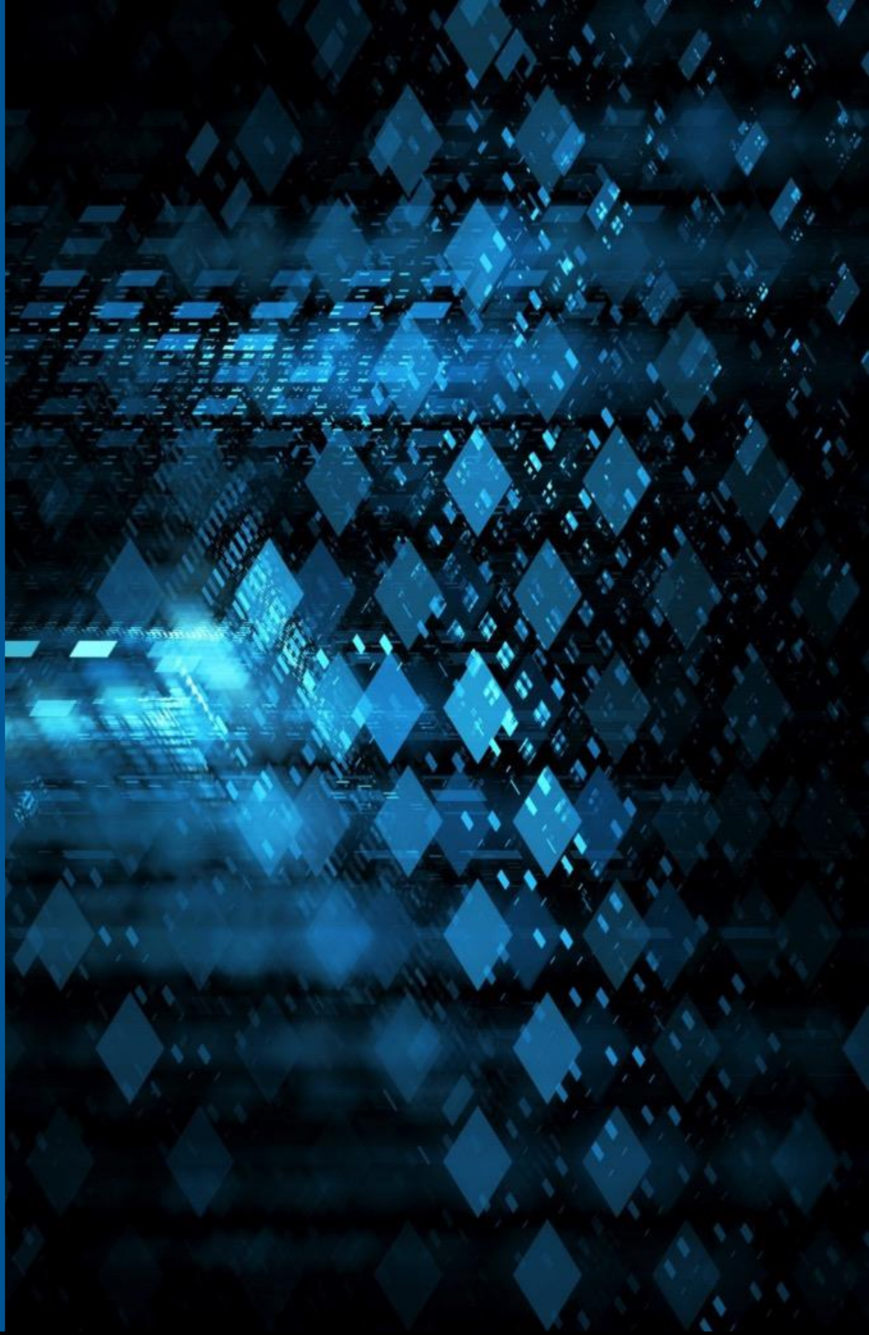
The Critical Role of Positive Incentives in Reducing Insider Threat

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



Copyright

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.

