Balancing Organizational Incentives to Counter Insider Threat

**Presenter:** Andrew P. Moore

**Contributors:** CERT Division’s National Insider Threat Center, SEI Human Resources, Organizational Effectiveness Group, CMU Heinz College and Tepper School of Business

**Website:** http://www.cert.org/insider-threat
Copyright 2018 Carnegie Mellon University and IEEE. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.


DM18-0691
Introduction

Insider threat behavioral analytics

• Typically involves analyzing data on the *behaviors of subject insiders* to identify indicators of increased risk

What about *organizational behaviors*? (i.e., non-security related practices)

• Can they be conducive to insider threat?
  • YES – historically known as situational factors
  • BUT - Little considered when forming insider threat programs
  • IMPLIES - Insider attacks are repeated as natural consequence

You can prevent, detect, respond to conducive organizational behaviors

• Just as with indicative insider behaviors
A CERT Research Project

Determine influence of workforce management practices on insider threat behaviors

**Negative Incentives**
Workforce management practices that attempt to *force* employees to act in the interests of the organization

**Employee Constraints, Monitoring, Punishment**

**Positive Incentives**
Workforce management practices that attempt to *attract* employees to act in the interests of the organization

**Focus on Employee Strengths, Fair & Respectful Treatment**

Negative incentives *alone* can *exacerbate* the threat they are intended to mitigate*

**Basic Belief:** Organizations should *explicitly* consider a *mix of positive and negative incentives* to build insider threat programs that are a net positive for employees

**Initial Scope:** Disgruntlement-spurred threat

Insider Threat Research Context

Insider Threat Defense

Prevent Insider Misbehavior

Detect and Respond to At-Risk Insider Behaviors

Prevent using Negative Incentives

Early detection with possible positive or negative response

Positive deterrence (monitoring not required)

Detection of organizational conditions conducive to insider threat

Prevent Insider Misbehavior

Detect and Respond to At-Risk Organizational Conditions

Prevent using Positive Incentives

Negative deterrence (monitoring not required)

A form of negative incentive
Three Broad Categories of Positive Incentives

People

Connected @ Work

Organization

Perceived Organizational Support

Job

Job Engagement
Previous Studies in the Organizational Behavior Literature: Counterproductive Work Behavior (CWB)

Citation Key:
(s) = (Sulea et al., 2012)
(a) = (Ariani, 2013)
(r) = (Rhoades, Eisenberger, & Armeli, 2001)
(c) = (Colbert, Mount et al. 2004)
(b) = (Bordia, Restubog, & Tang, 2008)
(f) = (Fatima et al., 2013)
(t) = (Tang, Ibrahim 1998)
* Stat for Psychological Contract Breach instead of POS
Two-Pronged Exploratory Research Approach*

1. *Insider Incident Case Study Analysis*
   - How engaged, connected, and supported are insider threat actors?

2. *Organizational Survey*
   - How much does organizational support influence insider cyber misbehavior?

Extension of previous work by focusing on
- Cyber-related insider threat behaviors
- Organizations actively establishing insider threat programs

Organizational Survey

How much does organizational support influence insider cyber misbehavior?

• **Challenge:** Hard-to-reach population suggests initial exploratory (non-random, small sample)

• **Method:** Survey Open Source Insider Threat (OSIT) Information Sharing Group
  - Independent variables on established 5-point scales
    • *Perceived organizational support* (36 questions)
    • *Organizational justice* (19 questions)
  - Dependent variable on 5-point frequency scale
    • *Cyber misbehavior* from case data (22 questions)

• **Response:**
  - 25 out of ~90 organizations responded

Results: 23 responses*

* Analysis used Deming Regression and Multiple Imputation by Chained Equations for missing values.

