A Theoretical Model for Customizable Learning/Training to Enhance Individuals’ Systems Security Behavior

Submission Type: Emergent Research Forum Papers

Peter Meso
Georgia Gwinnett College
pmeso@ggc.edu

Shuting Xu
Georgia Gwinnett College
sxu@ggc.edu

Yi Ding
Georgia Gwinnett College
Yding1@ggc.edu

Abstract

This paper presents a theoretical model for providing individually customized systems security education. It integrates theories on individual's protective/compliance behavior (Protection Motivation Theory), individual's competency (Dreyfus’ Five Stage Knowledge Acquisition Theory), individual's learning behavior (Learning Styles theory), and individual's risk behavior (consumer choice theory) to establish customized learning experiences for each individual. It is presented as an “emergent-research-forum-paper” reporting research that is still in progress.

Introduction

There is a broad consensus that our current and future workforce needs to be trained and educated effectively to deal with present, emergent, and future cyber security challenges. Currently, information security education and training are provided in a variety of avenues, including traditional lectures, hands-on exercises, real world simulations, online training, emails on security tips and updates, etc. However, the question of which combination of learning materials and instruction-strategy yields the best educational and security behavior outcomes for a specific student, remains unsolved.

As information security training is the most common method to improving security behavior (Puhakainen and Siponen 2010), 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 approaches, security awareness program approaches, process approaches, situational approaches, social engineering preventive approaches, and computer-based training approaches. 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 a theoretical model that combines learning theory, psychological theory, individual's competency and risk behavior to develop an individually customized security training system.

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 indicate that systems security competence and an individual's risk profile are important variables that influence one's security behavior too (Dreyfus, 1980; Kogan and Wallach, 1964; Weber, et. al. 2002). Therefore, realizing that there may be more to developing effective pedagogy for information and systems security awareness, we propose a theoretical model for providing individually customized systems security
education. Our aim (future work) is to implement the model as a Learner Profile Based Information Security Learning (LPBISL) Recommendation software application and empirically test its efficacy. However, this paper limits itself to presenting the conceptual theory-based model that forms the basis of the LPBISL system and requisite hypotheses that we seek to test in order to empirically validate the efficacy of this approach to providing information and systems security learning to college students. It is presented as an “emergent-research-forum-paper” reporting research that is still in progress.

**Theory-Based Conceptual Model and Hypotheses**

In higher education, information security awareness has been one of the major themes that make up college level Information Systems (IS) education courses (e.g., Baltzan 2012, Kroenke 2013, Stair and Reynold 2012). Many of those IS courses covering security topics such as malware, identity theft, password-based authentication, firewall, wireless security, etc. often follow traditional lecturing approaches, which typically rely on selected textbook materials, lecture slides, papers, group discussions, etc. Students’ learning outcomes are comprehended based on their performance on “paper-based and theoretical” assignments or tests (Vigna 2003). However, the effectiveness of such an approach has been questioned. Researchers have argued that traditional lecturing often leaves “students with little understanding of application of concepts” in a real-world scenario (Riskowski et al. 2009). In industry, a similar question exists for the effectiveness of various information security awareness training programs. In many organizations, information security awareness training is considered as one of the major countermeasures for effective information assurance (e.g., Schou et al. 2004; NIST 2002). Yet, users who get trained often choose to ignore what is recommended in the training programs when they return to their practices in a real world setting (Cone et al. 2007).

In the fields of science and technology, hands-on based training has been promoted as a key tool for achieving effective learning of scientific and technological subjects (Ma and Nickerson 2006; Meso et al. 2013). As many information security topics such as malware, password cracking, hacking, etc. are technical in orientation, to improve the effectiveness of security awareness training, numerous hands-on based labs and projects have been proposed and discussed (e.g., Logan and Clarkson 2005; Hill et al. 2001; Ariyapperuma & Minhas 2005; Schembari 2007; Locasto & Sinclair 2009). While it is evident that numerous training instruments (e.g., labs, tools, simulation methods, etc.) have been developed to provide students with hands-on educational experiences (Du and Wang 2008, Shumba 2004, Stevenson and Romney 2004), most of those hands-on exercises are typically used for advanced level of security skill training (Meiselwitz 2008). For the general public, most of which has neither background nor interest in information security, it has always been a challenge to find an effective security awareness training method to motivate them to not only learn basic security principles well but also have a willing to apply those principles in a real world setting (Herath and Rao 2009, Maughan 2010).

Therefore, we aim at identifying mechanism by which effective individualized training of non-expert end-users of information and systems security can be accomplished in a comprehensive theory-driven manner. We propose to achieve this by integrating theories on individual’s protective/compliance behavior (Protection Motivation Theory), individual’s competency (Dreyfus’ Five Stage Knowledge Acquisition Theory), individual’s learning behavior (Learning Styles theory), and individual’s risk behavior (consumer choice theory) to establish customized learning experiences for each individual. Our aim is to help provide a solution to the challenge of offering learning materials that would fit the individual learner’s computer background and learning style so that the learner can most effectively acquire systems security knowledge. To the best of our knowledge, this is the first time that behavioral theories will be applied in developing an individually customizable system for information security education. We follow PMT principles to develop the security learning materials with focus on promoting appropriate perception of the security threats, their severity, and efficacy of coping response to best motivate learning and behavior changes of learners.

The overarching theoretical model for the project is provided in Figure 1. Detailed explanation of the model ensues.
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 (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010; Woon et al. 2005). A leading theory that examines individual’s protective behavior is the Protection Motivation Theory (PMT). PMT seeks to explain people’s fear appeals and how people cope with them (Rogers 1975). An individual’s protection motivation is said to stems from both the appraisal of pertinent threats and the appraisal of one’s ability to cope. Threat appraisal assesses the severity of the situation and examines how serious the situation is. Coping appraisal is how one responds to the situation (Plotnikoff and Ronald, 2010). We employ PMT to capture an individual’s security behavior.

