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

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. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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

Positive Incentives

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

Employee Constraints, Monitoring, Punishment

Focus on Employee Strengths, Fair & Respectful Treatment

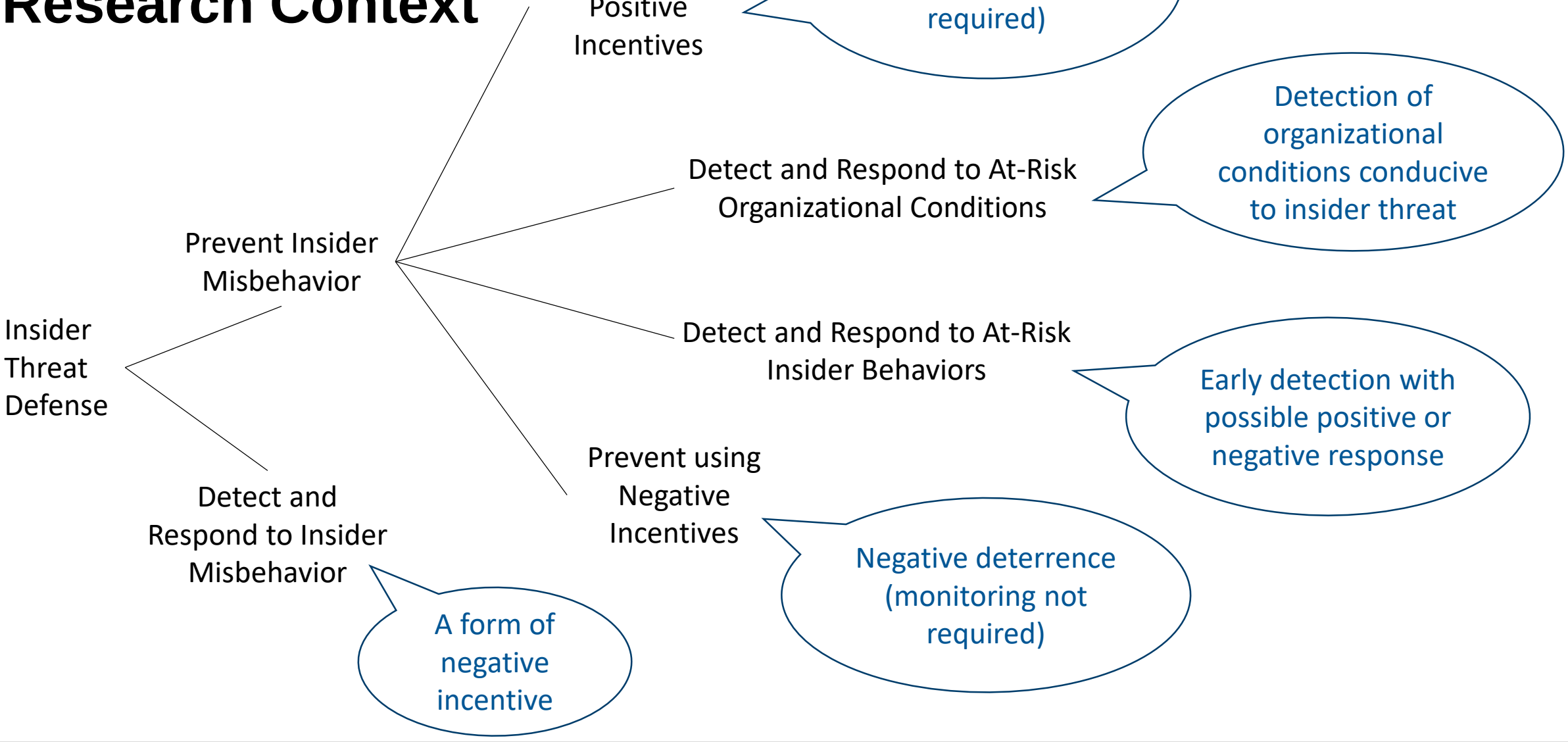
Negative incentives *alone* can *exacerbate* the threat they are intended to mitigate*

