behavioral theories (future work). According to Bostrom (Bostrom, et. al. 1990), learning style is an important predictor of a subject's learning performance, both by itself and through its interaction with training methods. Other studies have shown that knowledge gap and risk profile can be important variables that influence one's security behavior (Dreyfus, 1980; Weber, et. al. 2002). Recognizing the importance of those behavioral changing variables, our recommendation system is able to analyze trainee's risk profile, knowledge gap, and security behavior, and based on the analysis results, the system will choose appropriate learning materials to effectively influence one's security behavior. While some security training systems consider the users' learning styles, most of the current ones aim to improve the learners’ knowledge about information and systems security. These systems customize their materials based on the learner's knowledge gap. Our system, however, provides learning recommendations based on not only the learners’ knowledge gap and learning styles, but also their security behavior weakness and risk awareness. Moreover, our goals are not only to improve the users’ knowledge, more importantly, to influence their security behaviors. To the best of our knowledge, this is the first time that behavioral theories will be applied in developing a recommendation system for information security training/education.

In this paper we limit our focus on the efficacy of information security training based on risk profile. In information security literature risk perception has been studied as an important factor that could have an impact on information security behavior based on the Protection Motivation Theory (Vance, et. al. 2014). In this paper, we adopt the consumer choice theory (Cox 1967; Grewal, et. al. 1994), which posits that risk
assessment not only is situation specific but also is influenced by individual’s factors such as individual’s risk profiles. The contribution of this paper is two-fold. First, we will examine the efficacy of customized security training based on risk profile on security risk assessment. Second, we will evaluate the effect between risk assessment and security behavior. We describe the conceptual model, the hypotheses, and the methodology to validate the research model. The conceptual model presented will work as part of the theoretical foundation for LPBISL Recommendation System.

**Literature Review**

A variety of approaches have been proposed in literature for information security training (Karjalainen and Siponen, 2011), such as psychological training approaches, learning theories based, process based, security awareness approaches, situational approaches, social engineering preventive approaches, and computer-based training. According to (Karjalainen and Siponen, 2011), only 12 of the 32 IS security training approaches reviewed include any kind of theory or theoretical concepts. Of these 12 theory-based approaches, six apply learning theories; six employ theories from the field of psychology or social psychology and one uses criminology. In this paper, we propose an information security training recommendation system based on risk perception.

The design and implementation of web-based e-learning recommender systems have grown exponentially during the last several years. In general, e-learning recommender systems have three types of filtering approaches which are content-based filtering, collaborative filtering and knowledge-based filtering (Chughtai, et al., 2013). In content-based filtering, the users/learners are recommended relevant items/learning contents that are similar to the ones they preferred in the past (Adomavicius and Tuzhilin 2005). In collaborative filtering, the users/learners are recommended relevant items/learning contents that other users/learners with the similar interest and preferences liked in the past (Pan, et al., 2010). Knowledge-based filtering approach generates a relevant recommendation based on matching users/learner’s needs, interests and preferences (Burke 2002). With this approach, the relationship between users’ needs and relevant recommended items can be explicitly modulated in an underlying knowledge base (Shishehchi, et al. 2011). There are also research studies on developing an approach that identifies learning styles automatically from learners’ behavior in an online course (Graf, et. al. 2010). Most of these studies focus on the recommendation techniques such as collaborative filtering, association rule mining and clustering to improve the accuracy of performance and result of filtering (Dwivedi and Bharadwaj, 2013; Vesin et al. 2013). The goal of these recommendation systems is to improve users’ knowledge level. The goals of our proposed system are not only to improve knowledge, but also to change users’ behavior.

Risk perception has been used to predict information security behavior (Vance, et. al. 2014). A primary theory used is Protection Motivation Theory (PMT) and related health-belief models (Rogers, 1975). PMT will be depicted in detail in the following section. In this paper we adopt risk profile from consumer choice theory.

**Research Model**

*Consumer Choice Theory on Individual’s Risk Profile*

Consumer choice theory has established that when individuals make consumption decisions, one of the key factors that drives their decision is their perception of risk. Indeed “Decisions about risk are always about choices among alternatives, each of which is characterized by a variety of relevant attributes, including those that describe associated risk” (Conchan, et. al., 2004, p 418). The decision by an individual to abide by or ignore systems security requirements can be framed in the light of making a choice. Consequently, the specific information and systems security choices selected by the individual and the laxity or exactitude with which these decisions are made, can be deemed in light of consumer choice theory.

Consumer choice theory posits that risk is situation specific but is also influenced by individual factors. These factors, as enumerated by Conchan, Zinkhan, Peters and Olavarrieta (2004), define an individual’s risk profile and include

- Risk affinity: an individual’s affinity or attraction to risk and risky situations;
- Risk acculturation: an individual’s prior exposure and acquaintance to risk;
- Human motives: an individual’s motives or goals when engaging in risky undertakings or high-risk situations, and
- Sensation seeking trait: an individual’s thrill-seeking trait or an individual’s affinity to “adrenaline-enhancing” experiences, and
- Ambiguity intolerance: The trait that assesses or deals with an individual’s dislike of unclear, ambiguous and unstructured-problem situations.

