

# IS HIGH-RISK AIS SECURITY INVESTMENT A NO-WIN SITUATION? THE INFLUENCE OF ATTITUDES, NORMS, EFFICACY AND PRIOR OUTCOMES

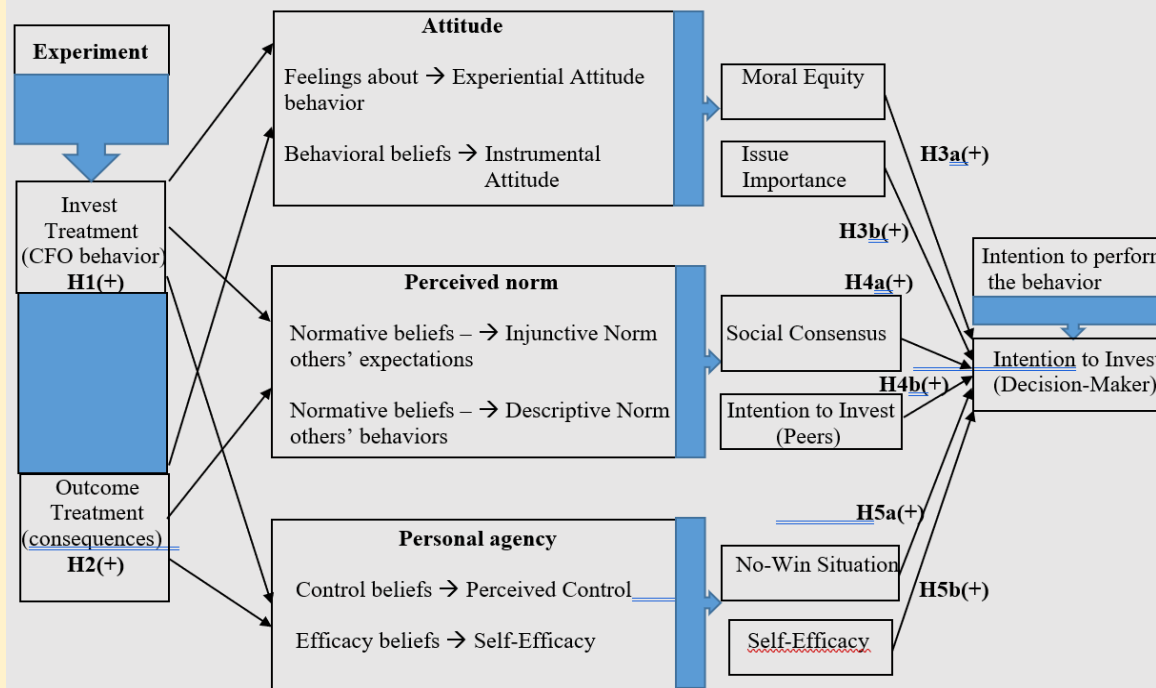
Gary Fleischman<sup>1</sup>, Sean Valentine<sup>2</sup>, Mary Curtis<sup>3</sup>, Partha S Mohapatra<sup>4</sup>

<sup>1</sup>Texas Tech University, <sup>2</sup>University of North Dakota, <sup>3</sup>University of North Texas, <sup>4</sup>CSU-Sacramento

**Objective:** To examine the psychological drivers (i.e., perceived attitudes, norms, and efficacy – personal agency) of the managerial reasoning process regarding high-risk investments in AIS security.

**Introduction:** While recent data breaches underscore importance of IS security, costs of necessary security may be prohibitive, forcing CFOs to make difficult financial and moral tradeoffs. Hence, based on the *Integrated Behavioral Model* (Montaño and Kasprzyk 2015), our specific research questions about risky investments in IS security focus on the role of manager perceptions relating to 1) *attitudes* about the morality and importance of an AIS hacking risk investment scenario, 2) *norms* representing how society and peers would likely evaluate the depicted investment trade-off, and 3) *personal agency* relating to efficacy and control.

## Hypothesized relationships:



**Methods:** We use a scenario that involves IS security investment decisions made by a Chief Financial Officer (CFO).

Use a 2x2 experimental randomized design. Four treatments: The observed CFO, 1. Invested in security and had a favorable organizational outcome; 2. Invested in security and had an unfavorable organizational outcome; 3. Did not invest in security and had an unfavorable organizational outcome, and 4. Did not invest in security and had a favorable organizational outcome. Graduate students from B-Schools (with average experience of 5.5. years) participated in our study.

## Findings & Conclusion:

We find that managers are more likely to invest similarly to scenario CFOs who choose to invest in protective security (supporting H1), and are also more likely to invest in a similar manner as CFOs who invest in protective security when the firm is hacked, supporting H2. Findings also support other hypotheses except for H3b (Issue Importance) and H5b (Self-Efficacy). Findings suggest:

- Middle manager participants intend to invest in a similar (dissimilar) manner as the scenario CFO when the CFO chooses to invest (not invest) in needed security.
- Perceived norms from peers and society drive participant investments in AIS, and serially mediate organizational outcomes.
- Peer versus societal influence dominance varies depending on experimental context.
- Perceptions that the situation overall reflects a no-win situation also drives managerial investment decisions.
- Confident independent thinkers make more appropriate investment decisions to protect sensitive client data despite possible harm to personal cost cutting reputations.