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

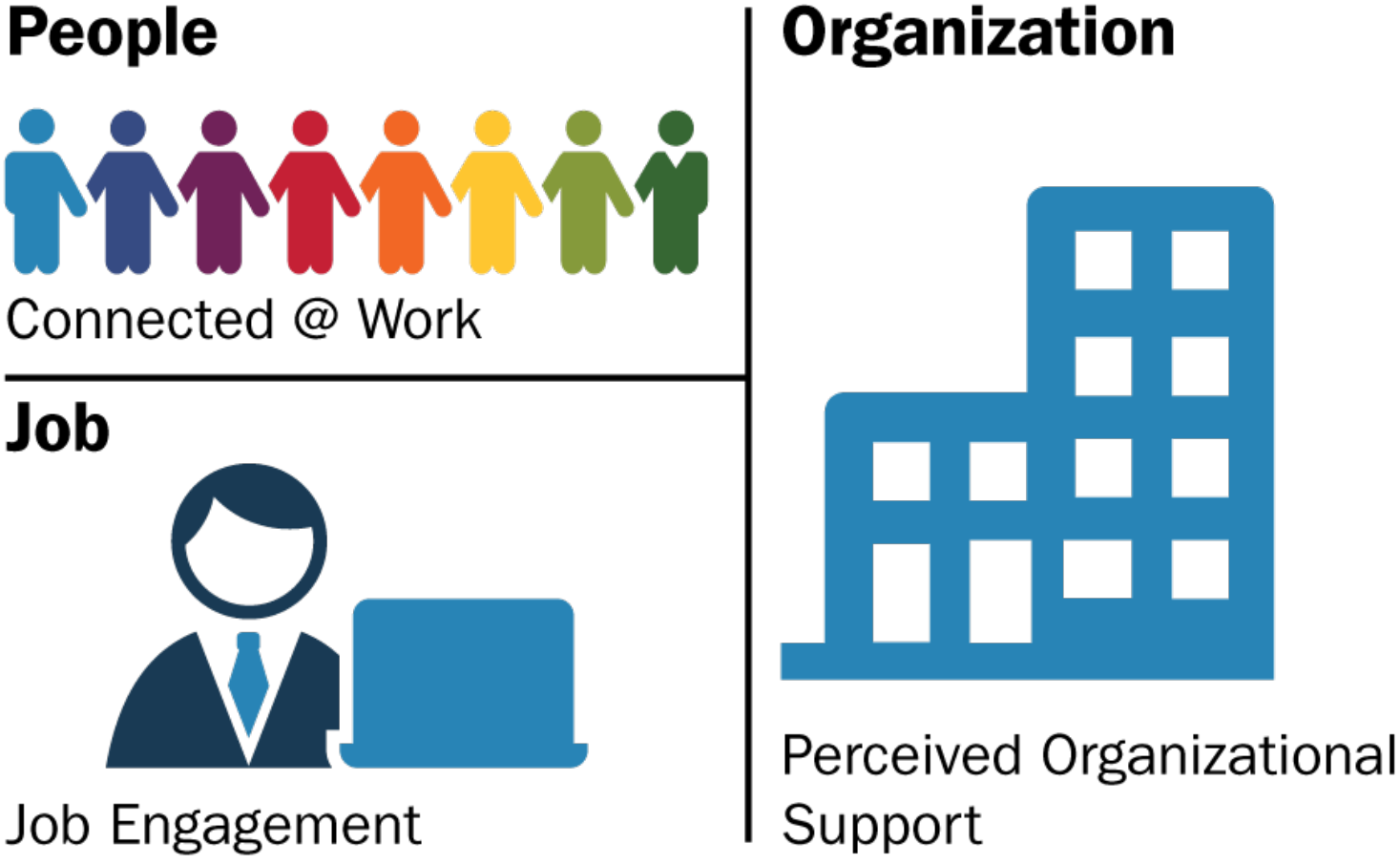
Initial Scope: Disgruntlement-spurred threat

* See "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," SEI Digital Library, March 2015.