Risk is also conceptualized as comprising of two key constructs namely uncertainty and consequences (Cox 1967; Grewal, et. al. 1994). Uncertainty is the measure of the unknown or undeterminable outcomes. Consequences are the costs of the outcome or result of a risky decision. Within the context of information and systems security, uncertainty entails the measure of the unknown deleterious effects that may impact the user (or the system) as a result of behaving in certain ways (e.g. using a weak password). Consequences are the costs suffered by the individual user (or the system) owing to the system security behavior (e.g. the consequence of using a weak password may be theft of one’s identity – a user specific cost, or take-over of the system by a hacker – a system specific cost).

Consumer choice theory suggests that an individual’s risk profile has a bearing on how that individual assesses/ perceives uncertainty and also on how that individual assesses consequences that would accrue from a risky situation (Conchan, et. al. 2004). In this regard, Consumer Choice theory is in correspondence with Protection Motivation theory.

An individual’s choices pertaining to information security could mitigate or enhance the user’s and/or the system’s exposure to unfavorable/costly outcomes. Further, the individual’s choices pertaining to information security are influenced by the individual’s risk profile. Given that these individual choices are a function of the individual’s risk profile, it becomes important to determine the individual’s risk profile in order to provide effective security training interventions – interventions that hopefully alter the individual’s assessment of risk uncertainty and consequences and improve his or her capability to make better information security choices. Hence we hypothesize that (see Figure 1):

H1: Training customized by risk profile has a positive impact on individual’s assessment of risk uncertainty.

H2: Training customized by risk profile has a positive impact on individual’s assessment of risk consequences.

**Information Security Behavior**

An individual’s compliance or reaction to information security protocols can be deemed to be informed by the individual’s protective behavior. A leading theory that examines individual’s protective behavior is the Protection Motivation Theory (PMT). Originated by Rogers in 1975, PMT seeks to explain people’s fear appeals and how people cope with them (Rogers 1975). 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). Protection motivation stems from both the threat appraisal and the coping appraisal. The threat appraisal assesses the severity of the situation and examines how serious the situation is. The coping appraisal is how one responds to the situation. The threat and coping appraisal variables combine in a fairly straightforward way, although the relative emphasis may vary from topic to topic and with target population.

The threat appraisal process consists of both the severity and vulnerability of situation. It focuses on the source of the threat and factors that increase or decrease likelihood of maladaptive behaviors (Plotnikoff and Ronald, 2010). The total amount of threat experienced is the sum of the perceived severity and perceived vulnerability.

**Perceived vulnerability (PV)** refers to an individual’s assessment of the probability of threatening events. In this paper, it refers to the trainee’s assessment of the probability of security breaches.

**Perceived severity (PS)** refers to the severity of the consequences of the event. In this paper, it refers to the trainee’s assessment of the severity of security breaches.
The coping appraisal consists of the response efficacy, self-efficacy, and the response costs. It 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). The amount of coping ability that one experiences is the combination of response efficacy and self-efficacy, minus the response costs.

**Response efficacy (RE)** is the perceived effectiveness of the recommended behavior in removing or preventing possible harm. In this paper, it refers to the trainee’s assessment of various security protection methods and software.

**Self-efficacy (SE)** is the belief that one can successfully enact the recommended behavior. In this paper, it refers to the trainee’s ability to apply appropriate methods and software to protect security.

**Response costs (RC)** are the costs associated with the recommended behavior. In this paper, it refers to the monetary, time, and efforts expended in applying appropriate methods and software to protect security.

In this study, we employ PMT to capture an individual's security behavior both before and after receiving information security training. We envision the individual’s assessment of risk uncertainty and consequences enhance their competency in assessing vulnerabilities that may be exposing themselves to, severity of those vulnerabilities, the cost of responding to the vulnerability, the effectiveness of their response to the vulnerability and their self-confidence concerning responding to perceived vulnerabilities. Hence we hypothesize that (see Figure 1):

**H3:** Individual’s assessment of risk uncertainty has an impact on his/her threat appraisal (PV and PS).

**H4:** Individual’s assessment of risk uncertainty has an impact on his/her coping appraisal (RE, SE, and RC).

**H5:** Individual’s assessment of risk consequences has an impact on his/her threat appraisal (PV and PS).

**H6:** Individual’s assessment of risk consequences has an impact on his/her coping appraisal (RE, SE, and RC).

![Figure 1. Research Model](image)

**Methodologies**

A survey questionnaire will be used as pre-training assessment to determine a trainee’s risk profile, risk assessment and security behavior. Objective hands-on exercises will also be used to evaluate trainee’s threat appraisal and coping appraisal. The trainees will be separated into a treatment group and a control group. The trainees in the treatment group will receive training customized by individual's risk profile, while the trainees in the control group will receive common information security training not customized by individual’s risk profile. After the training process the trainees in both groups will receive post-training assessment on risk assessment and security behavior similar to the one used in pre-training assessment. The results obtained from both pre-training and post-training assessment will also be used to evaluate the effect between risk assessment and information security behavior.
Future Works

The future work of this project will be to design and construct a prototype of the LBPISL Recommendation System. The LBPISL recommendation system will be an online software that can be used as a tool for self-paced e-learning or a supplement to the traditional information security courses. Past research indicates that risk and learning style remain untapped as factors for developing education specific recommendation systems. Consequently, in our system, the recommendations will be based on the learners’ competence, learning styles, security behavior weaknesses and risk profiles.

Upon successful development of a prototype of the system, we plan to test its efficacy using survey-collected as well as actual-usage generated data.

References


