Kennesaw State University
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2016 KSU Conference on Cybersecurity Education, Research and Practice

# Training Decrement in Security Awareness Training

Tianjian Zhang
tj.zhang@okstate.edu

Zhang, Tianjian, "Training Decrement in Security Awareness Training" (2016). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 8.
https://digitalcommons.kennesaw.edu/ccerp/2016/Student/8

**Abstract**

This study determines if there is a decremental effect following IT security awareness training. In most security policy compliance literature, the main focus has been on policy design. Studies that address security awareness training are seldom theory driven and even fewer are empirically based. To fill this gap, we draw from the theory of vigilance decrement as well as forgetting curves in psychology, and propose a classroom experiment showing that participants' IT security awareness decreases over a 45-day period since the training at day one. The result adds to the security policy compliance literature and suggests that some policy violations are due to the decrement in vigilance and security knowledge. The practical implications are that companies need to train their employees repeatedly overtime in order to maintain a high level of IT security policy compliance.

**Disciplines**

Information Security | Management Information Systems | Technology and Innovation

**Comments**

This is a work in progress.

Keywords: security awareness, training, vigilance decrement, forgetting curve.

# SUMMARY[1]

Information security breaches have been a major issue for organizations. According to the 2011 Computer Crime and Security Survey by the Computer Security Institute (CSI), 41.1% of organizations experienced computer security breaches within the past year.

Many of the breaches are of non-malicious nature. The recent Ernst & Young's Global Information Security Survey suggests that careless or unaware employees is considered the leading security vulnerability. However, the same survey also reveals that at least 30% of the organizations have no security awareness training program. Other surveys suggest the percentage may be higher.

While the industry has recognized the lack of security awareness training, academia has yet to shift more focus towards awareness training. Most security policy compliance literature focus on the mechanism behind employees' intentions to comply. Studies that do address security awareness training are seldom theory driven and even fewer are empirically based. To fill the gap, we draw from the theory of memory retention in psychology, and propose a classroom experiment to show that *participants' IT security awareness decreases over time following the security awareness training*. This study suggests that even those with training programs do not necessarily prepare employees to deal with security issues in the long run.

Participants of the study are from three different sections of an introductory class in information systems in a large mid-western public university. Security knowledge will be measured by security awareness quiz results. On day 1, participants took an in class quiz (pretest) on security training. A week after the pretest, a lecture on security awareness was delivered by the course instructor to serve as the security awareness training. Immediately after the lecture, participants took quiz (posttest 1). Depending on which of the three class sections the students are in, participants will take a third in class quiz (posttest 2) 15, 30 or 45 days after posttest 1. We expect posttest 2 scores to be lower than that of posttest 1, and the difference to be positively related to the number of days in between. We will use repeated measures ANOVA to analyze the data. Prior studies have shown the amount of time it takes for knowledge to tend to 0 ranges from one to three weeks.

[1] Data collection is in process.

The longer time interval in this pilot study is to ensure we capture the decrement. Further studies will adjust the interval length accordingly.

Limitation of the study includes the use of student sample, and not measuring the effect of repeated training on knowledge retention. The latter is partly due to the time cost of repeated training in a classroom. The study will add to the security policy compliance literature suggesting that some policy violations are due to the decrement in security knowledge. The practical implications are that companies need to train their employees repeatedly over time in order to maintain a high level of IT security policy compliance.