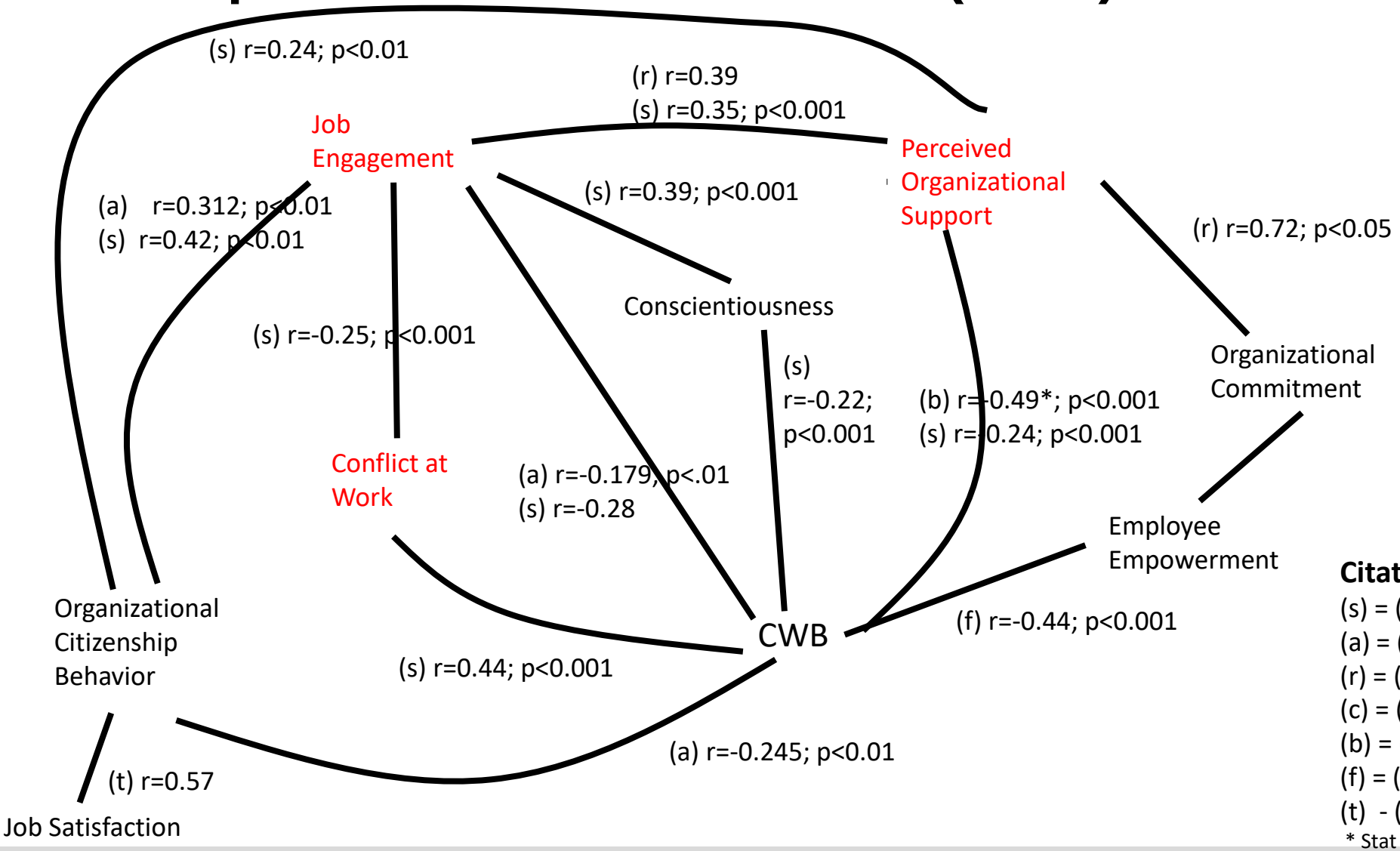
Insider Threat Research Context



Three Broad Categories of Positive Incentives



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

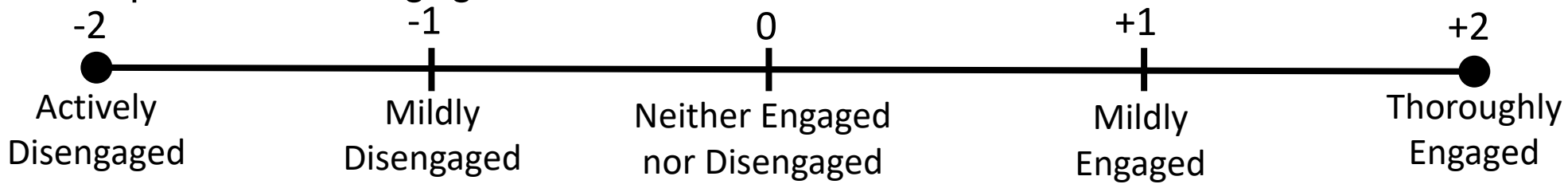
- Cyber-related insider threat behaviors
- Organizations actively establishing insider threat programs

* 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

Insider Incident Case Study Analysis (Exploratory)

