The Misunderstood Link: Information Security Training Strategy
Emergent Research Forum (ERF)

Henry G Torres
Arkansas State University
htorres@astate.edu

Saurabh Gupta
Kennesaw State University
sgupta7@kennesaw.edu

Abstract

Insecure user behavior and failure to identify phishing is a leading cause of information security breaches triggering increased company costs in keeping information secure. Training employees toward secure information systems (IS) behavior is a way for organizations to attempt keeping information secure. Herein we outline how using traditional goals for information security training is a contributing factor to continued rise of insecure employee behavior. We posit that the approach to information security training recommended in extant literature is failing because of focus on improving skills in procedural, policy, and compliance activities. We propose a model suggesting alternative goals and draws propositions regarding its effectiveness. The model is of interest to investigate if using a training design that includes goals/inputs matching tools and users, a training process matching inputs to methods, and knowledge transfer outcomes emphasizing affective and meta cognitive learning, has a positive impact on secure behavior when using IS. The paper presents a design science model for a training strategy regarding information systems secure behavior.

Keywords
Information security, training, information security training, security education training, information security training strategy, training strategy, phishing, security awareness, SETA, design science.

Introduction

Employee secure behavior is the first line of defense and the most important information security guard for organizations (BakerHostetler, 2017; Laberis, 2016). Insecure user behavior when dealing with information systems (IS) can lead to unauthorized access of confidential corporate data, personal identifiable information, credit card numbers, and other financial information. Common forms of unauthorized access causing information security breaches are phishing, network penetration, hacking, malware, viruses, and ransomware (Johnston & Warkentin, 2010). Security incidents from insecure user behavior and negligence such as failure to recognize and prevent risks by phishing and social engineering attacks increased from 62% in 2015 to 70% in 2016 and cost at average $207,000 per incident (Ponemon, 2017). Such access is the leading cause of worldwide data breaches since 2005 as reported by the Privacy Rights Clearinghouse (“Data Breaches,” 2017).

Training employees towards secure behavior has been one of the primary ways organizations are trying to keep their information systems secure (Jensen, Dinger, Wright, & Thatcher, 2017). Researchers argue that use of information security education, and training can help emphasize and improve secure and protective motivated behavior (Al-Omari et al., 2012; Boss et al., 2015; D’Arcy et al., 2009; Posey et al., 2015). The key assumption behind the training approach towards secure behavior is that such training is similar to previous end-user training; consequently, findings from the said literature are applicable there. Skills training in information security preventative applications and compliance techniques are key focus areas sought by participants in the SIM 2017 IT trends study (Johnson et al., 2017). Despite the increase in IT budget spending on information security and the increased focus on security training (Siponen, Baskerville, & Heikka, 2006), information security incidents continue to rise (Ponemon, 2017). An important intervention to improve end user secure behavior is security training (D’Arcy et al., 2009; Jenkins et al., 2016; Puhakainen and Siponen, 2010). However, employee secure behavior is different from end-user
The Misunderstood Link: Information Security Training Strategy

training in three critical ways. First, traditional training is focused on enhancing individual job/task performance (Dubois & Rothwell, 2004) such as users being trained to integrate the mail merge feature in MS Word to improve processing time when dealing with mass mailings of individualized form letters. Thus, the motivation is to improve personal performance. Secure behavior, on the other hand, helps enhance either the organizational or IT departments’ performance and does nothing to enhance short term individual performance. As a matter of fact, following secure behavior protocol may instead degrade performance and be viewed as a nuisance or as interruptive behavior decreasing performance (Jenkins et al., 2016). Second, traditional technology training has generally been targeted and focused on its functionality and specific skill development instead of its underlying concept (Olfman et al., 2006). In cases of IS security, however, employees, due to lack of awareness, might have to deal with threats (intrusions) that may not be part of the current training protocol (Ayyagari & Figueroa, 2017). Finally, outcomes of traditional technology training tend to be imminently used such as a webmaster being trained to embed a ready to watch video on a webpage. Imminent technology training is increasing with the movement towards just in time and on the job training (Jungck, 2011). Secure behavior training might have to focus on non-imminent threats. Consequently, we postulate that despite the skills training, studies indicate the training that companies are doing to combat employee error and negligence are not enough (Curry, 2016; Hatch, 2016; Ponemon, 2017).

