Virtual Gamification in a PBS SETA Program

Mrs. Krista Stacey and Dr. Jeff Landry

November 14, 2024

UNIVERSITY OF SOUTH ALABAMA

CISSE Presentation

Motivation

- Need more effective SETA programs to counter insider threats
- If fear appeals are not effective, then what?
- High Protection Motivation (PM) and Self-Efficacy (SE) → higher compliance
- How to increase both?
- Education-based behavioral pedagogy + data-driven learning methodologies
- Goal: Boost PM & SE using Positive Behavior Supports (PBS), gamification, and mixed-reality (XR).

(Posey et al., 2015)

Research Questions

RQ1: Will a SETA program designed with PBS principles increase protection motivation and self-efficacy, thereby increasing InfoSec policy compliance?

RQ2: At what intensity of virtuality and gamification will a SETA program developed in XR increase InfoSec policy compliance over traditional methods?

Literature Review

- Insider Threat
  - Malicious
    - Controllable vs Uncontrollable
    - Belonging/Environment (PMT)
  - Non-Compliant
    - SE more mitigating
  - Culture impacts insider PM
- Gap: Focus on the connection between PM, SE and compliance

(Guo et al. (2011), Liang et al. (2016), Sharma & Aparicio (2022), Willison & Warkentin (2013))

Literature Review

- SETA
  - Part of deterrence
  - "Key" of security action cycle
  - Individualized
  - Positive reinforcement over fear
  - Social norms
  - Feedback loop: Positive reinforcement builds compliance through iterative learning
- Gap: addressing PM, SETA and SE as a feedback loop

(Boss et al. (2015), D'Arcy et al. (2008), Johnston et al. (2019), Straub & Welke (1998))

Literature Review

- Problem: current SETA focuses on the training itself
- PBS
  - Treat the source of the misbehavior
  - Positive reinforcement throughout training **and** environment
  - Meet the learner where they are
  - Individualize
  - Data-driven learning methods
- Gap/Goal: PBS implementation of SETA

(Estrada et al. (2022), Kam et al. (2022) Martens & Andreen (2013),Young et al. (2012))

Literature Review

- Gamification
  - Data-driven methodology
  - Positive reinforcement (PBS backed)
  - Meet the learner where they are
  - Interest, immersion → motivation and belonging (PM)
  - Possibilities for individualization
- Gap: Gamification to study effects on PM, SE, compliance

(Bohné et al. (2022), Dicheva et al. (2015), Li & Chu (2021))

Literature Review

- Virtualization
  - Trend: simulation-based training
  - Data-driven methodology
  - Interest, immersion → PM
  - Increase humanness of the technology
  - Possibility of Individualization
- Gap: Virtualization of SETA simulations, effect on PM, SE, compliance

(Lankton et al. (2015), Patel et al. (2020), Zhang et al. (2020))

