Thwarting the Malicious Insider Evolution Process: The Theory of Strained Betrayal

Sanjay Goel
Chair & Professor, Dept. of Information Security & Digital Forensics, School of Business, University at Albany, State University of New York
Allen Johnston
Associate Professor, School of Business, University of Alabama, Tuscaloosa

https://nsf.gov/awardsearch/showAward?AWD_ID=1912874&HistoricalAwards=false

OVERVIEW

- The United States has lost billions of dollars in intellectual property to corporate espionage, primarily through malicious insiders, intrusion into corporate networks by hacking, and forced technology transfers. Preventing insider data theft is critical to protecting intellectual property and national secrets.
- This project will help clarify the evolution of the malicious insider, and how situational and dispositional factors associated with employees and their workplace contribute to this evolution. Further, we examine both emotion-focused and problem-focused interventions aimed at disrupting this evolution.
- This research on evolution of malicious insiders is grounded in General Strain Theory (GST), where we examine the role of strain (situational factors) and personality (dispositional factors) in motivating individuals to commit malicious, clandestine insider attacks.
- This research will be done in three phases: first we use a scenario study to conduct a preliminary evaluation of the TSB model in different situational contexts that activate strain (e.g., social injustice & personal injustice); second, we conduct experiments to induce strain, and evaluate the subjects' behavior related to insider theft; third, we test interventions to reduce the strain, and in the process, decrease the likelihood of malicious behaviors.

PROBLEM

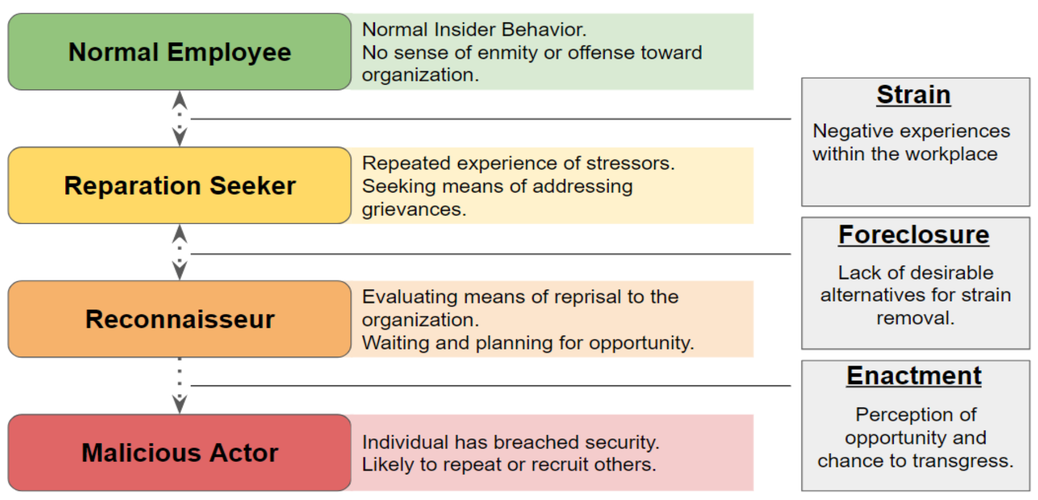
- Insider threats can be accidental or deliberate, with completely different underlying behavioral mechanisms. The focus of this research is intentional malicious behavior.
- Past work on insider threats has focused on post exfiltration detection and on remediation and containment of the breach when damage is already done.
- Detection of insider malicious activities has relied primarily on analysis of user behavior from computer and network log where anomalous is deciphered from traces of activities latent in the data.

GOAL

- Understand the Evolution of Malicious Insiders in Organizations.
- Examine the role of dispositional factors in moderating how an employee perceives strain from situational factors and how h/she acts upon that strain.
- Synthesize criminological and organizational theories to create an explanatory basis for the evolution of a malicious insider.
- Define and test interventions that will delay or halt the evolution of malicious insiders.
- Apply concepts derived from the proposed research to reduce incidence of insider theft the precursors of insider threat.

