Training Report

Effectiveness of Cybersecurity Training

Human Resources Division
& Jaclyn Martin, University of South Florida

Executive Summary

TxDOT partnered with Jaclyn Martin of the University of South Florida to examine the effectiveness of cybersecurity training using a quantitative framework called Signal Detection Theory (SDT). This study used organizational data in a quantitative study to demonstrate the effectiveness of adult training at TxDOT which revealed the following:

- TxDOT's current cybersecurity training changes employee email behavior.
- Participants who enjoyed training or found it useful did better at detecting phishing e-mails.
- "Fear Appeals" did not have an effect on detecting phishing e-mails.
- Signal Detection Theory fits employee email behavior at TxDOT.
- Higher intelligence (cognitive ability) correlates with lower phishing susceptibility.

Introduction

The Texas Department of Transportation (TxDOT) uses training interventions to mitigate risks for a variety of policy-based operations. Cybersecurity is a recent focus area among Departments of Transportation and has been an area of attention during at least the last two legislative sessions in Texas. As a result, legislation has been passed, training has been mandated, and policies have been enacted. However, the means for evaluating the effectiveness of training among adult learners in an active work environment have been limited. Contemporary adult learning theory uses the methods first outlined by Donald Kirkpatrick in 1959, but this widely accepted methodology relies heavily on self-reporting and subjective perceptions.

To address this gap, TxDOT partnered with a researcher at the University of South Florida to examine the effectiveness of cybersecurity training using a quantitative framework called Signal Detection Theory (SDT; Green & Swets, 1966). The research, conducted by Jaclyn Martin, was significant because this study used real organizational data in a quantitative study to demonstrate the effectiveness of adult training, moving TxDOT past the traditional "Level 1 surveys" to show that compliance training on cybersecurity is indeed effective.

This Training Report is a summary of Dr. Martin's findings as interpreted for TxDOT staff by the Workforce Development Section of the Human Resources Division (Martin, 2019).

Background

Organizations recognize that employees who use the organization's information technology systems must be trained on the knowledge, skills, and policies related to cybersecurity (Beyer & Brummel, 2015), but only 54% of information security professionals have been able to quantify a reduction in phishing susceptibility based on their training (Wombat Security Technologies, 2018). One type of training used to reduce phishing susceptibility includes providing informational training ranging from simple lists of internet tips, to cartoons that help explain tips in a story format (Anti-Phishing Phil; Sheng et al., 2007), all the way to game-based phishing training that sends test e-mails to participants (PhishGuru; Kumaraguru et al., 2007). One successful avenue for training in cybersecurity research appeared to be through the use of *fear appeals*, or messages intended to scare employees by emphasizing the dangers in not following training recommendations (Tannenbaum et al., 2015).

For adult training, Baldwin and Ford (1988) created the most cited theoretical model of training transfer. According to their model, effective successful training transfer depends on both training inputs (trainee characteristics, training design, and work environment) and training outputs

(learning and retention). The trainee characteristics that have the greatest effect on training transfer are learning goal orientation, cognitive ability, negative affect, openness, self-efficacy, perceived utility, organizational commitment, and pre-training motivation (Baldwin & Ford, 1988). Related to the evaluation of training, the Kirkpatrick Method is a four level training evaluation model in use with most training organizations (Kirkpatrick, 1959). Level 1 surveys assess participant reactions to learning and contain questions about a participant's opinion about the utility of the training. Level 2 surveys assess learner comprehension and are typically end-of-course examinations. Level 3 assessments determine behavioral changes in the organizational environment after training has been completed, consisting mostly of surveys similar to the Level 1 surveys that are completed by the participant, and even supervisors, about 30-60 days after the end of a training event at TxDOT. Level 4 projects measure the organization's return on training investment and are largely a financial analysis exercise. At TxDOT, as with most organizations, execution of the Kirkpatrick Method relies heavily on Level 1 surveys and Level 2 "checks on learning" to demonstrate training effectiveness. In both cases, the Kirkpatrick method is not able to fully evaluate training transfer.

Signal Detection Theory (SDT) enables us to measure both sensitivity (e.g. a person's ability to discern phishing emails from real emails) and response bias (e.g. a person's tendency to be loose or cautious when evaluating emails as a threat). SDT distinguishes these two factors as separate because sensitivity is about distinguishing signal from noise, while response bias is about consequences (e.g. a participant can recognize a threat, but click on it anyways if they don't care about the outcome). In this manner, TxDOT's cybersecurity training ultimately seeks to optimize both sensitivity to cyberthreats and to optimize response bias among employees. Further, these factors can be measured before and after training events with SDT. In addition to SDT, this research looked at the individual factors identified by Baldwin and Ford that could impact the effectiveness of training. Trainee characteristics, including demographics and intelligence, as well as the participants' perceptions of the training, were examined at all stages of this research.

