The Critical Role of Positive Incentives in Reducing Insider Threat

Presenter: Andrew P. Moore
Contributors: SEI CERT, SEI Human Resources, SEI Organizational Effectiveness Group, CMU Heinz College/Tepper School of Business

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
The Critical Role of Positive Incentives in Reducing Insider Threat
February 2017
© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 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.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0004535
Research Objective

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

Three Dimensions of Employee-Organization Alignment

People

Connected @ Work

Organization

Perceived Organizational Support

Job Engagement

Job
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?

**Method:** Survey Open Source Insider Threat (OSIT) Information Sharing Group

**Results:** based on 23 out of ~90 organizations

![Graph showing the relationship between perceived organizational support and insider cyber misbehavior frequency. The slope is -1.04, statistically significant at the 95% confidence level.](image_url)

Slope = -1.04

Statistically significant

95% confidence level
Positive Incentive-Based Principles and Practice Areas

**Preconditions** involving recruiting and hiring the right staff

- **Positive incentives promoting satisfaction, performance, and retention**
- **Positive incentives reducing insider threat**

**Organizational Justice (Fairness)**
- Performance-based rewards and recognition
- Transparent and Respectful Communication
- Professional and Personal Supportiveness
- Culture and Working Conditions

**Mastery**
- Level of autonomy commensurate with experience and competence
- Flexibility and respectfulness upon employee potential
- Expanding job skills, employee strengths, and interests

**Purpose**
- Conflict resolution, grievance, and anonymous commenting procedures available and encouraged

**Autonomy**
- Level of autonomy commensurate with experience and competence
- Flexibility and respectfulness upon employee potential
- Expanding job skills, employee strengths, and interests

**Connectedness**
- Conflict resolution, grievance, and anonymous commenting procedures available and encouraged

---

The Critical Role of Positive Incentives in Reducing Insider Threat

February 2017

© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.
Vision: Extending the Traditional Security Paradigm

Balanced Deterrence: Extending the Traditional Security Paradigm

- Fewer unintended consequences
- Satisfaction, performance, retention

Balanced Deterrence

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

Security Through Positive Incentives
- Engagement Feedback
- Engagement
- Connectedness
- Connected Employees
- Organizational Supportiveness
- Supported Employees

Traditional Security Approach (Negative Incentives)
- Deterrence Feedback
- Deterrence
- Deterred Abuse
- Restriction
- Prevented Abuse
- Monitoring
- Detected Abuse
- Sanctions
- Punished Abuse
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 Buttles

**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

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

• For more details on this research see “The Critical Role of Positive Incentives in Reducing Insider Threat,”
Categories of Negative Unintended Consequences in Insider Threat Programs (InTP)*

1. Interference with legitimate whistleblower processes and protections
2. InTP management/employee relationships
3. InTP management’s lack or loss of interest in the InTP
4. Purposeful Misuse of the InTP by its staff or other employees
5. Accidental Misuse of the InTP by its staff or other employees

Research Context

Insider Threat Defense

Prevent Insider Misbehavior

Detect and Respond to At-Risk Insider Behaviors

Detect and Respond to At-Risk Organizational Conditions

Prevent using Positive Incentives

Positive deterrence (i.e., no detection)

Detection of organizational conditions conducive to insider threat

Detect and Respond to At-Risk Insider Behaviors

Prevent using Negative Incentives

Negative deterrence (i.e., no detection)

Early detection with possible positive or negative response

A form of negative incentive
Insider Incident Case Study Analysis

How engaged, connected, and supported are insider threat actors?

- **Method:** Rate dimensions on 5-point Likert scales over three time periods
  - For example, for Job Engagement

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>Actively Disengaged</td>
</tr>
<tr>
<td>-1</td>
<td>Mildly Disengaged</td>
</tr>
<tr>
<td>0</td>
<td>Neither Engaged nor Disengaged</td>
</tr>
<tr>
<td>+1</td>
<td>Mildly Engaged</td>
</tr>
<tr>
<td>+2</td>
<td>Thoroughly Engaged</td>
</tr>
</tbody>
</table>

- **Challenge:** Assessing insider perceptions through observables (w/o interview)
- **Results:** (3 prominent incidents)
  - Dimensions became increasingly negative over time, with some fluctuation
    - *Organizational Support* most strongly negative in all 3 incidents
    - *Job Engagement* negative in 2 out of 3 incidents
    - *Connectedness at Work* negative in 1 out of 3 incidents

- **Initial Decision:** Focus on perceived organizational support as foundation.
Future 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

**Adoption**
- Determine how organizations can
  - determine an appropriate mix of positive and negative incentives
  - transition to that from their current state