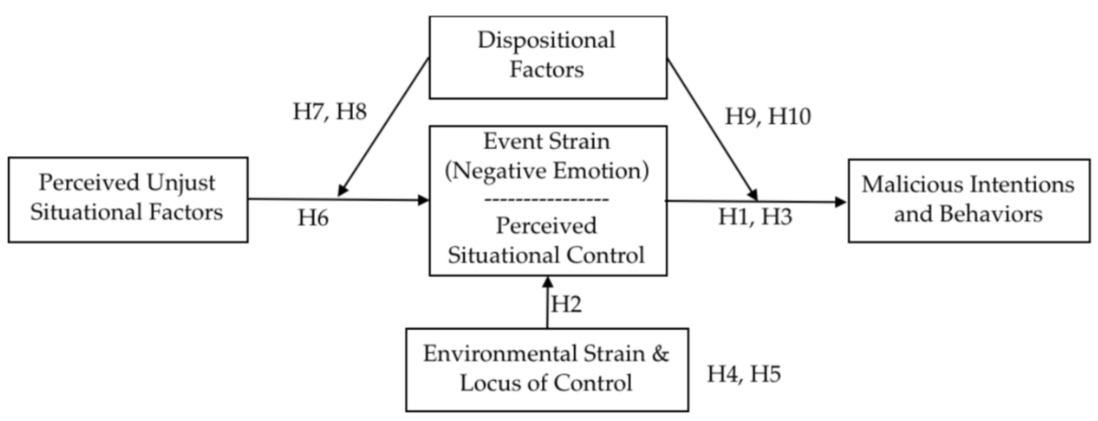
CONTRIBUTION

- This project will help clarify the evolution of the malicious insider, and how situational and dispositional factors associated with employees and their workplace contribute to this evolution. Further, this body of research suggests both emotion-focused and problem-focused interventions aimed at disrupting this evolution.
- The evolution of a malicious insider is best described by the insider threat kill chain.



MODEL

The Theory of Strained Betrayal (TSB) model leverages the emotion-centered model of voluntary behavior (ECM), which identifies how negative emotional states and perceived behavioral control result in counterproductive work behaviors (Spector & Fox, 2002), and the GST, which helps to explain the strain that individuals feel from imbalances between their socially-constructed goals and their reality (Agnew, 2007). The model explains behavioral intentions to commit malicious insider activities as dependent on the situational factors imposed on an employee, the strain that those factors engender, decreased perceptions of situational control, and the moderating effects of the employee's disposition on those relationships.



EXPERIMENTAL DESIGN

PHASE 1: SCENARIO STUDIES

Participants will read realistic scenarios and role play an insider to articulate their expected responses to specific situations. The scenarios will be designed to manipulate perceived unjust situational factors in the workplace. Users are given three options: 1) taking legitimate channels; 2) stealing information; 3) publicly shame the company/ individual.

PHASE 2: EXPERIMENTAL MANIPULATION OF STRAIN

Participants perform a series of tasks before the focal task where the opportunity for malicious behavior arises. In these prior tasks, we manipulate prior strain by varying the number of stressors that participants encounter while performing the tasks.

We directly manipulate feelings of injustice by manipulating experiences of injustice during a computer-based activity, and then providing participants the opportunity to engage in malicious cybersecurity behaviors. We also measure personality variables and locus of control beliefs to test the TSB model.

PHASE 3: INTERVENTION TO MITIGATE STRAIN

In this study the the justice manipulations used in phase 2 is merged to create an unjust and just condition. Interventions are tested to evaluate their efficacy in preventing insider threat behaviors.

The participants, like those in the previous experiment, will also be provided with a window of time in which they will have the opportunity to act out against the strain caused by personal injustice by accessing, altering, and exfiltrating files that appear to belong to the researcher.

BROADER IMPACT

- This work can assist in reducing strain on employees in organization and improving quality of work.
- The outcomes of this work can help protect organizational intellectual property and national secrets.
- The proposed research outcomes will impact other information security issues and stimulate further research in behavioral security and security economics.
- This research will provide a reference point for investigating human factor issues in other domains.
- This research on insider threat evolution will be integrated into two new courses: A new doctoral course on behavioral theories for cybersecurity research; and an elective course on insider threats in UAlbany's MS program in Digital Forensics and Cyber Security.
- A doctoral and an undergraduate student will be directly involved in the research, acquiring research and organizational insider threat mitigation skills.
- The results of this work will be disseminated through conference presentations and journal publications. PI Goel has organized the Annual Symposium on Information Assurance (ASIA) in conjunction with the New York State Cyber Security Conference for the past decade. In 2021, an insider threat research track will be organized in the Annual Symposium of Information Assurance.
- UAlbany sponsors, through its EOP office, an annual Summer Research Program (UASRP), which offers qualified underrepresented undergraduates research experience. We will take two students each year from this program engaged in research related to this project.

Agnew, R. (2007). *Pressured into crime: An overview of general strain theory.*
Spector, P. E., & Fox, S. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human resource management review, 12(2)*, 269-292.