IARPA (RESCIND)

Sanjay Goel (and Team)

University at Albany, School of Business

Insider Threats (NSF)

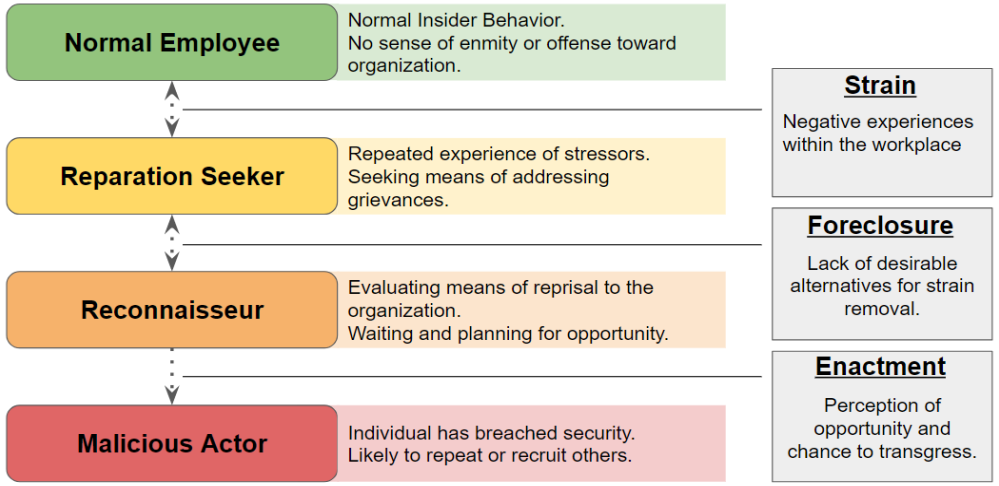
Thwarting the Malicious Insider: The Theory of Strained Betrayal

Background:

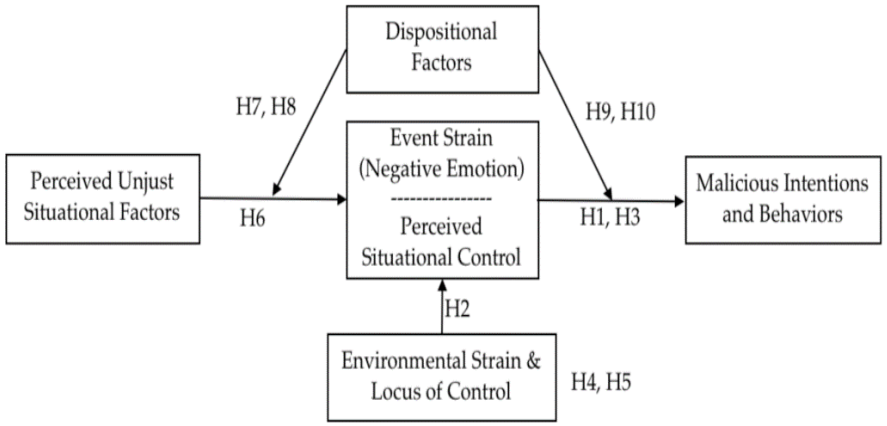
- The Theory of Strained Betrayal formalizes a model of the process of a loyal employee transforming into a malicious one that captures the dynamics of job strain manifestation and its culmination in malicious insider activity.
- A series of studies designed to test the evolution model of insider threat and develop emotion-focused and problem-focused interventions aimed at disrupting the manifestation of malicious behavior originating from strain.

Potential Contribution:

- This research help clarify the evolution of the malicious insider, and how situational and dispositional factors associated with employees and their workplace contribute to this evolution.
- 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.



Theoretical Model:



Study Design:

- Data collection completed
- 30 full-time employees

- Two-wave online survey
- Data collection done
- In the process of data analysis

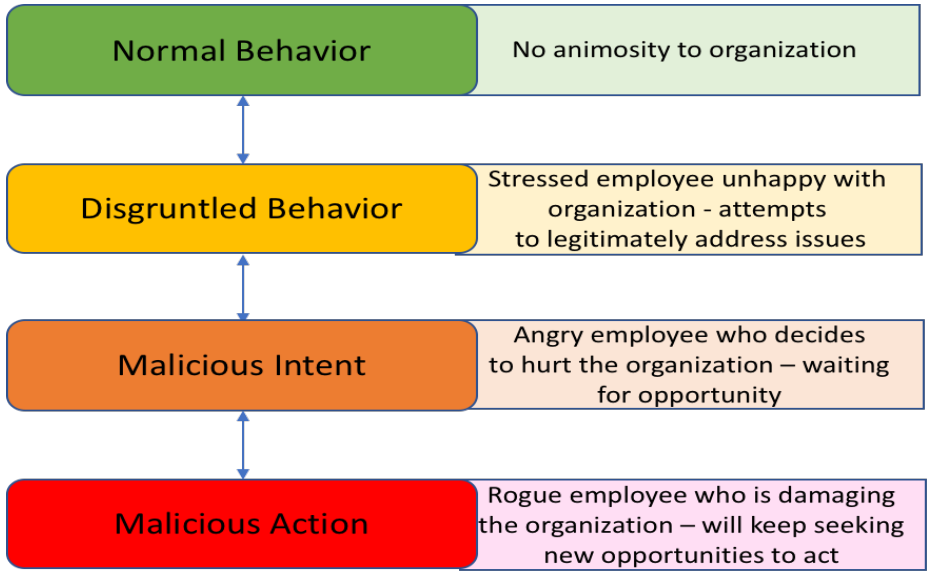
- Experimental design completed
- Data collection paused due to COVID-19

- Need to be based on results of previous studies.

