ABSTRACT
This research examines the impact of information systems security training upon non-malicious insiders at various organizational levels. The transfer of knowledge attributed to these training programs will be evaluated utilizing both quantitative and qualitative methodologies including a simulated phishing attack.

KEYWORDS: Computer security, Employee training, Phishing

INTRODUCTION
Information systems security is a severe and ongoing concern (Ledin, 2011). Organizations are faced with the constant challenge of making information available to employees and other stakeholders while simultaneously safeguarding that information from inappropriate access, deliberate and accidental misuse, and unintentional release. These attacks can be deliberate or accidental, and may come from inside or outside the organization. Multiple approaches to information systems security have been explored; these range from technical approaches to behavioral approaches (Trcek, Trobec, Pavesic, & Tasic, 2007). Most of these efforts target malicious individuals (Trcek, Trobec, Pavesic, & Tasic, 2007).

LITERATURE REVIEW
Unintentional Release of Confidential Data and Computer Usage Policies
Extant research suggests that more organizations face data loss caused by non-malicious insiders than from malicious attacks (PricewaterhouseCoopers, LLP., 2013). Despite the lack of malicious intent from these insiders, the release or loss of data is still a serious threat and must be addressed by organizations. Although technical security approaches such as passwords and encryption are very effective against many types of attacks, these unintentional releases of data are often the result of phishing and social engineering attacks in which the insider is simply tricked into releasing confidential data by visiting a web site or sharing passwords or other data with another person. In cases such as this, technical security is nearly worthless: the person causing the harm has full access to the data! Examples of these phishing or social engineering attacks include the receipt of emails that appear to come from a trusted friend, coworker, important person, contest or publication, or another legitimate source. These emails often attempt to convince the recipient to open an attachment, download a file, or visit a website. These actions compromise the targeted computer and thus any network to which the device is
connected (Friedman & Hoffman, 2008). As a result, organizations must rely upon behavioral security: an attempt to change the behavior of the individuals through some combination of organizational policy and training (Workman & Gathegi, 2007; Sasse, Brostoff, & Weirich, 2001; Bresz, 2004).

Organizational computer usage policies are often considered the cornerstone of computer security (Backhouse & Dhillon, 1995); however, if individuals are unaware of or do not understand these policies, then the policies become worthless. Extant literature suggests that individuals within organizations are not familiar with policies—they’ve either never read the policies or only read them once and simply don’t recall what the policies said (Foltz, 2000; Cronan, Foltz, & Jones, 2006).

**Security Training**

One possible solution to this issue is training. Training is a way to provide information to individuals such that they have a better understanding of the importance of information systems security— and their role within information systems security—within the organization (Workman & Gathegi, 2007). Unfortunately the impact of training upon information systems security has not been well researched. Little research has examined the various approaches to training or the impact of training on security awareness. Factors contributing to the success or failure of training to enhance information systems security awareness have not been well evaluated (Bulgurcu, Cavusoglu, & Benbasat, 2010). For example, what types of training are best? Is a single training session sufficient, or should training be repeated frequently? Are employees able to utilize their training in new situations? How effective is current training (if it even exists)? Answers to these questions will help us provide better security for organizations.

Organizations approach training in a variety of ways including lecture style, group discussion, and computer aided training. 74% of organizations that have corporate ethics training programs, in general, utilize computer based trainings; however, the effectiveness of this training may be questionable (Weber & Wasieleski, 2013). Organizations also commonly use lecture style (48%), group discussion (55%), and group discussion of case studies (39%) (Weber & Wasieleski, 2013).

**Training for Transfer**

In order for security training programs to be effective, the employees receiving the training must be able to apply the information they have learned when they encounter a security threat. Training programs often attempt to enable an individual to adapt and to apply their limited learning to other settings, issues and problems. This is transfer (Wiggins & McTighe, 2006). “Transfer involves figuring out which knowledge and skill matters here and often adapting what we know to address the challenge at hand” (Wiggins & McTighe, 2006), p. 41.

According to (Council, 1999), key components for learning are achieving a sufficient threshold of initial learning, utilizing a “deliberate practice” with feedback rather than “time on task”, learning rather than memorizing, employing a variety of learning contexts, developing flexible understanding of when, where, and why to use knowledge, learning about the new domain first and then grasping knowledge quickly, and leveraging trainee strengths.
Transfer best occurs when the training leverages strengths that students bring (Wiggins & McTighe, 2006). In order to transfer knowledge, learners have to achieve a sufficient threshold of initial learning (Wiggins & McTighe, 2006; Broad, 1992). Security courses are often taught by IT representatives who have great knowledge in the area of security but not in the area of teaching. Experts in a topic can have difficulty breaking the concept into component parts. “Instructors often have “blind sights” to what they think learners know coming into the training” (Wiggins & McTighe, 2006), p. 45. As such, the training presentations may begin at a different level than the threshold of initial learning that trainees bring with them to the learning experience. Trainings can be improved if the students have a way to begin the training with their own, perhaps incorrect, assessment and contrast that thinking with others (Bransford & Schwartz, 2001).

