An Alternative to the One-Size-Fits-All Approach to ISA Training: A Design Science Approach to ISA Regarding the Adaption to Student Vulnerability Based on Knowledge and Behavior

THOMAS JERNEJCIC, PHDIS STUDENT

DSU WIP Poster **February 11, 2020**

Abstract

Any connection to the university's network is a conduit that has the potential of being exploited by an attacker, resulting in the possibility of substantial harm to the infrastructure, to the university, and to the student body of whom the university serves. While organizations rightfully "baton down the hatches" by building firewalls, creating proxies, and applying important updates, the most significant vulnerability, that of the student, continues to be an issue due to lack of knowledge, insufficient motivation, and inadequate or misguided training. Utilizing the Design Science Research (DSR) methodology, this research effort seeks to address the latter concern of training by seeking to design a methodology that will sufficiently support the automatic adaptation of security training, which will be based on the assessment of student vulnerability determined by the student's overall Information Security Awareness (ISA) knowledge and computer security behavior.

Background

The purpose of this research endeavor is to close the gap between security and ISA training through the proposition of IT artifacts to support the automated adaptation of training to address student vulnerability based on knowledge and behavior. Using the Design Science Research Methodology (DSRM), we seek to design a methodology and an application, the latter which will suffice as an instantiation of the proposed methodology, serving as validation.

Literature Review

THREATS: Farooq et al. [1] identified a taxonomy of threats (Figure 1).

ISA: ISA is more than awareness but includes assurance and enforcement of positive behavior towards mitigating risks [2].

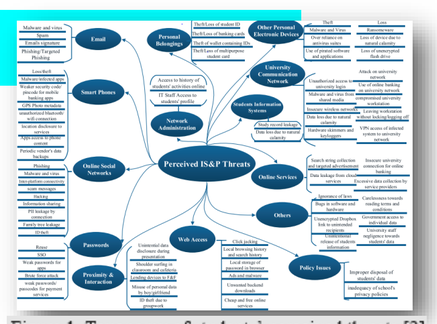

Figure 1. Taxonomy of students' perceived threats [2]

BEHAVIOR: A review of behaviorally related literature identified security training as an enabler of users to adopt "best practices" as defined by the organization [3]. Also, training indirectly supports security behavior by fostering self-efficacy and mandatory compliance, which positively impacts behavior [3].

TRAINING: Market will grow to $10 billion by the year 2027 [4]. Training is insufficient at most universities [5]. In addition, students at educational institutions have less motivation to comply with stated security policies [6]. While many training packages boast making training fun and interactive, none take an adaptive approach at the frontend, which is the driving force behind this specific DS research endeavor.

ALTERNATIVES: Discovered multiple publications with recommendations for ISA training [4,7-10]. Of those discovered, only a few were somewhat adaptive, including allowing the user to determine content [9], but none disclosed automated processes based on prior knowledge and expected behavior, exhibiting a gap in current offerings regarding automated adaptation. Research suggests users' competence to comply with security policies are out of alignment with requirements based activities [11].

Methodology and Plan

Seek to develop expert IS artifacts that will help target security competency gaps. This is consistent with IS governance frameworks such as ISO 27001 [12]. By adapting to one's current knowledge and perceived behavior, training will be most effective by promoting knowledge of vulnerability and severity while increasing self efficacy and response efficacy.

Artifacts

"To be effective, an educational campaign must first understand users' perceptions of computer and online security" [8]. We understand this assertion to be credible but seek to enhance effectiveness through automated real-time adaptivity by proposing two new artifacts: The Security Automated Adaptability Training (SAAT) methodology (Figure 2) and the SAAT Web application prototype (Figure 3). SAAT constructs are informed by the Universal Constructive Instructional theory [13] and the Cognitive Load theory [14].