The objective of this paper is to present a design science model for a training strategy regarding information systems secure behavior. The model argues that the focus on traditional training goals for information security training is a contributing factor to the continued rise of insecure employee behavior. We posit that the approach to information security training as depicted and recommended in extant literature is failing because it is focused on improving employee skills in procedural, policy and compliance activities. To address this, we utilize a design science approach that builds on a three-stage process that initiates goals towards outcomes, via a thorough training process, ending with post-training evaluation (Olfman et al., 2006). The proposed model suggests alternative goals and draws propositions regarding its effectiveness.

Literature Review

A literature review of extant studies pertaining to IS security training was conducted using the Webster and Watson (2002) literature review article as a guide. The structure of the review emphasized concept-centric studies on information security training and information security behavior. This review of empirical studies highlights the Olfman et al., (2006), framework described herein that uses an overall training and learning process that includes three stages: (1) initiation, where goals and outcomes are identified towards building a training strategy, (2) training and learning, where the training process occurs, and (3) post-training, where outcomes/measurement of success occurs. To further solidify this framework a design science research approach will be applied that includes rigorous measures and evaluation.

Goals

Training goals can be categorized into four areas. Skill, cognitive, affective, and meta-cognitive. Training for skills focuses on procedural knowledge and the how to; training for the cognitive is focused on building broader knowledge of the subject; training for affective learning focuses on the level of immersion into the subject; and meta-cognition training focuses on the trainees’ ability to understand their own inner processing procedure to learn (Gupta and Bostrom, 2009). The reviewed literature shows that nine of the eleven studies used in this presentation focused on skill training and cognitive learning towards policy and procedures. All of the studies had a singular focus and approach to training towards achieving the specific goal. None of the literature emphasized or contained a strategy towards an overall training approach.

Training

Training can be defined as a common method to enhance productivity of employees and to communicate organizational goals to them (Gupta and Bostrom, 2006). All of the studies focused on a specific training intervention directed towards achieving the specific goal and did not include a strategy towards an overall training process. In the area of training process and type, the studies organized their training process paired with a training type to achieve the desired outcome. None of the studies considered the trainee
characteristics and their matched training tools to identify a specific training process or training type via use of a training strategy. The studies did not consider identifying the type of training tools matched to the characteristics of the trainee to determine the best training process and type to apply.

Outcomes

In the area of training outcomes, the studies focused on improving secure behavior or specific cognitive knowledge building. None of the studies considered affective or meta-cognitive knowledge-based outcomes via use of a training strategy. The studies did not consider identifying outcomes focused on improving affective states such as attitude and meta-cognitive knowledge to learn self-efficacy techniques for preventing information security incidents. Essentially, the literature review points to the absence in extant research of using an overall information security training strategy that considers goals/inputs (matching tools and users), training processes (matching inputs to methods), and outcomes (emphasizing affective and meta cognitive learning).

Approach

Summarizing the gaps found in the literature review, we note the lack of emphasis in a formal design science theory in that all of the studies had a singular focus for training towards achieving a specific goal. None of the literature emphasized or contained an overall training strategy approach. The studies did not consider identifying the type of training tools matched to the characteristics of the trainee to determine the best training process and training type to apply. The studies did not consider identifying outcomes focused on improving affective states such as attitude and meta-cognitive knowledge to learn self-efficacy techniques for preventing information security incidents. Hence, our rationale to emphasize a design science research approach that can bring focus to an overall training strategy will include as its goals to fill these gaps.