Problem Statement, Purpose of the Study, & Significance

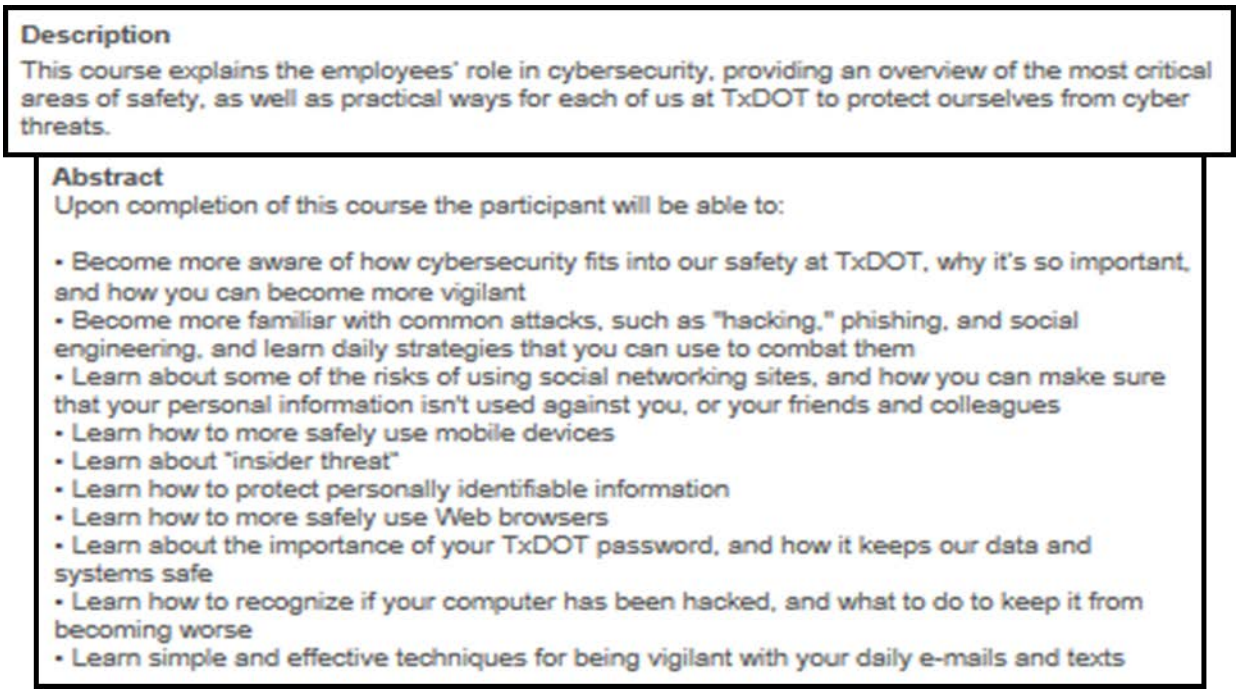
It is not known if TxDOT's mandatory cybersecurity training changes the behavior of its workforce. This study applied Signal Detection Theory in order to determine if TxDOT's training improved sensitivity to cyberthreats and/or increased caution in responding after assessing a cyberthreat in a convenience sample. This study also considered participant characteristics of demographics, job data, and cognitive ability to determine if statistically significant relationships existed between participant characteristics and training outcomes. This study was significant because it applied a robust theoretical model in an active workplace to evaluate the effectiveness of organizational compliance training.

Research Questions

This study had three research goals: the first goal was to evaluate the effectiveness of phishing e-mail training using informational approaches (e.g. traditional online compliance training) and *fear appeals*. The second goal was to distinguish between sensitivity and response bias in phishing susceptibility following training. The third goal was to understand if individual participant characteristics played a role in training outcomes.

Research Methodology & Design

During a three-month period, TxDOT employees coming due for annual cybersecurity training (EL8474, *Figure 1*) received an e-mail invitation to participate in a study with a link to both the pre-training assessment and post-training assessments, all hosted by the survey platform of Qualtrics. Participants were instructed to take the pre-training assessment, complete their training as normal in PeopleSoft, and then return to the e-mail to click on a link to complete the post-training assessment.