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



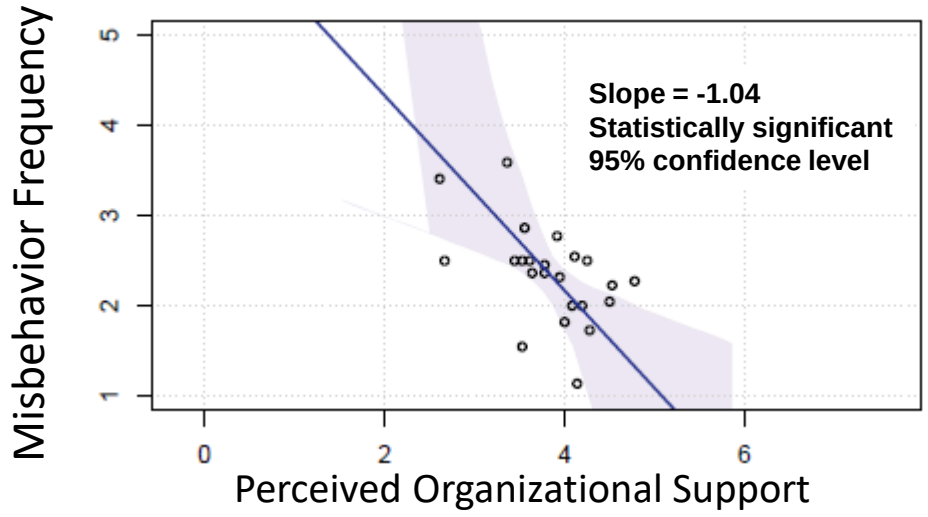
- **Challenge:** Assessing insider perceptions through observables (w/o interview)
- **Results:** (3 prominent incidents)
  - Dimensions became increasingly negative over time, with some fluctuation
    - *Organizational Support* most strongly negative in all 3 incidents
    - *Job Engagement* negative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

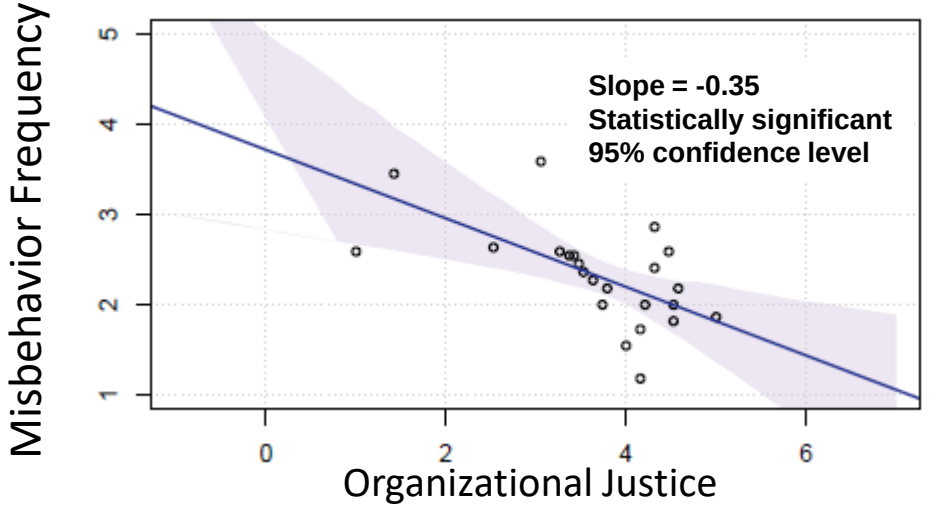
Organizational Survey

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.

Surveyed Items on Insider Cyber Misbehaviors (Intentional)