![Misbehavior Frequency vs Perceived Organizational Support](image1)

Slope = -1.04
Statistically significant 95% confidence level

![Misbehavior Frequency vs Organizational Justice](image2)

Slope = -0.35
Statistically significant 95% confidence level
### Surveyed Items on Insider Cyber Misbehaviors (Intentional)

<table>
<thead>
<tr>
<th>Violating acceptable use</th>
<th>Disabling security controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taking proprietary information upon departure</td>
<td>Posting negative perceptions about organization</td>
</tr>
<tr>
<td>Violating security policy</td>
<td>Sabotaging coworkers work</td>
</tr>
<tr>
<td>Stole significant items</td>
<td>Purposely damaging organizational equipment</td>
</tr>
<tr>
<td>Logged in to appear as if working</td>
<td>Plagiarizing work of coworkers</td>
</tr>
<tr>
<td>Inappropriately transmitting proprietary information internally</td>
<td>Sending threatening or harmful emails</td>
</tr>
<tr>
<td>Purposely producing low quality work</td>
<td>Purposely installing harmful software</td>
</tr>
<tr>
<td>Unauthorized remote access</td>
<td>Vandalizing website</td>
</tr>
<tr>
<td>Inhibiting coworker progress</td>
<td></td>
</tr>
</tbody>
</table>

---

(DISTRIBUTION STATEMENT A) Approved for Public Release; Distribution is Unlimited
Limitations and Directions

Insider Threat Incident Analysis
- Analysis of three incidents does not permit drawing strong conclusions
- Used to narrow hypothesis for survey work

Organizational Survey
- Challenges reaching population suggested non-random sample of OSIT
- Vulnerable to the self-selection bias
- Data does not support causal analysis and results not generalizable

Our research just scratches the surface, BUT
- Justifies additional fundamental research in area (will discuss later)
- Combined with previous organizational behavior research, (arguably) justifies piloting of positive incentives (applied research)
  - Focus on practices associated with perceived organizational support
Organizational Supportiveness Principles and Practice Areas

Attract and retain staff to achieve mission

- Preconditions involving recruiting and hiring the right staff
  - Positive Incentives reducing insider threat while promoting satisfaction, performance, and retention
    - Incentives
      - Positive incentives
      - Negative incentives
      - Motivation
      - Mastery
      - Purpose
      - Autonomy
      - Connectedness
    - Performance and Personal Supportiveness
      - Supportive management
      - Effective communication
      - Professional Development
      - Compensation
      - Time Off and Leave
      - Staff Relations
      - Confident employee assistance programs providing an impartial third-party to discuss issues both personal and professional
  - Perceived Organizational Support
    - Functional support
      - Organizational Justice (Fairness)
        - Fair and equitable distribution of rewards
        - Fair and ethical recognition
        - Fair and ethical treatment
        - Fair and ethical communication
        - Fair and ethical conflict resolution
        - Fair and ethical grievance procedures
      - Effective communication
      - Professional Development
      - Compensation
      - Time Off and Leave
      - Staff Relations
      - Confident employee assistance programs providing an impartial third-party to discuss issues both personal and professional
  - Organizational Supportiveness
    - Preconditions
      - Needs assessment by hiring group to identify job descriptions
      - Preconditions
        - Incentives
          - Positive incentives
          - Negative incentives
          - Motivation
          - Mastery
          - Purpose
          - Autonomy
          - Connectedness
        - Performance and Personal Supportiveness
          - Supportive management
          - Effective communication
          - Professional Development
          - Compensation
          - Time Off and Leave
          - Staff Relations
          - Confident employee assistance programs providing an impartial third-party to discuss issues both personal and professional
  - Positively Retain Staff
    - Positive incentives
      - Positive incentives
      - Negative incentives
      - Motivation
      - Mastery
      - Purpose
      - Autonomy
      - Connectedness
    - Performance and Personal Supportiveness
      - Supportive management
      - Effective communication
      - Professional Development
      - Compensation
      - Time Off and Leave
      - Staff Relations
      - Confident employee assistance programs providing an impartial third-party to discuss issues both personal and professional

© 2018 Carnegie Mellon University
May 2018
Balancing Organizational Incentives to Counter Insider Threat

[DISTRIBUTION STATEMENT A] Approved for Public Release; Distribution is Unlimited
## Monitoring and Response (Examples)

<table>
<thead>
<tr>
<th>Organizational Support Dimension</th>
<th>How to Reduce Incident Baseline (example)</th>
<th>What Organization Behavior to Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Justice (Fairness)</td>
<td>Align compensation internally and externally</td>
<td>Consistency of compensation levels with organizational benchmarks</td>
</tr>
<tr>
<td>Performance-based Rewards and Recognition</td>
<td>Use performance-based criteria for promotions</td>
<td>Consistency of promotions with employee competency and performance track record</td>
</tr>
<tr>
<td>Transparent &amp; Respectful Communication</td>
<td>Regular employee expectation setting</td>
<td>Level of employee complaints and grievances</td>
</tr>
<tr>
<td>Personal and Professional Supportiveness</td>
<td>Strengths-based professional development</td>
<td>Employee job engagement</td>
</tr>
</tbody>
</table>
Areas of Research