Insider Threats (IARPA)

Active Indicators – Behavioral Probes

- Intentional behavior can be conceptualized as function of motivation (incentive), capability, opportunity.
- Through use of active probes we can form predictive profiles using personality and other measures to identify threats.
- Environmental and disposition precursors may involve greed, perception of being undervalued, disgruntlement, perceived social injustice, patriotism.
- We designed scenarios to build situational context and tested user behavior on simulated opportunities to steal data.



Scenario: Joe works for a large conglomerate that produces water filtration systems that are critical for poor countries where the water supply is severely contaminated. Typical water filtration systems are very expensive, however, Joe and his colleagues have developed a system that is highly cost effective. Despite the cost of producing this new filtration system being only a few dollars, Joe's company has gauged the price to charge hundreds of dollars. Ultimately, Joe is outraged at this policy, since many countries will no longer be able to afford this system, leading to widespread sickness and death.

Active Defense (NSA)

Engaging with Adversaries (Objectives)

PROFILING HACKERS

- Understanding and mapping a hacker's decision-making processes - the 'who', 'why', 'when', 'what', 'how' behind the observed probing and attacking behaviors, and more importantly, 'what next' of attacks.
- This may increase the visibility of risks and open up opportunities for defenders to exploit the hackers' characteristics and dissuade or prevent them from achieving their aims.
- Focus: attackers' motivation, personality, knowledge, skills, and how they are associated with particular attacking behaviors or behavioral sequence.

EXPLOITING COGNITIVE BIASES

- Designing systems that can elicit attackers' cognitive bias and lure them into the traps.
- Exploiting these biases to disrupt, delay and deny the attackers' access to their targeted assets.
- **Target biases and heuristics:** confirmation bias, availability heuristic, anchoring and adjustment heuristic, overconfidence, overclaim, aversion to ambiguity, loss aversion, sunk cost fallacy, illusion of control, ostrich effect
- Examining the prevalence of each cognitive bias and heuristics in hackers; designing and testing cues that can trigger the biases and heuristics; exploring ways of application/integration of the cues with defense systems

Active Defense (NSA)

Engaging with Adversaries (Preliminary Work)

LITERATURE REVIEW

- Cataloged typologies of hackers from literature and identified characteristics associated with the different type of hackers that might have an impact on how they hack.
- Literature review on common cognitive biases and heuristics and selected the ones that might be most significant in the hacker population

INTERVIEW STUDY

- Interview studies with students who had hacking experience, collecting data on their learning/training background, knowledge and skill levels, motivations, and their specific hacking experience
- Found some dominantly preferred ways of handling the data they obtained and some common challenges they face in decision making.
- Next step: Expand the interview studies to other hacker groups and include personality in the equation and examine the correlations among all the factors.

SCENARIO STUDY

- Designing study that present participants a hacking scenario that might (or might not) include a cue that is hypothesized to trigger certain cognitive bias or heuristic and measures their decision making in the hypothesized scenario
- Working on testing instrument validity

RESCIND (IARPA)

TEAM

UALBANY

- Sanjay Goel (Professor Information Security and Digital Forensics): Focus on cyber security behavior and motivation, active defense, and intrusion detection.
- Kevin Williams (Professor I/O Psychology): Expertise in assessment and security behavior.
- Jingyi Huang (Postdoc I/O Psych): Exploring human's roles in information security policy compliance, privacy attitude, and compliance with health policy. Also engaged in worker stress, coping, emotions, motivation and performance, and personality.
- Sherin Shaju (Doctoral Student I/O Psych): Research interests include performance appraisal, organizational justice, and diversity within the workplace.

OTHER KEY RESEARCHERS

- Justin Peletier: Justin Pelletier is the Director of the Cyber Range and Training Center in RIT's Global Cybersecurity Institute. Runs collegiate cyber competitions (CCDC, CPTC)
- Richard Roberts (Rad Solutions): Expert cognitive and non-cognitive skill assessment
- Franklin Zaromb (National Authority for Measurement and Evaluation in Education) Expert in cognitive psychology (human learning, memory, judgment and decision-making), assessment of biases in cognition

OTHER PARTNERSHIPS:

IBM, GE Global Research, Active Defense Vendors, Tufts

LOOKING FOR:

Expertise on Software Development for phase III and computational cognitive modeling