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

Descriptive Stats: Insider Cyber Misbehaviors

Frequency Rating

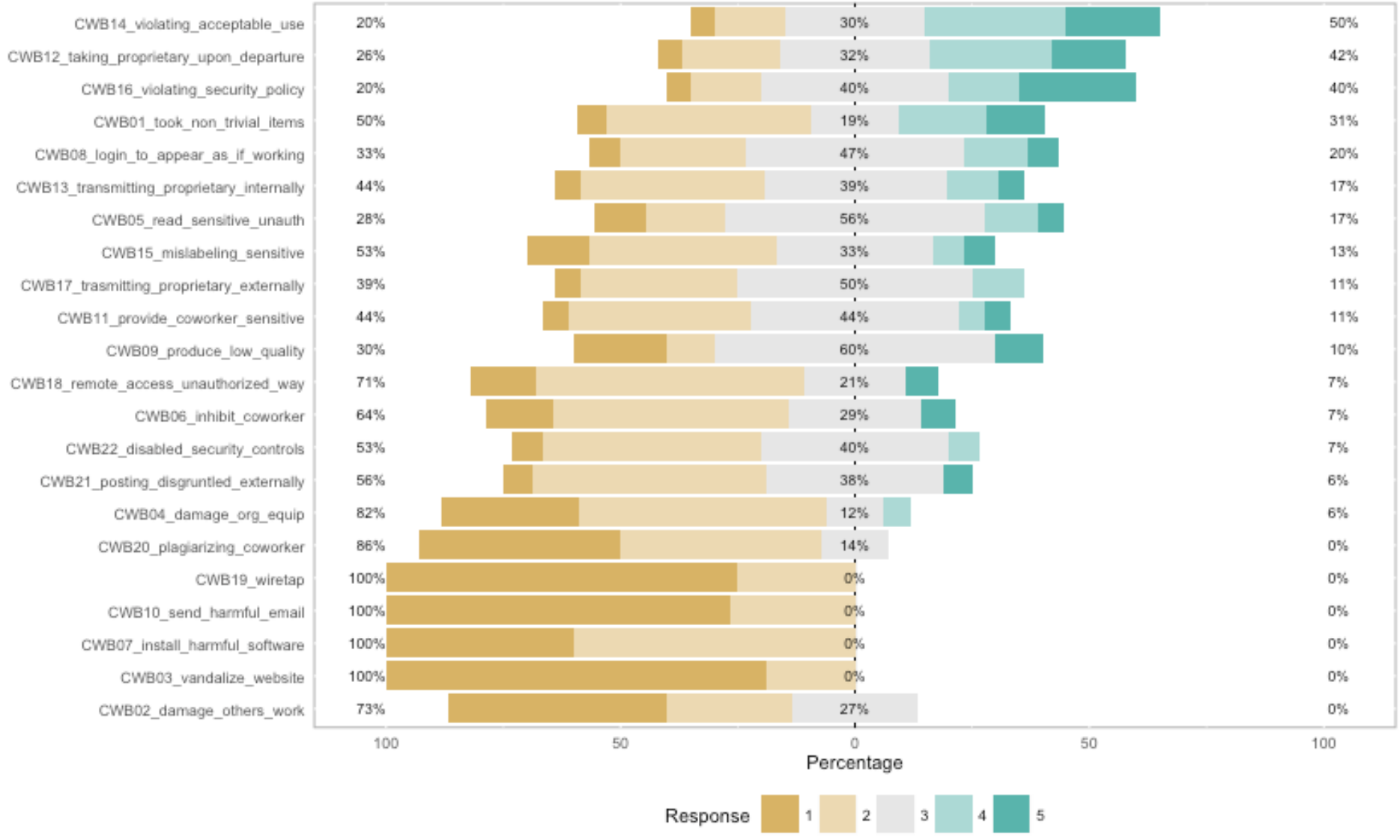
5: All the time
- At least once daily

4: Often
- At least once a week

3: Sometimes
- At least every other month

2: Occasionally
- At least once a year

1: Never



Limitations and Directions

Insider Threat Incident Analysis