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

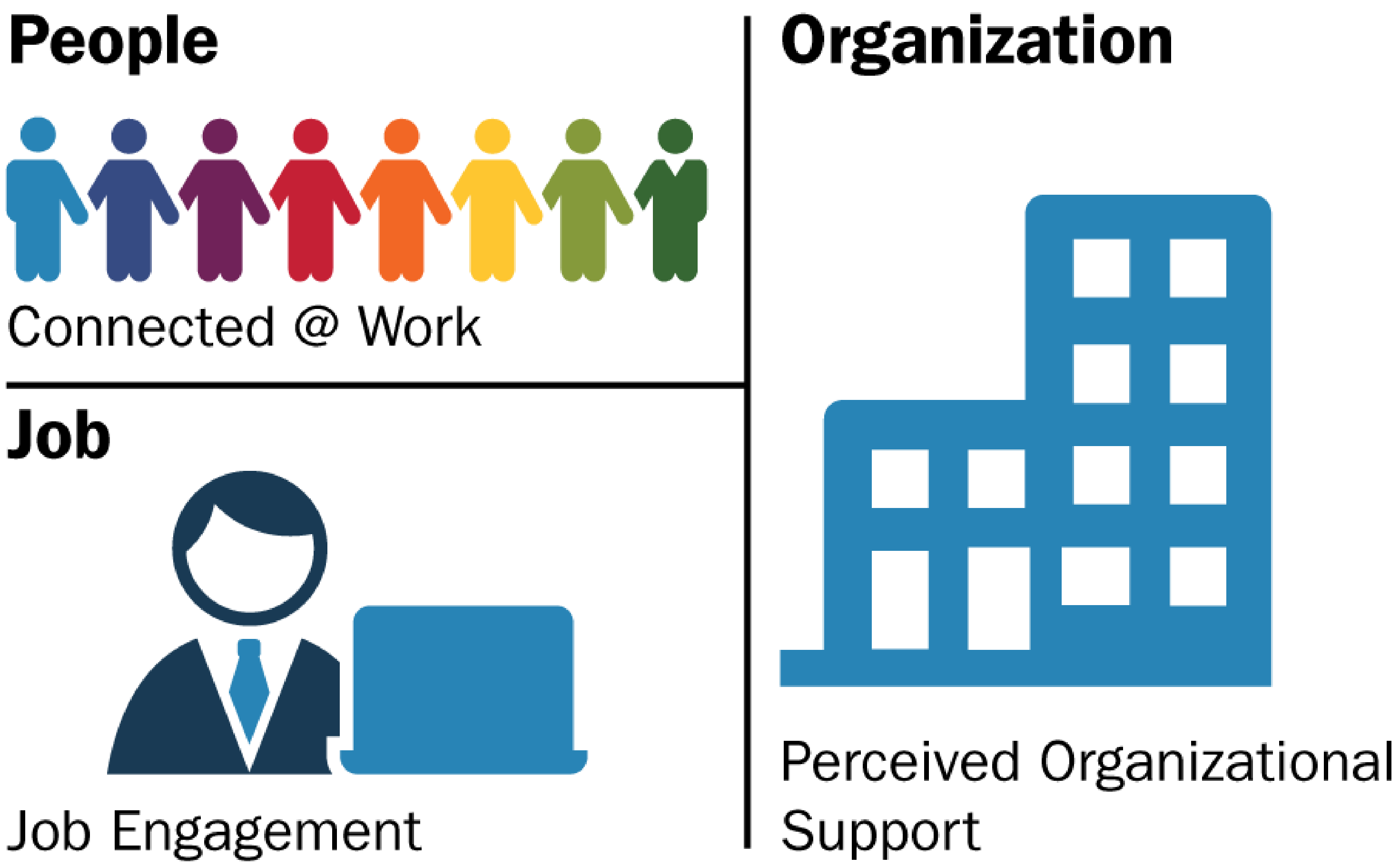
Negative incentives *alone* can *exacerbate* the threat they are intended to mitigate*

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

* See "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," SEI Digital Library, March 2015. http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