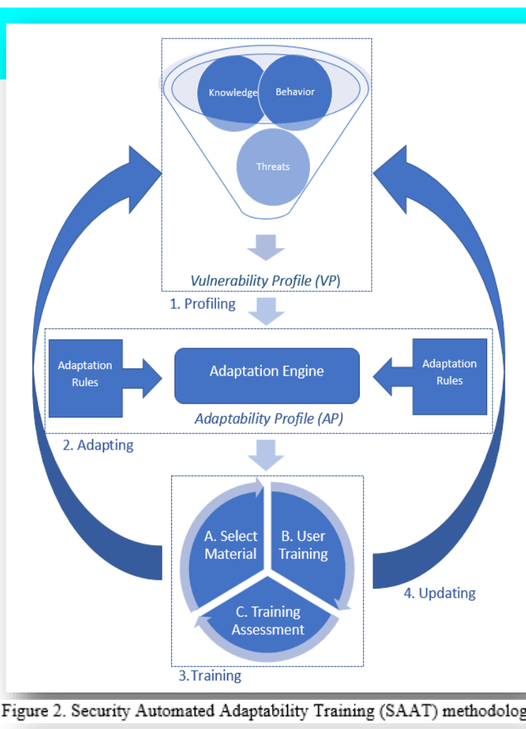

Figure 2. Security Automated Adaptability Training (SAAT) methodology

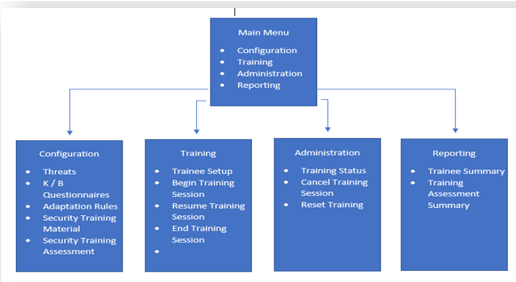

Figure 3. SAAT Web application prototype

Evaluation

Separate focus groups composed of student subjects of like demographics will be assessed of their ISA knowledge and perceived behavior before and after training. The control group will be trained on all ISA material (absent SAAT) and the experimental group will be trained using the SAAT web prototype. Success will be determined based on whether the experimental group experiences the same or greater improvement. To ensure homogeneity, subjects will be randomly assigned to each group. Data analytics will consist of descriptive and inferential analysis techniques in order to describe and summarize data points and perform hypothesis testing to determine statistical significance of the findings.

Expected Contributions

Contributions will include a design science approach to adaptive security training, implementation in the form of a Web application, a methodology to inform increased effectiveness of ISA training, decreased risk of direct cyberattacks on students, and decreased risk of indirect cyberattacks on universities.

References

[1] A. Farooq, S. Rameez Ullah Kakakhel, S. Virtanen, and J. Isoaho, "A taxonomy of perceived information security and privacy threats among IT security students," ed, 2015, pp. 280-286.
[2] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors," vol. 1, ed: IEEE, 2015, pp. 352-359.
[3] J. Omidosu and J. Ophoff, "A theory-based review of information security behavior in the organization and home context," ed, 2016, pp. 225-231.
[4] S. Morgan, "Please Don't Send Me to Cybersecurity Training," *Cybersecurity Business Report,* Available: https://www.csoonline.com
[5] E. Kim, "Recommendations for information security awareness training for college students," *Information Management & Computer Security,* vol. 22, no. 1, pp. 115-126, 2014.
[6] K. Underwood, "Universities Schooled On Cybersecurity," *Signal,* vol. 72, no. 6, pp. 30-32, 2018.
[7] M. H. Wilson, J., "Building an Information Technology Security Awareness and Training Program (NIST 800-50)," in *NIST 800-50*, ed: National Institute of Standards and Technology, 2003.
[8] S. M. Furman, M. F. Theofanos, C. Yee-Yin, and B. Stanton, "Basing Cybersecurity Training on User Perceptions," *IEEE Security & Privacy,* vol. 10, no. 2, pp. 40-49, 2012.
[9] S. Abraham and I. Chengalur-Smith, "Evaluating the effectiveness of learner controlled information security training," *Computers & Security,* vol. 87, 2019.
[10] B.-H. Kim, K.-C. Kim, S.-E. Hong, and S.-Y. Oh, "Development of cyber information security education and training system," *An International Journal,* vol. 76, no. 4, pp. 6051-6064, 2017.
[11] A. Tsohou and P. Holtkamp, "Are users competent to comply with information security policies? An analysis of professional competence models," *Information Technology & People,* vol. 31, no. 5, pp. 1047-1068, 2018.
[12] ISO-27001, "Information Technology - and Security Techniques - and Information Security Management Systems - and Requirements," 2013.
[13] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly,* vol. 34, no. 4, p. 757, 2010.
[14] R.-S. Shaw, H.-C. Keh, N.-C. Huang, and T.-C. Huang, "Information Security Awareness On-Line Materials Design with Knowledge Maps," *International Journal of Distance Education Technologies,* vol. 9, no. 4, p. 41, 2011.