Description

This course explains the employees' role in cybersecurity, providing an overview of the most critical areas of safety, as well as practical ways for each of us at TxDOT to protect ourselves from cyber threats.

Abstract

Upon completion of this course the participant will be able to:

- Become more aware of how cybersecurity fits into our safety at TxDOT, why it's so important, and how you can become more vigilant
- Become more familiar with common attacks, such as "hacking," phishing, and social engineering, and learn daily strategies that you can use to combat them
- Learn about some of the risks of using social networking sites, and how you can make sure that your personal information isn't used against you, or your friends and colleagues
- Learn how to more safely use mobile devices
- Learn about "insider threat"
- Learn how to protect personally identifiable information
- Learn how to more safely use Web browsers
- Learn about the importance of your TxDOT password, and how it keeps our data and systems safe
- Learn how to recognize if your computer has been hacked, and what to do to keep it from becoming worse
- Learn simple and effective techniques for being vigilant with your daily e-mails and texts

Figure 1: Course description and training objectives for TxDOT's mandatory cybersecurity awareness training (EL8474), due within 90 days of hire and every year thereafter.

The pre-training assessment survey contained an informed consent, a phishing e-mail simulation, a request for demographic information, and a cognitive assessment. The phishing e-mail simulation contained 30 e-mails, 20 of which were legitimate and ten of which were phishing e-mails. After completing the pre-training assessment, participants completed the cybersecurity training (EL8474) in PeopleSoft as normal. After completing training, participants then took a post-training assessment that contained a randomly assigned *fear appeal* (strong, weak, and none). These fear appeals were designed to manipulate employees' perceptions of what might happen if they fell for phishing e-mails (adapted from Jansen, 2018). At the end of the fear appeal message, the respondent answered two questions to evaluate the individual impact of that message. Participants then completed the final post-training assessment, which contained both a phishing e-mail simulation and Level 1- type questions about the training itself (Kirkpatrick, 1959).

Descriptive Data

The target population was a subset of TxDOT employees who were within 90 days of becoming past due for annual cybersecurity training over a 2 month period. Based on those parameters, there were 1,714 TxDOT employees in the target population from among the total population of about 12,000 employees. Employees were encouraged to participate and responses were anonymous, with no penalty for choosing not to participate. A sample size of 100 was targeted using G*power (Faul, Erdfelder, Buchner, & Lang, 2009). This recruitment strategy resulted in a sample of 248 respondents who completed the pre-training survey and 174 respondents who completed the post-training survey. Duplicate and partial responses were removed. The final sample of respondents that completed all tasks was 139. About 50% of participants came from Engineering, Engineering Support, and Maintenance Operations. Over 60% were District employees from rural, urban, and metro Districts. Over 70% reported they typically spent less than 2 hours per day on e-mail.

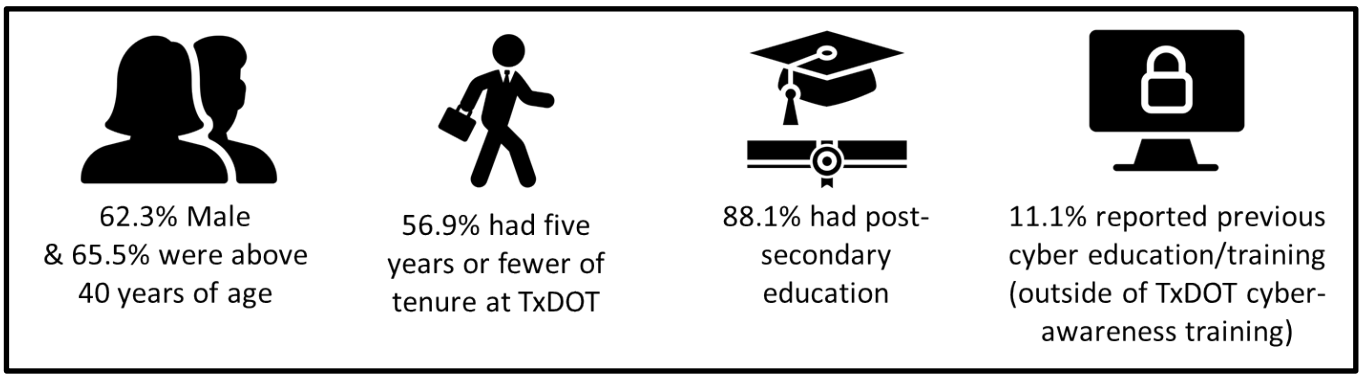


Figure 2: Select sample demographics (Martin, 2019).