Risk Profile:

According to Consumer Choice Theory, risk is one of the key factors that drives an individual’s consumption decisions (Arnett, 1994; Budner, 1962; Cox 1967; Fischhoff et al., 1990; Grewal et al, 1994). The decision by an individual to abide by or ignore information security requirements can be framed in the light of making a risky consumption decision (Chen and He, 2003). If all goes well, the user gets access to the information system or other system-specific benefit that may be under consideration. If things do not go as expected, the user suffers some loss which may be as minor as not gaining access to a system or as grave as permanently losing valuable data-files. Consequently, the specific information security choices selected by the individual and the laxity or exactitude with which these decisions are made, can be deemed to be influenced by an individual’s risk profile. This being the case, then one's risk profile may have a bearing on how they perceive information systems threats and how they perceivably cope in the event of such threats. Said otherwise:

H1: An individual’s risk profile has a positive influence on his/her security behavior within the context of using an information system
**Level of Competence:**

Individuals who do not have adequate training on the relevance and value of security in computational environments and/or on the value of protecting and securing their personal data and digital assets may not behave as expected or comply to the requisite requirements for secure computing when accessing, working in or using a secured computation environment (Ding et al., 2014). Also, an individual’s security competence has an impact on the individual’s ability to appraise the severity of a threat and also the individual’s coping-appraisal capabilities. Given that, according to PMT, threat appraisal and coping appraisal are the key determinants of an individual’s security behavior, we hypothesize that:

H2: An individual’s information and systems security competence positively influences his/her security behavior
**Systems and Security Awareness Training:**

We see training as enhancing an individual’s systems security behavior. There are three fundamental elements that we posit should be considered when developing training regimens for individual users.

The first is the individual’s current level of competence. According to Hubert Dreyfus and Stuart Dreyfus (1986) five stages model of knowledge acquisition, individuals can be classified as novices, advanced beginners, competent, proficient, or experts. The objective of training is to elevate an individual through the stages from the novice stage and hopefully into the expert stage. Consequently, an individual’s initial level of expertise is an important factor in determining how he/she ought to be trained. In order to maximize the efficacy of training, the training regimen to be provided to an individual should match the individual’s level of expertise/competence and allow for the systematic advancement of the individual up the ranks of expertise/competence. Therefore, we hypothesize that:

\[ H_3: \text{The alignment of training-material with individual's pre-training competence will have a positive impact on the efficacy of training.} \]

The second is the individual’s risk profile. Consumer choice theory posits that an individual’s choices are influenced by the individual’s risk profile (Arnett, 1994; Budner, 1962; Conchan et al. 2004). Given that individual choices concerning systems security have consequences to both the individual and to the organization operating the secured computing environment a training program that capitalizes on the individual’s specific risk-profile signature in order to provide the right combination/configuration of security training intervention may most effectively alter the individual’s perception of risk, or enhances the individual’s capability to make more rational and fact-based assessment of risk thereby affording him or her the capability to make better information security choices. Thus we hypothesize that:

\[ H_4: \text{An individual’s risk profile has a positive impact on the efficacy of the training s/he receives} \]

The third is the individual’s learning style. Several theories in the discipline of education point to the fact that individuals learn differently and that learning should be customized to match an individual’s learning style (Felder and Soloman, 2014; Kolb, 1984). We plan to employ the Barsch Learning Styles Inventory (BLSI) (Barsch, 1980) to assess and classify individuals according to their learning styles. While we do not envision an individual’s learning style as having a direct bearing/impact on their information security behavior, we envision it as having a mediating effect. This training in turn influences the information security behavior of the individual. Hence we hypothesize that:

\[ H_5: \text{An individual’s learning style has a positive impact on the efficacy of the training s/he receives, and} \]

\[ H_6: \text{Security Training has a positive influence on an individual’s security behavior} \]

Further, we posit that a customized security training regimen, that is training that factors in the individual’s learning style, risk profile and current level of information and systems security competence, will be much more effective at enhancing an individual’s security behavior than a non-customized security training regimen.

\[ H_7: \text{Customized security training is more effective than non-customized security training in enhancing/altering an individual’s security behavior} \]

**Methodologies:**

A survey questionnaire will be used as pre-training assessment to determine a trainee’s knowledge level, security behavior, risk profile and learning style. The expected knowledge level and security behavior is predefined based on the security learning objectives and outcomes. The trainee’s survey results will be compared with the expected knowledge level and security behavior to determine the trainee’s knowledge gap and the behavior expectation gap. The combination of the evaluated gaps, trainee’s risk profile and learning style will lead to the selection of the training module for the specific trainee. After the trainee completes the selected training module, s/he will receive a post-training quiz/test to assess the amount of individual-level learning that occurs during the training. Similar questionnaires used in pre-training...
assessments will also be used for post-training assessment to determine if the user has met the learning objectives or not. If the learning objectives are not achieved, the system will generate a new round of training process based on the post-training assessment results. The proposed hypotheses will be evaluated using the data collected from pre-training and post-training assessments.

Future Work:

The next step in this project will be to design and construct a prototype of the LPBISL Recommendation System. We envision LPBISL recommendation system to 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. The design and implementation of web-based e-learning recommender systems have grown exponentially in the last years. In general, e-learning recommender systems have three types of filtering approaches. These are (a) content-based filtering, (b) collaborative filtering and (c) 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 focusing on developing an approach that identifies learning styles automatically from learners' behavior in an online course (García, et. al. 2007; 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). 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