**Theory Development**
- Experiment-based determination of cause-effect relationship between perceived organizational support and insider threat

**Technology Development**
- Detection of
  - at-risk organizational conditions associated with organizational support
  - insider alienation through indicative changes in insiders’ network of workplace relationships
- HR tools can facilitate positive incentives (e.g., performance management)
  - BUT, Employee Relationship Management tool development needed to support analysis of and diagnostics for one-on-one relationship between manager and direct reports

**Adoption**
- Determine how organizations can
  - determine an appropriate mix of positive and negative incentives
  - transition to that from their current state
Ways of Working With Organizations (Now)

Goal: Identify specific recommendations on positive incentive-based workforce management practices with the goal of reducing insider threat

Options:
1. Analyze existing data, practices, and/or incidents
2. Conduct surveys, interviews, or focus groups to better understand employee attitudes and behaviors
3. Analyze tools that support employee relationship management
4. Conduct a multi-phase assessment, training, and coaching study to determine outcomes associated with specific practices

CMU Faculty Collaborator: Professor Denise Rousseau
- Carnegie Mellon University Organizational Psychologist
- Founder of the theory of psychological contracts
Vision for Integrating Positive and Negative Incentives

Balanced Defense: Extending the Traditional Security Paradigm

• Fewer unintended consequences
• Satisfaction, performance, retention

Positive Deterrence

Balanced Defense

Negative Deterrence

• Fewer insider incidents and misbehaviors
• Lower investigative costs, productivity loss

Security Through Positive Incentives

Engagement Feedback →

Engagement

Connectedness

Organizational Supportiveness

Supported Employees

Connected Employees

Engaged Employees

Traditional Security Approach (Negative Incentives)

Deterrence Feedback →

Deterrence

Restriction

Monitoring

Sanctions

Detected Abuse

Detected Abuse

Punished Abuse

Prevented Abuse

Detected Abuse

Detracted Abuse

Detracted Abuse

Detracted Employees

(Straub and Welke, 1998)
Conceptualizing a Metric for Balanced Defense

The optimal ratio and acceptable range may vary depending on the specifics of the organization or the team in which it is applied.

**Optimal Ratio:**
Positive Incentive / Negative Incentive

- Too little negative incentive (or too much positive incentive)
- Too little positive incentive (or too much negative incentive)

Good starting place is to think about the negative incentives (security constraints, practices, and technologies) that you currently have in place.

- Regulatory Focus Theory provides a basis for determining optimal ratio
- A basic principle is that more is not always better!
Key Take-Aways

Insider goodwill is important to both
• keeping intentional insider threat to a minimum
• AND ensuring organization success generally

Organizational practices that undermine insider goodwill exacerbate risk
• If not addressed, such practices allow attacks to recur as natural consequence
• Includes unintended consequences of existing cybersecurity practices

Positive incentive-based principles and practice areas can be used to
• Reduce the *baseline* insider incident frequency
• AND Target *user* and *organizational* behavior monitoring

Insider threat programs that balance positive and negative incentives can become an advocate for the workforce and a means to improve employee worklife
• a welcome message to employees threatened by a focus on discovering insider wrongdoing
Contact Information*

Presenter / Point of Contact:
Andrew Moore
Lead Insider Threat Researcher
Telephone: +1 412.268.5465
Email: apm@cert.org

Contributors:

SEI CERT:
Samuel J. Perl
Jennifer Cowley
Matthew L. Collins
Tracy M. Cassidy
Nathan VanHoudnos

SEI SSD:
William Novak
David Zubrow

SEI Directors Office:
Palma Butbles

SEI Human Resources:
Daniel Bauer
Allison Parshall
Jeff Savinda

SEI Organizational Effectiveness Group:
Elizabeth A. Monaco
Jamie L. Moyes

CMU Heinz College and Tepper School of Business:
Professor Denise M. Rousseau

Life Dimensions Coaching and Counseling:
Susan B. Moore

Special thanks to the Open Source Insider Threat (OSIT) Information Sharing Group for their responses to our survey.

References