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

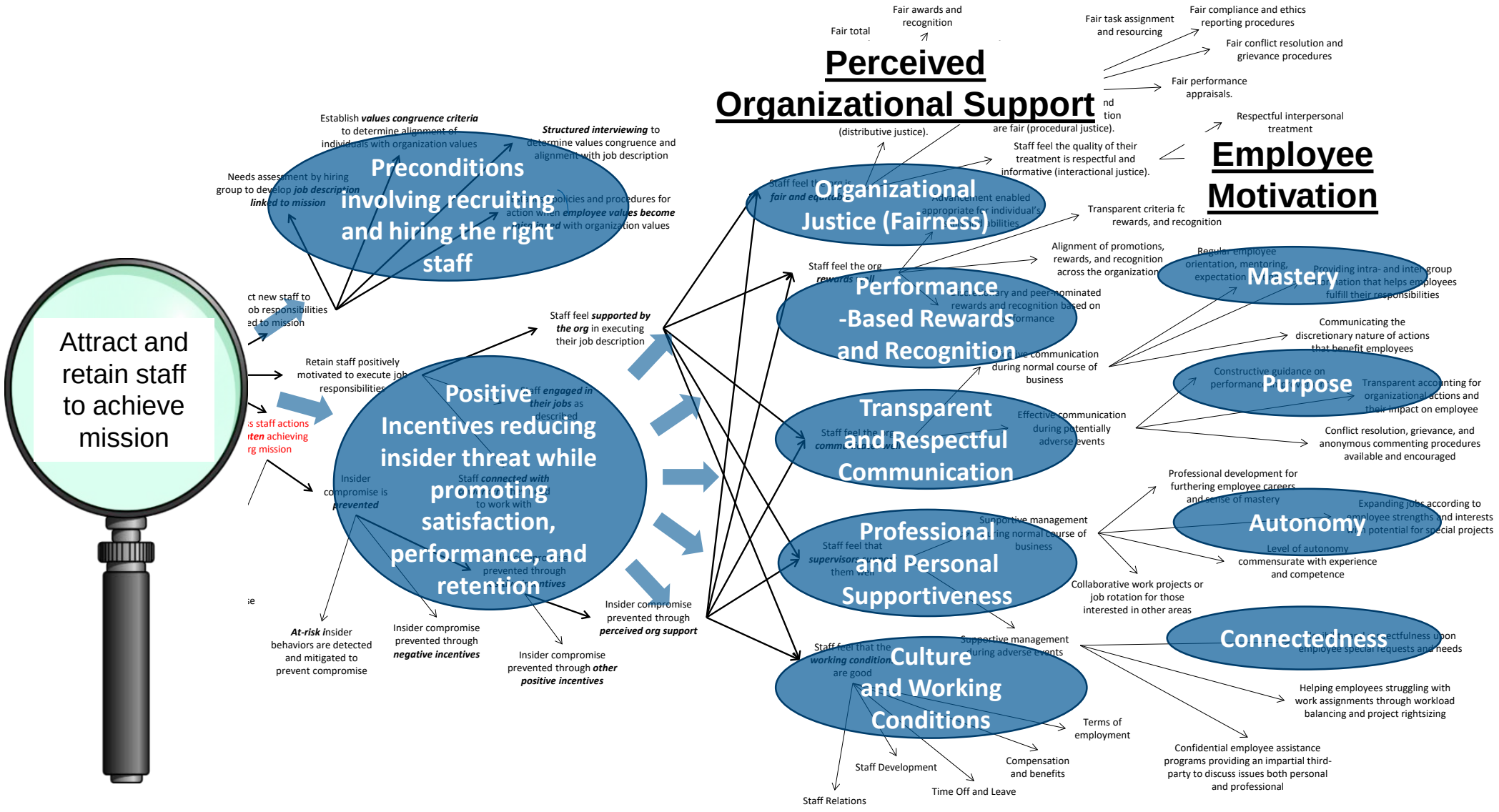
Organizational Survey

- 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



Monitoring and Response (Examples)

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

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

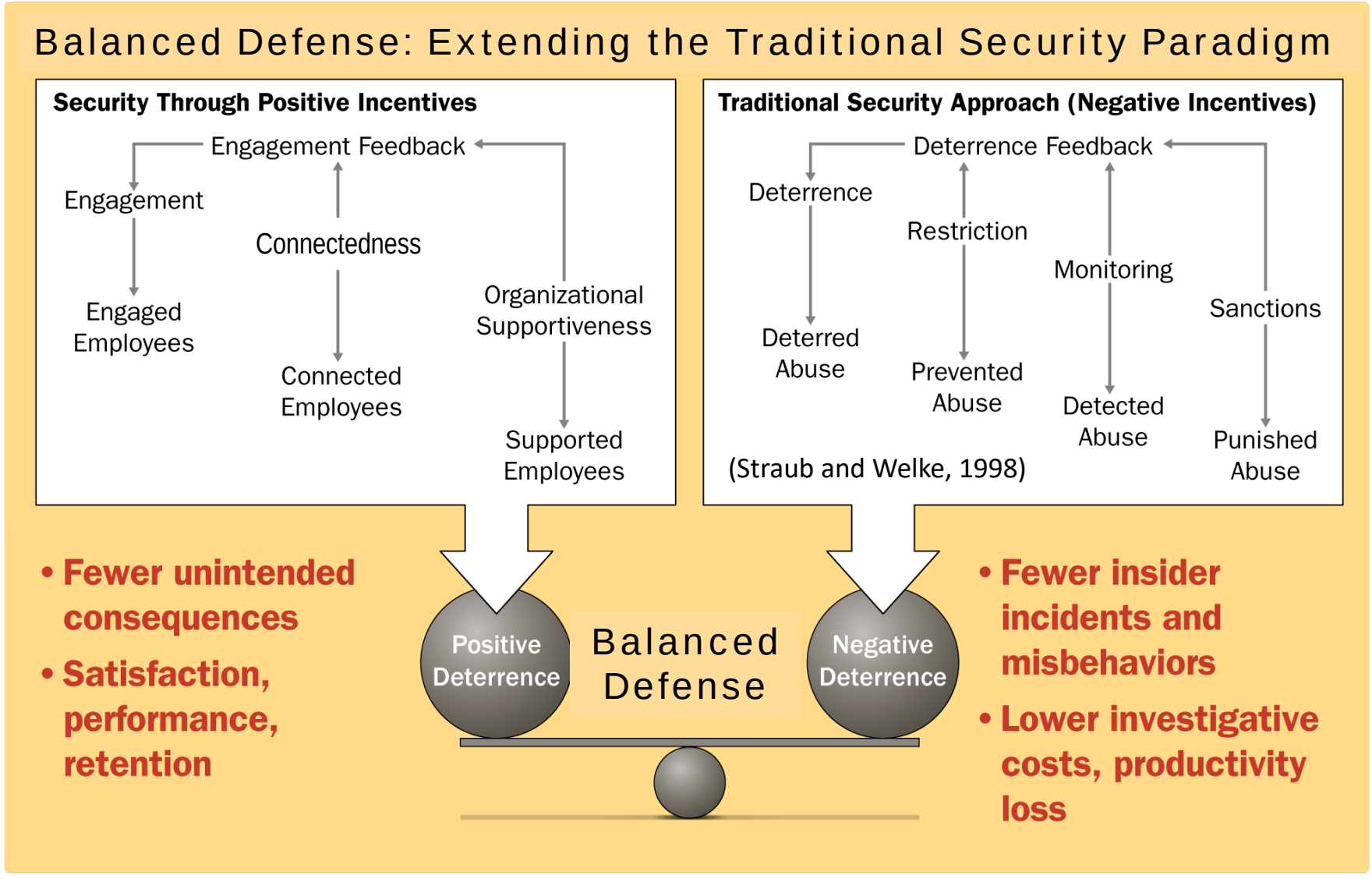
Options:

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

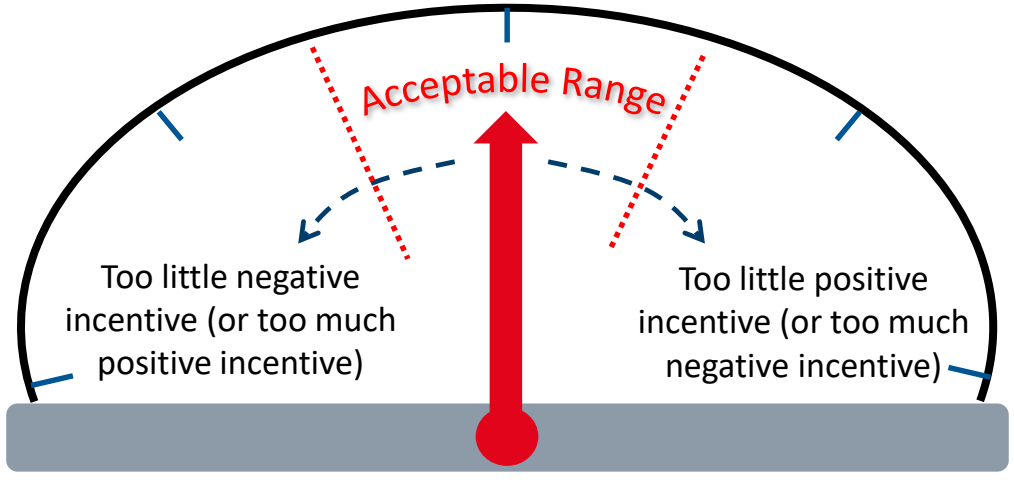


Conceptualizing a Metric for Balanced Defense

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

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

***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

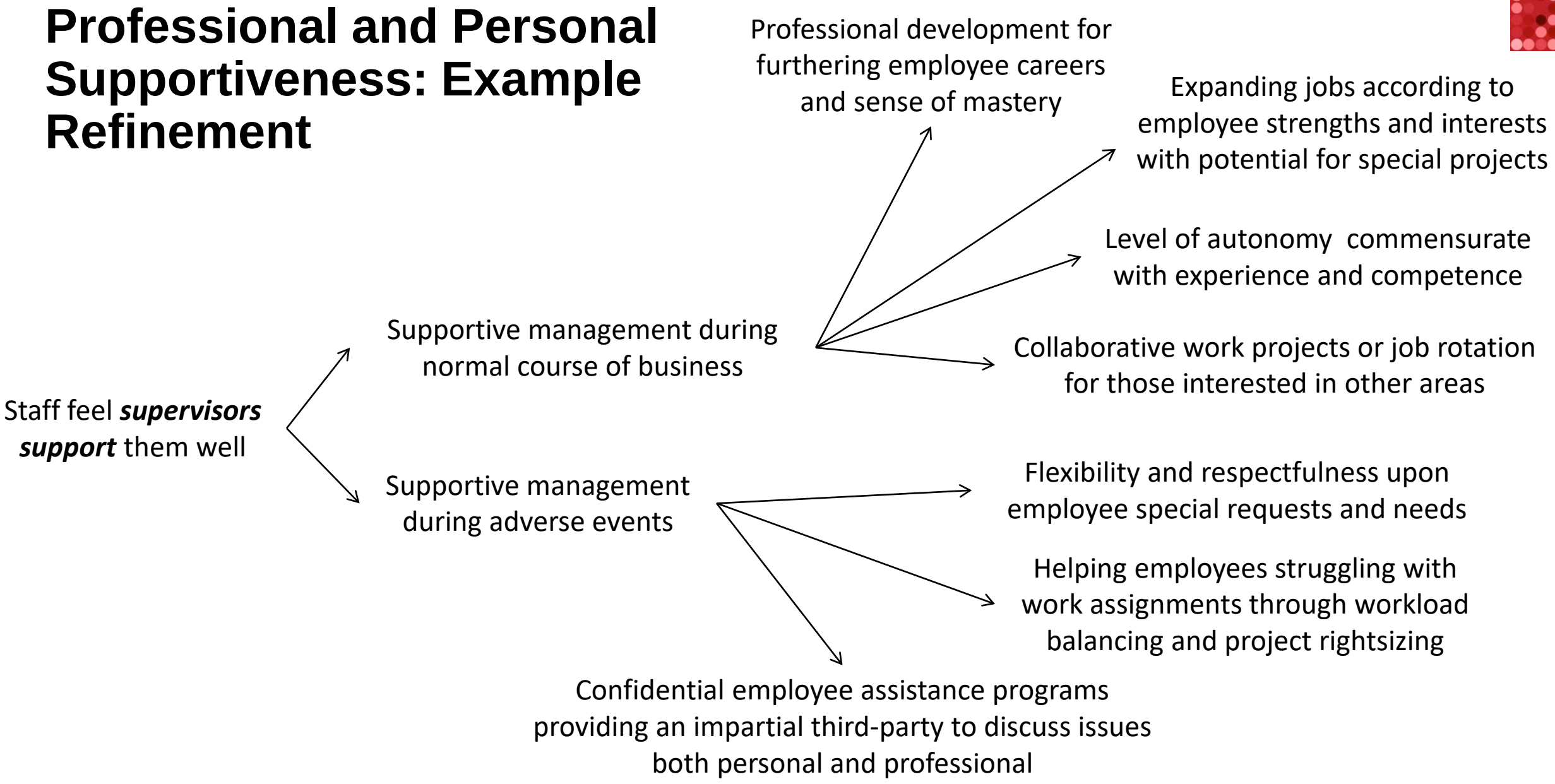
Life Dimensions Coaching and Counseling:

Susan B. Moore

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

* For more details on insider threat research see http://www.cert.org/insider-threat. For specifics of 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

Professional and Personal Supportiveness: Example Refinement



References

Ariani, D. W. (2013). The Relationship between Employee Engagement, Organizational Citizenship Behavior, and Counterproductive Work Behavior. *International Journal of Business Administration, 4*. doi:10.5430/ijba.v4n2p46

Bordia, P., Restubog, S. L. D., & Tang, R. L. (2008). When employees strike back: investigating mediating mechanisms between psychological contract breach and workplace deviance. *Journal of Applied Psychology, 93*(5), 1104. Retrieved from http://psycnet.apa.org/journals/apl/93/5/1104/