Research Model

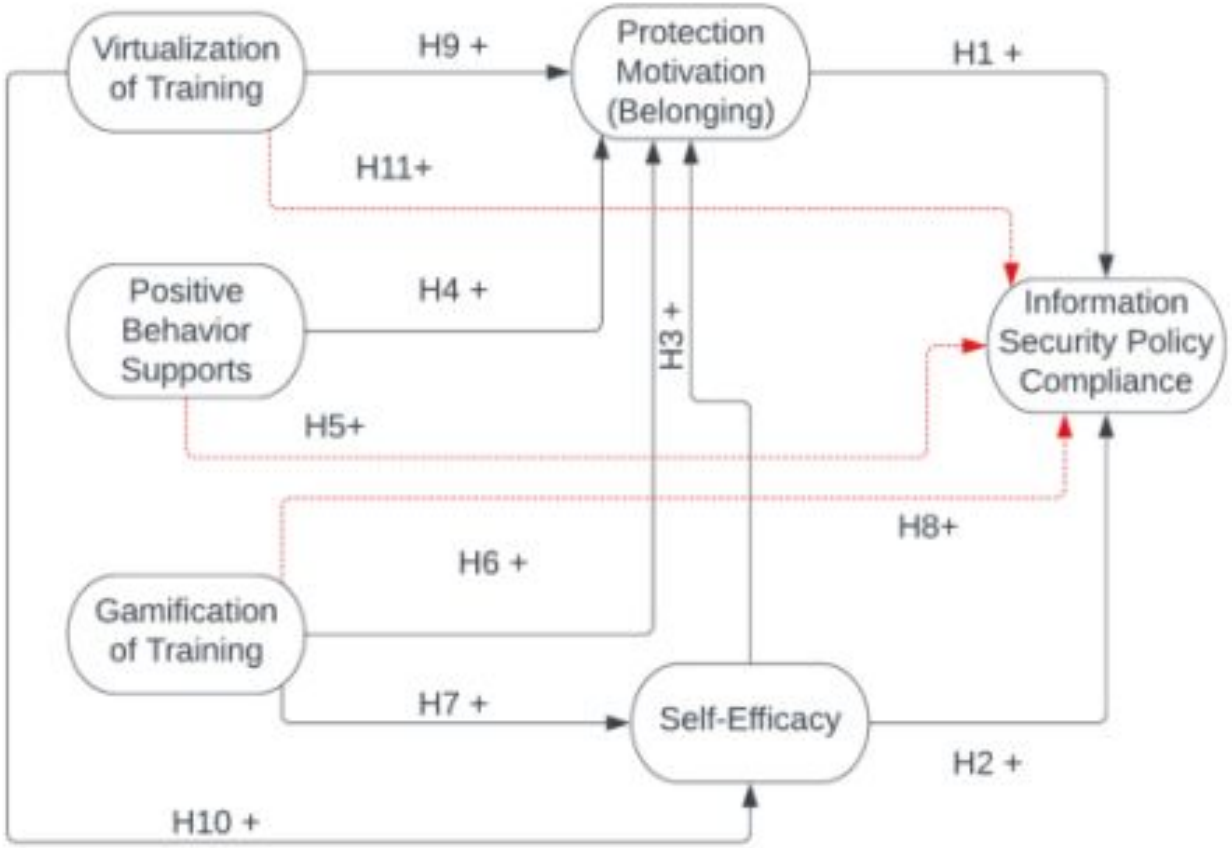

Figure 1: Nomological Model

Hypotheses

H1: PM as measured by belonging increases Information Security policy compliance.

H2: SE increases Information Security policy compliance.

H3: SE positively affects PM.

H4: Positive Behavior Supports positively affects PM.

H5: Positive Behavior Supports positively affects compliance.

Hypotheses

H6: Gamification of training positively affects the user's PM.

H7: Gamification of training positively affects the user's SE.

H8: Gamification of training positively affects compliance.

Hypotheses

H9: XR simulation training positively affects a user's PM.

H10: XR simulation training positively affects a user's SE.

H11: XR simulation training positively affects a user's compliance.

Discussion (Proposed Methodology)

- Pretest survey: Rating of PM(Belonging)/SE/Intentions to Comply
- 2x2x2 experiment
  - Mix of high/low of the variables PBS, Virtualization, Gamification
- Posttest survey: Repeat of pretest plus evaluation of SETA effectiveness
- Longitudinal Action Research
  - Implement "most effective" combination as well as PBS training

Expected Contributions

Theoretical:

- Address environment as a factor in compliance
- Bridge gap between educational theory and SETA, test combinations of constructs

Practical:

- Give IS Managers an implementation of SETA that addresses all insiders by increasing PM and SE.

(Chan & Wei (2008), Kam et al. (2022))

Questions?

Key Citations

N. Liang, D. P. Biros, and A. Luse, "An Empirical Validation of Malicious Insider Characteristics," *Journal of Management Information Systems*, vol. 33, no. 2, pp. 361–392, Apr. 2016. [Online]. Available: https://doi.org/10.1080/07421222.2016.1205925 .

T. Chan and V. Wei, "Teaching for Conceptual Change in Security Awareness," *IEEE Security & Privacy*, vol. 6, no. 6, pp. 67–69, Nov. 2008. [Online]. Available: https://doi.org/10.1109/MSP.2008.157 .

J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems*, vol. 31, no. 2, pp. 285–318, Oct. 2014. [Online]. Available: https://doi.org/10.2753/MIS0742-1222310210 .

D. W. Straub and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, vol. 22, no. 4, pp. 441–469, Dec. 1998 .

E. Young, P. Caldarella, M. Richardson, and R. Young, *Positive Behavior Support in Secondary Schools: A Practical Guide*. New York, NY: Guilford Press, 2012 .

D. Patel, et al., "Developing Virtual Reality Trauma Training Experiences Using 360-Degree Video: Tutorial," *Journal of Medical Internet Research*, vol. 22, no. 12, p. e22420, Dec. 2020. [Online]. Available: https://doi.org/10.2196/22420 .

S. Sharma and E. Aparicio, "Organizational and Team Culture as Antecedents of Protection Motivation among IT Employees," *Computers & Security*, vol. 120, p. 102774, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2022.102774 .

T. Bohné, I. Heine, F. Mueller, P.-D. J. Zuercher, and V. M. Eger, "Gamification Intensity in Web-Based Virtual Training Environments and Its Effect on Learning," *IEEE Transactions on Learning Technologies*, pp. 1–19, 2022. [Online]. Available: https://doi.org/10.1109/TLT.2022.3208936 .

D. Dicheva, C. Dichev, G. Agre, and G. Angelova, "Gamification in Education: A Systematic Mapping Study," *Journal of Educational Technology & Society*, vol. 18, no. 3, pp. 75–88, Jul. 2015 .

Lankton, N. K., D. H. McKnight, and J. Tripp, "Technology, Humanness, and Trust: Rethinking Trust in Technology," *Journal of the Association for Information Systems*, vol. 16, no. 10, pp. 880–918, 2015 .