Results & Findings

This study had three research goals: the first goal was to use the Signal Detection Theory framework to evaluate the effectiveness of phishing e-mail training using both informational approaches and *fear appeals*. The second goal was to distinguish between sensitivity and response bias in phishing susceptibility following training.

Based on the comparison of this data set and what was predicted by SDT, this framework appeared to fit the data well, which may mean that SDT could be useful in measuring the effectiveness of future training or other business process interventions at TxDOT. Based on the good fit of SDT, results showed that informational approaches to training (e.g. traditional online compliance training) were effective in getting participants to detect phishing e-mails. Results showed there was a significant difference in detection ability (sensitivity) after training, but there was no difference in what participants did after assessing the threat (response bias). In both cases, receiving a fear appeal (strong or weak) did not change phishing e-mail detection ability or what the participants did after they detected the phishing e-mail. It is possible that the fear appeal intervention was not strong enough to manipulate response bias, or that participants recognized the exercise as a training event without consequences.

The third goal of this research was to understand if individual participant characteristics played a role in training outcomes. While no other demographic information correlated to differences in training outcomes, intelligence (cognitive ability) correlated positively with phishing e-mail detection. Additionally, individual attitude, as shown in Level 1 survey results, about the usefulness and enjoyability of the training, did predict changes in phishing e-mail detection. However, just like the fear appeals, individual attitudes did not change what participants did after detecting the phishing e-mails (response bias).

Summary, Conclusions, & Recommendations

TxDOT's current cybersecurity training changes employee email behavior.

- TxDOT's current cybersecurity training meets its current objectives for cybersecurity awareness.
    - Given the lack of change in response bias, TxDOT should consider further research targeting response bias and consider changes to training that emphasize the actions to be taken after assessing email threats.
- Pre and post-test training evaluation strategies showed training effectiveness.
- Individual attitudes about training correlated with training success.

"*Fear Appeals*" did not have a significant effect on cybersecurity tasks.

- Attempts to scare employees into taking phishing e-mails more seriously did not appear to have any impact on the ability to correctly detect or respond to phishing e-mails.

Signal Detection Theory fits employee email behavior at TxDOT.

- SDT is a model that quantifies both sensitivity to stimuli and the attitude towards the responses to those stimuli.
- SDT should be considered for future program evaluation as well as training evaluation.
- SDT may have applications at TxDOT in behavioral traffic safety operations, customer service, public outreach, and media relations.

Higher intelligence correlates with lower phishing susceptibility.

- Intelligence (cognitive ability) is a known and consistent predictor of job performance that is frequently used as part of selection processes in other organizations.
- Subsets of cognitive ability, such as selective attention, may also help in identifying those who would benefit most from additional phishing training without having to administer a full cognitive assessment.

For further questions about this report or the research, please contact the Workforce Development Section of the Human Resources Division at: training@txdot.gov.

References

Alliger, G. M., Tannenbaum, S. I., Bennett Jr, W., Traver, H., & Shotland, A. (1997). A meta-analysis of the relations among training criteria. *Personnel Psychology*, *50*(2), 341–358. https://doi.org/10/dn84s7

Baldwin, T. T., & Ford, J. K. (1988). TRANSFER OF TRAINING: A REVIEW AND DIRECTIONS FOR FUTURE RESEARCH. *Personnel Psychology*, *41*(1), 63–105. https://doi.org/10/cq3btj

Beyer, R. E., & Brummel, B. J. (2015). *Implementing Effective Cyber Security Training for End Users of Computer Networks*. 1–22.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10/b22kn7

Green, D. M., & Swets, J. A. (1966). Signal detection theory and psychophysics. 1966. *New York*.

Jansen, J. (2018). *Do you bend or break?: preventing online banking fraud victimization through online resilience*.

Kirkpatrick, D. L. (1959a). Techniques for evaluating training programs. *Journal of ASTD*, (13), 3–9.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, 70–81. ACM.

Martin, J. (2019). *Phishing in dark waters: A quasi-experimental approach with evaluating cyber-security training for end-users* (Order No. 13813719). Available from Dissertations & Theses @ University of South Florida - FCLA; ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Global. (2240073001). Retrieved from https://search.proquest.com/docview/2240073001?accountid=14745

PhishMe, Inc. (2017). *Enterprise Phishing Resiliency and Defense Report: Analysis of Susceptibility, Resiliency and Defense against Simulated and Real Phishing Attacks*.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178–1204. https://doi.org/10/f7wvhw

Wombat Security Technologies. (2018). *State of the Phish*.