(CERT 2010) Insider Threat Conceptual Framework: Groupings and Definitions, *Software Engineering Institute Special Report,* December 2010.

Colbert, A. E., Mount, M. K., Harter, J. K., Witt, L. A., & Barrick, M. R. (2004). Interactive effects of personality and perceptions of the work situation on workplace deviance. *Journal of Applied Psychology, 89*(4), 599.

Fatima, A., Iqbal, M. Z., & Imran, R. (2013). Organizational Commitment and Counterproductive Work Behavior: Role of Employee Empowerment. In *Proceedings of the Sixth International Conference on Management Science and Engineering Management* (pp. 665-679). Springer London.

Rhoades, L., Eisenberger, R., & Armeli, S. (2001). Affective commitment to the organization: the contribution of perceived organizational support. *Journal of Applied Psychology, 86*(5), 825.

Sulea, C., Virga, D., Maricutoiu, L. P., Schaufeli, W., Dumitru, C. Z., & Sava, F. A. (2012). Work engagement as mediator between job characteristics and positive and negative extra-role behaviors. *Career Development International, 17*, 188-207. doi:10.1108/13620431211241054

Tang, T. L. P., & Ibrahim, A. H. S. (1998). Antecedents of organizational citizenship behavior revisited: Public personnel in the United States and in the Middle East. *Public Personnel Management*, *27*(4), 529-550.