Three Dimensions of Employee-Organization Alignment



People

Connected @ Work

Job

Job Engagement

Organization

Perceived Organizational Support

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

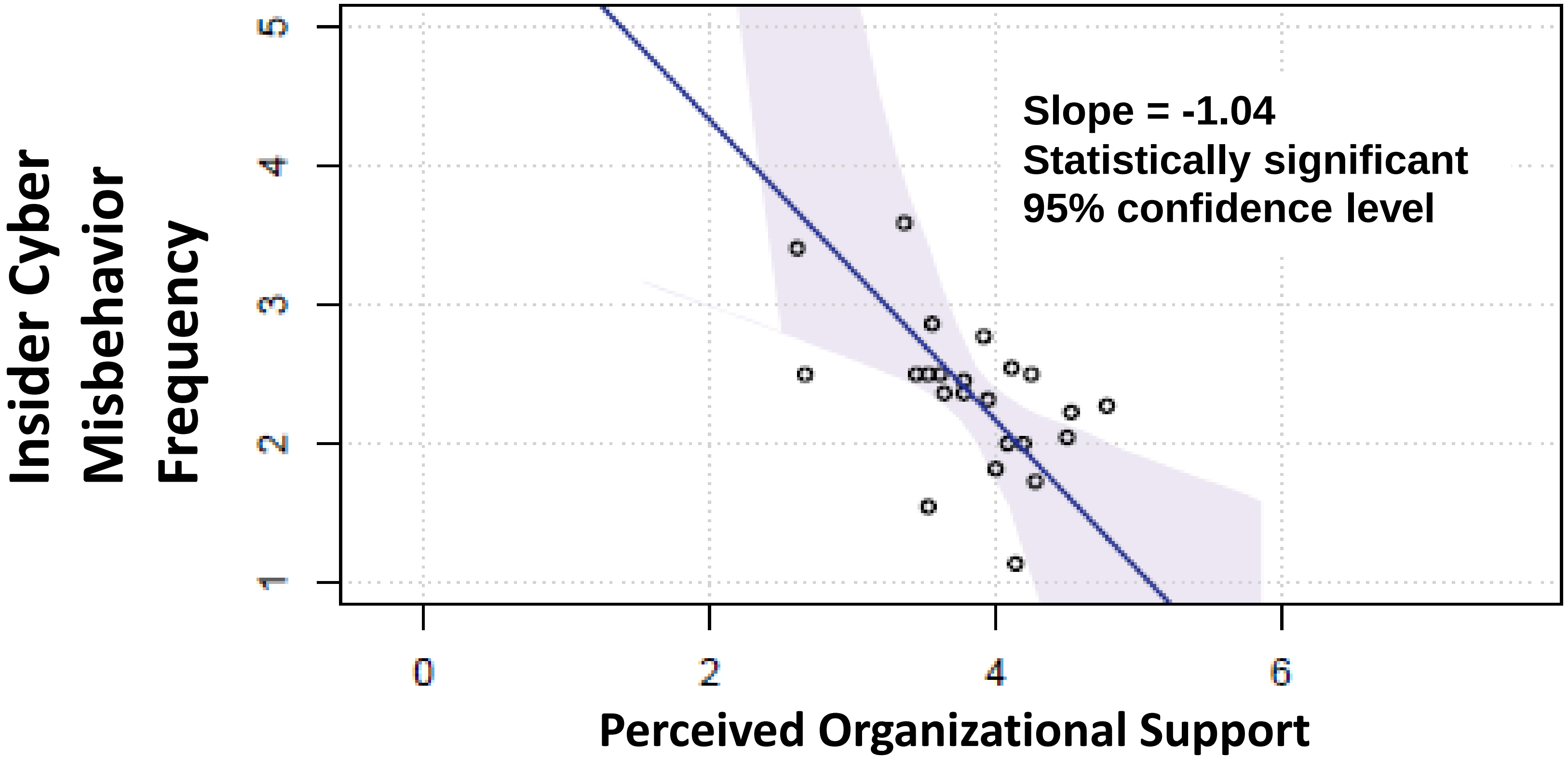
- Cyber-related insider threat behaviors
- Organizations actively establishing insider threat programs

Organizational Survey

How much does organizational support influence insider cyber misbehavior?