Transfer also requires a training approach that utilizes a “deliberate practice” with feedback rather than “time on task” (Wiggins & McTighe, 2006). Training taught by problem-solving is more likely to be utilized than memorizing simple facts (Bransford & Schwartz, 2001). Most organizations provide training through computerized systems (Weber & Wasieleski, 2013). These systems do not typically provide deliberate practice in avoiding security threats but require that trainees complete a module. Transfer seeks to enhance learning rather than memorizing (Wiggins & McTighe, 2006). If the goal is to pass the quiz at the end rather than to be informed about computer security, then trainees are less likely to engage in the process and learn. To enhance learning, examples should be concrete and realistic (Bransford & Schwartz, 2001). Contrasting examples also help trainees better understand the topic (Bransford & Schwartz, 2001).

Transfer suggests employing a variety of learning contexts. There is little evidence that organizations invest in this variety of training (Weber & Wasieleski, 2013). Similarly, transfer requires trainees to develop a flexible understanding of when, where, and why to use knowledge.

Assessing Training

Measuring a trainee’s ability to transfer helps trainers evaluate and improve their instruction (Council, 1999). Only 40% of organizations conducting general ethics trainings had a methodology to assess the effectiveness of their security programs (PricewaterhouseCoopers, LLP., 2013). Ideally students will “bump up against the world” in the assessment to test their training (Bransford & Schwartz, 2001). “Assessments of people’s abilities can be improved by moving from static, one-shot measures of ‘test taking’ to environments that provide opportunities for new learning” (Bransford & Schwartz, 2001). Few organizations are evaluating their training programs; and those who do are likely not using a realistic testing method that requires students to respond to a typical computer security threat.

Some companies are hiring outside firms to determine how employees will evaluate security threats. For example, “Password theft via fake websites (phishing) is wide spread” (Herzberg & Margulies, 2013) and some institutions are adding a fake phishing website to see which employees respond. The continued accidental omissions that lead to security threats suggest that security training programs may not be effective.
Organizational Responses to Training

Extant research suggests a concerning dichotomy in ethical and security awareness based on individual position within the organization. Upper level managers often view their organizations as more ethical than mid-level or lower-level managers (Jin, Drozdenko, & Basset, 2007). This same variation can be observed in universities: administration, faculty, staff, and students have different understandings of ethics and also of information systems security (Jin, Drozdenko, & Basset, 2007).

Executives think that the most powerful inhibiting force to training is lack of involvement by top management (Broad, 1992). Being too centralized and too staff centric are also concerns. Finally, executives believe that programs are unrealistic and expect too much too soon. (Broad, 1992).

Trainers believed that training was unsuccessful due to lack of job enforcement, interference from work environment, a non-supportive organizational culture, trainees’ perception that it was impractical or irrelevant, trainees’ discomfort with change, trainee’s perception of poorly designed or delivered training and pressures from peers to resist change. (Broad, 1992). Many of these training barriers, such as lack of job reinforcement, are the responsibility of the manager. Organizational culture contributes to interference from immediate work environment, non-supportive culture, and trainees’ pressure from peers to resist training (Broad, 1992).

METHODOLOGY

This research will examine the perceived effectiveness of training at reducing non-malicious data disclosure by insiders at various levels and organizational influences on that training within a university setting. The research will also examine the actual effectiveness of training. Since the university already has a training program in place to explain correct and incorrect use of information systems by various stakeholders (administrators, faculty, staff, and students), randomly selected individuals at each level will be surveyed regarding their initial security knowledge, their annual security training time, their understanding of that training, their understanding of the provided training materials, and their contextual usage of that security training. These individuals will also be asked to evaluate their perception of overall effectiveness of the training and the organizational context in which the training occurs. A subset of these randomly selected individuals will receive (at a random time) an email containing a phishing attack: basically the users will be invited to follow a link. The hyperlink will lead to a second (online) survey which will explore why the person failed to recognize the phishing attack.

HYPOTHESES

H1. Employees that engage the phishing scheme will report less initial knowledge regarding security than employees that do not engage the phishing scheme.

H2. Time spent on annual security training will not be significantly different between those who phish and those who do not.

H3. Employees who phish will be more likely to report simply completing the security questionnaire without reading for content than employees who do not.
H4. Employees who phish will be less likely to report using security in a variety of contexts than employees that do not phish.

H5. Employees who phish will report a lesser understanding of the training materials than employees that did not phish.

H6. Upper level managers are more likely than lower level managers to believe that employees will act ethically regarding security.

H7: Executives are more likely to think that the most powerful inhibiting force to training is lack of involvement by top management.

H8: Executives are more likely to think that training is too centralized as compared with other employees.

H9: Executives are more likely to think that training programs were unrealistic as compared with other employees.

H10: Employees that phish are more likely to perceive the security training as impractical and/or irrelevant.

H11: Employees that phish are more likely to perceive that the training was poorly designed or executed.

H12: Employees that phish are more likely to report a lack of training reinforcement on their job.

There will be a qualitative analysis of the results of why the employee phished to provide characterization and nuance to the survey results.

DATA COLLECTION AND ANALYSIS

Data collection and analyses are anticipated for Fall 2015.

REFERENCES