As an informing framework we will analyze, evaluate, and select one, or a combination of, educational learning theories for best fit in use with this approach. Taking a constructivist approach, we will emphasize cognitive and affective processes to address the end-user’s method to make choices via the humanistic theory (Schunk, 2012). During initial design stages of the approach, consideration will be given to the use of goal theory to explain and predict end-users achievement behaviors (Schunk, 2012). The end result will be an overall information security training strategy to conduct the training sessions.

We posit that this model will create an improved artifact solution that will contribute to design science research knowledge (Gregor & Hevner, 2013) in the form of an overall training strategy and process. The contribution type will be in use of a well searched and defined nascent design theory that utilizes knowledge as part of the operational approach to support our constructs (Gregor & Hevner, 2013). Attention to the method of building the artifact grounded in the sound theoretical three stage Olfman et al., (2006) framework will be highlighted with the respective assessment measurements for both pre and post application of each training experiment that is prescribed. As outcomes we will detail the incremental and gained useful knowledge and record all findings throughout the study for use in the publication of results.

In the next section we include the description of the theoretical and design science guidelines to achieve this model. In the concluding statements we include Figure 1 to depict a flowchart of this proposed DSR approach to create an information security training strategy.

Conclusion

The objective of this paper is to present a design science model regarding training in information systems secure behavior. The model argues that the focus on traditional training goals for information security training is a contributing factor to the continued rise of insecure employee behavior. We posit that the approach to information security training as depicted and recommended in extant literature is failing because it is focused on improving employee skills in procedural, policy and compliance activities. We propose to use the design science research guidelines by Hevner, March, Park, Jinsoo, Ram, and Sudha, (2004) that are described as follows embedded with how we will accomplish the proposed research.
Figure 1. DSR Approach to Create Information Security Training Strategy

Guideline 1: Design as an artifact – we will produce experiments to match a developed strategy for training. The artifact will be the design of a strategy highlighting the three stage Olfman et al., (2006) framework and will include experiments towards assessing the effectiveness of each stage incorporating: (1) initiation goals and outcomes, (2) the training and learning process, and (3) post-training measurement of success.

Guideline 2: Problem relevance – we will design the strategy that is relevant to the gaps identified herein such as identifying the type of training tools matched to the characteristics of the trainee to determine the best training process and type to apply. We will identify outcomes focused on improving affective states such as attitude and meta-cognitive knowledge to learn self-efficacy techniques for preventing information security incidents.

Guideline 3: Design evaluation – utility, quality, and efficacy of the training strategy will be measured for each of the three training strategy stages as defined above and will also include pre and post training assessments.

Guideline 4: Research contributions – by use of appropriate design methodology, we will provide clear and direct contribution to a verifiable solution. It is expected that gained incremental knowledge will be shared as significant contribution throughout the entire study from inception through completion.

Guideline 5: Research rigor – we will institute rigorous methods in constructing and evaluating the training strategy design.

Guideline 6: Design and search process – search of an effective training strategy will be completed by exhausting alternative training techniques to match the objective.

Guideline 7: Communication of research – after design, testing, and analyzing the results of the research, we will publish the findings in the appropriate journal for both researchers and practitioners.

This approach suggests alternative goals and draws propositions regarding its effectiveness. We present a solid case for future research that can assess how information security behavior is influenced by an overall training strategy and what impact this can have on information security practices. This proposition has the potential to extend the research on information security training. To our knowledge no prior information security training studies have utilized design science and a complete and overall training strategy model.

This proposed study provides additional substance to researchers with interests in both information security behavior and information security training. There is an opportunity to introduce a novel approach in information security training research by examining how an overall information security training strategy might impact information security behavior and it may prove to be the misunderstood link.

REFERENCES


Jenkins, J. L., Durcikova, A., & Burns, M. B. (2012). Forget the fluff: Examining how media richness influences the impact of information security training on secure behavior (pp. 3288–3296). IEEE.


*The Misunderstood Link: Information Security Training Strategy*