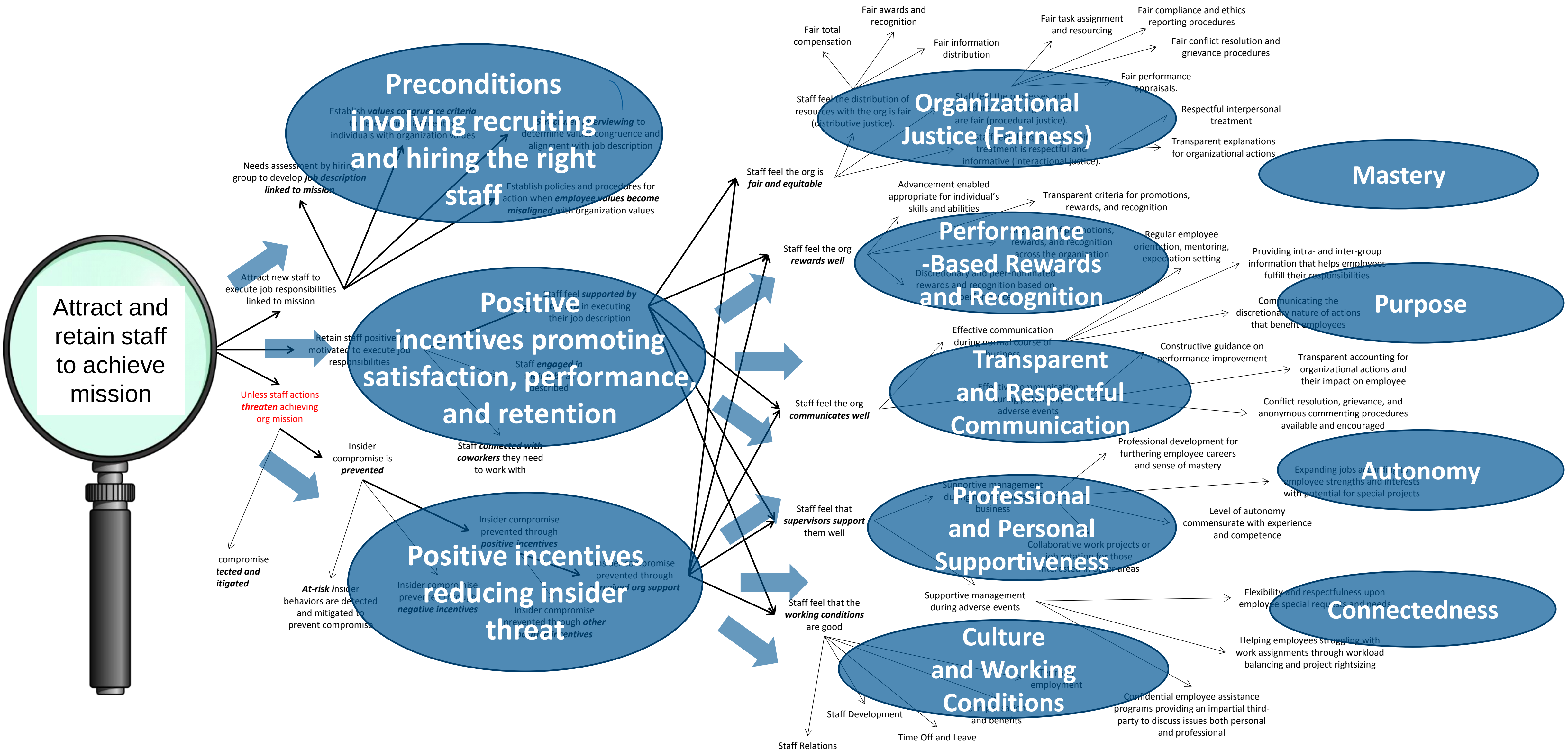
Method: Survey Open Source Insider Threat (OSIT) Information Sharing Group

Results: based on 23 out of ~90 organizations



Slope = -1.04
Statistically significant
95% confidence level

Positive Incentive-Based Principles and Practice Areas



Attract and retain staff to achieve mission

Attract new staff to execute job responsibilities linked to mission

Retain staff positively motivated to execute job responsibilities

Unless staff actions ***threaten*** achieving org mission

Preconditions involving recruiting and hiring the right staff

Needs assessment by hiring group to develop ***job description linked to mission***

Establish ***values congruence criteria*** to determine alignment of individuals with organization values

Structured interviewing to determine values congruence and alignment with job description

Establish policies and procedures for action when ***employee values become misaligned*** with organization values

Positive incentives promoting satisfaction, performance, and retention

Staff feel ***supported by the org*** in executing their job description

Staff ***engaged in*** [illegible] described

Staff ***connected with coworkers*** they need to work with

Insider compromise is ***prevented***

compromise ***tected and itigated***

At-risk insider behaviors are detected and mitigated to prevent compromise

Positive incentives reducing insider threat

Insider compromise prevented through ***positive incentives***

Insider compromise prevented through ***negative incentives***

Insider compromise prevented through ***perceived org support***

Insider compromise prevented through ***other positive incentives***

Staff feel the org is ***fair and equitable***

Organizational Justice (Fairness)

Staff feel the distribution of resources with the org is fair (distributive justice).

Staff feel the processes and procedures in the organization are fair (procedural justice).

Staff feel the quality of their treatment is respectful and informative (interactional justice).

Fair total compensation

Fair awards and recognition

Fair information distribution

Fair task assignment and resourcing

Fair compliance and ethics reporting procedures

Fair conflict resolution and grievance procedures

Fair performance appraisals.

Respectful interpersonal treatment

Transparent explanations for organizational actions

Staff feel the org ***rewards well***

Performance-Based Rewards and Recognition

Advancement enabled appropriate for individual's skills and abilities

Transparent criteria for promotions, rewards, and recognition

Alignment of promotions, rewards, and recognition across the organization

Discretionary and peer-nominated rewards and recognition based on performance

Regular employee orientation, mentoring, expectation setting

Staff feel the org ***communicates well***

Transparent and Respectful Communication

Effective communication during normal course of business

Effective communication during potentially adverse events

Providing intra- and inter-group information that helps employees fulfill their responsibilities

Communicating the discretionary nature of actions that benefit employees

Constructive guidance on performance improvement

Transparent accounting for organizational actions and their impact on employee

Conflict resolution, grievance, and anonymous commenting procedures available and encouraged

Staff feel that ***supervisors support*** them well

Professional and Personal Supportiveness

Supportive management during normal course of business

Collaborative work projects or job rotation for those interested in other areas

Professional development for furthering employee careers and sense of mastery

Level of autonomy commensurate with experience and competence

Supportive management during adverse events

Flexibility and respectfulness upon employee special requests and needs

Helping employees struggling with work assignments through workload balancing and project rightsizing

Confidential employee assistance programs providing an impartial third-party to discuss issues both personal and professional

Staff feel that the ***working conditions*** are good

Culture and Working Conditions

Terms of employment

Compensation and benefits

Staff Development

Time Off and Leave

Staff Relations

Mastery

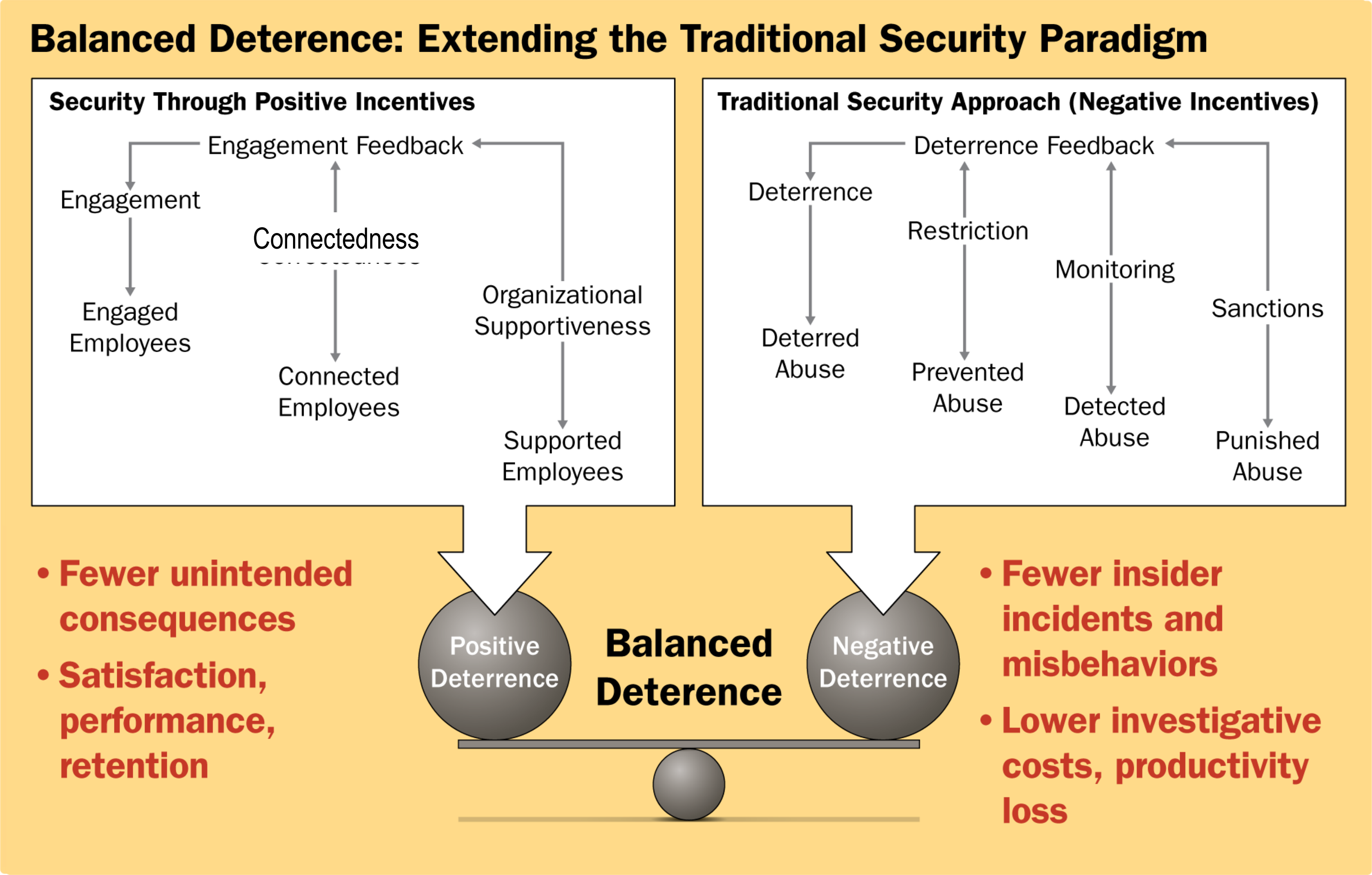
Purpose

Autonomy

Expanding jobs according to employee strengths and interests with potential for special projects

Connectedness

Vision: Extending the Traditional Security Paradigm



Balanced Deterence: Extending the Traditional Security Paradigm

Security Through Positive Incentives

Engagement Feedback

Engagement → Engaged Employees

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

- Fewer unintended consequences
- Satisfaction, performance, retention

Positive Deterrence

Balanced Deterence

Negative Deterrence

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

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

***Contributors* :**

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,” *SEI Technical Report CMU/SEI-2016-TR-014*, December 2016. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484929.pdf

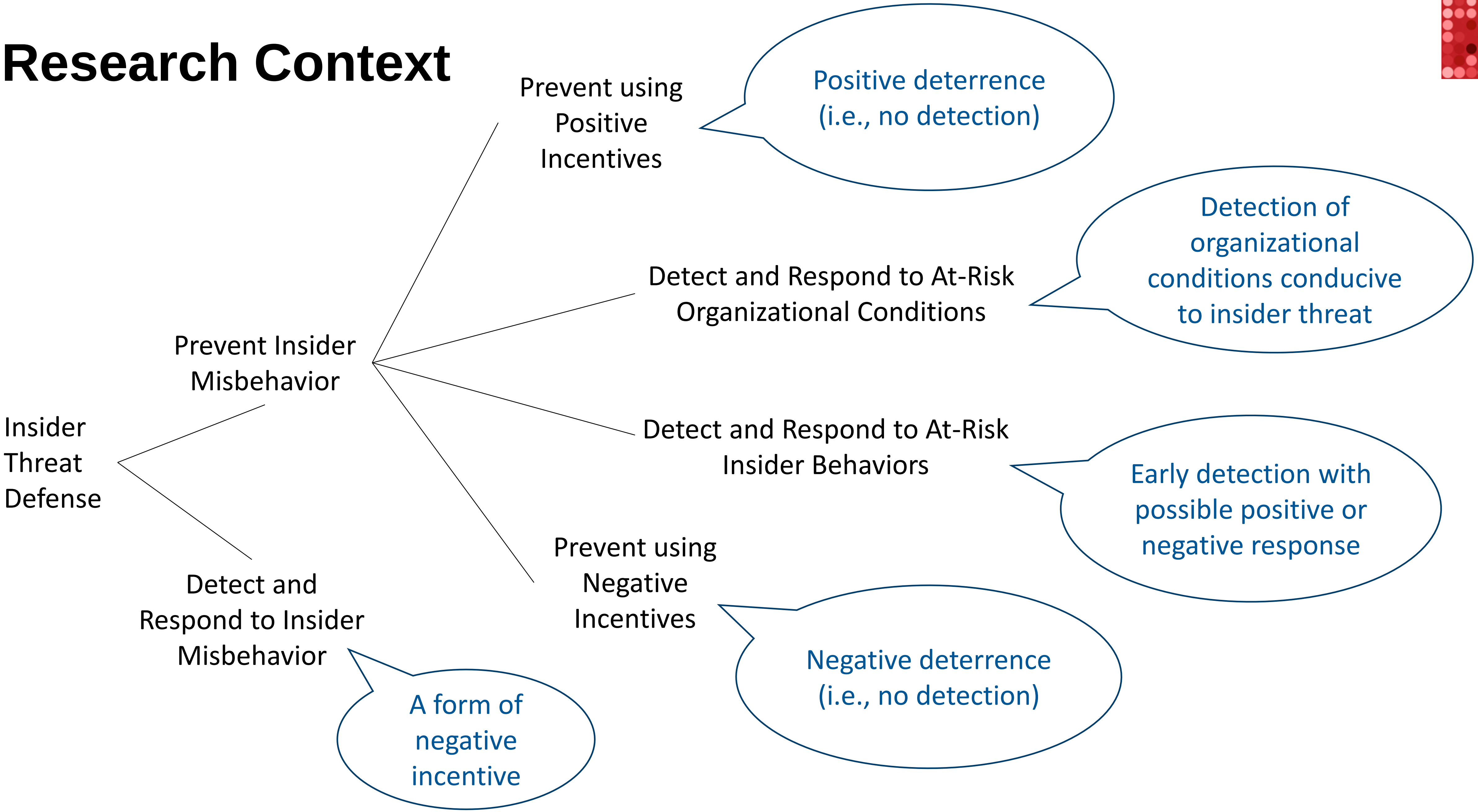
Backups

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

* See "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," SEI Digital Library, March 2015. http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

Research Context



Insider Threat Defense

Prevent Insider Misbehavior

Prevent using Positive Incentives

Positive deterrence (i.e., no detection)

Detect and Respond to At-Risk Organizational Conditions

Detection of organizational conditions conducive to insider threat

Detect and Respond to At-Risk Insider Behaviors

Early detection with possible positive or negative response

Prevent using Negative Incentives

Negative deterrence (i.e., no detection)

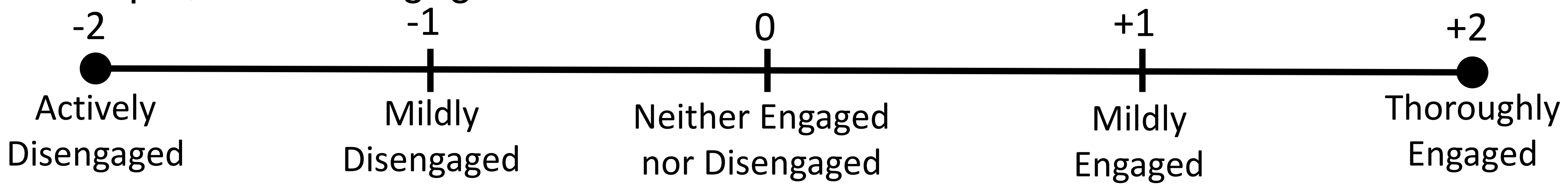
Detect and Respond to Insider Misbehavior

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



-2 Actively Disengaged

-1 Mildly Disengaged

0 Neither Engaged nor Disengaged

+1 Mildly Engaged

+2 Thoroughly Engaged

- **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