



# The Critical Role of Positive Deterrence in Managing Insider Risk

Andrew P. Moore

CMU/SEI Insider Risk Management Symposium

Arlington, Virginia

August 14, 2024

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2024 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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](mailto:permission@sei.cmu.edu).

DM24-0946

# Three Types of Influence of the Workforce\*

## Compliance

- Influence due to desire to gain specific rewards

## Identification

- Influence due to desire to establish or maintain a satisfying relationship with the organization

## Internalization

- Influence due to congruence of individual and organizational goals and values

Command  
and Control  
(C&C)

Positive  
Deterrence  
(PD)

Depends on

- Pressure through extrinsic motivation
- Organizations' prevention through constraints and detection through monitoring and response

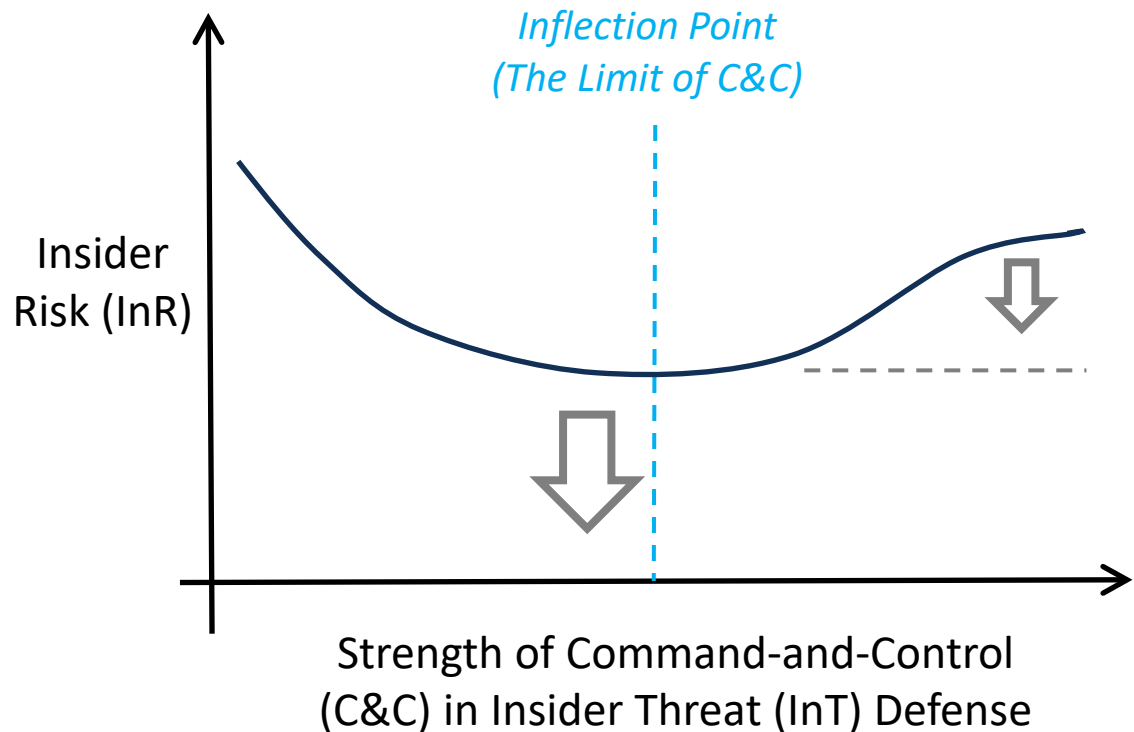
Depends on

- Attraction through intrinsic motivation
- Individual's instinctive response, aka, self regulation

\* [Kelman 1958, O'Reilly 1986]

Positive deterrence is defined as a set of evidence-based workforce practices promoting the mutual interests of employees and their organization in ways that reduce insider risk (InR). [Moore 2022] "Reducing Insider Risk through Positive Deterrence"

# The Limits of Command-and-Control (C&C) of InR\*



- Excessive C&C can exacerbate InR
- Shape of curve depends on organization (mission, culture, etc.)
  - Adding positive deterrence (PD)
    - will change the shape of this curve
    - will reduce risk due to excessive command-and-control
    - BUT PD will also tend to shift the whole curve downward to lower levels of risk

\* [Moore 2015] “Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls”

# Three Categories of Positive Deterrence-Related Practices

## People



Connected @ Work

## Job



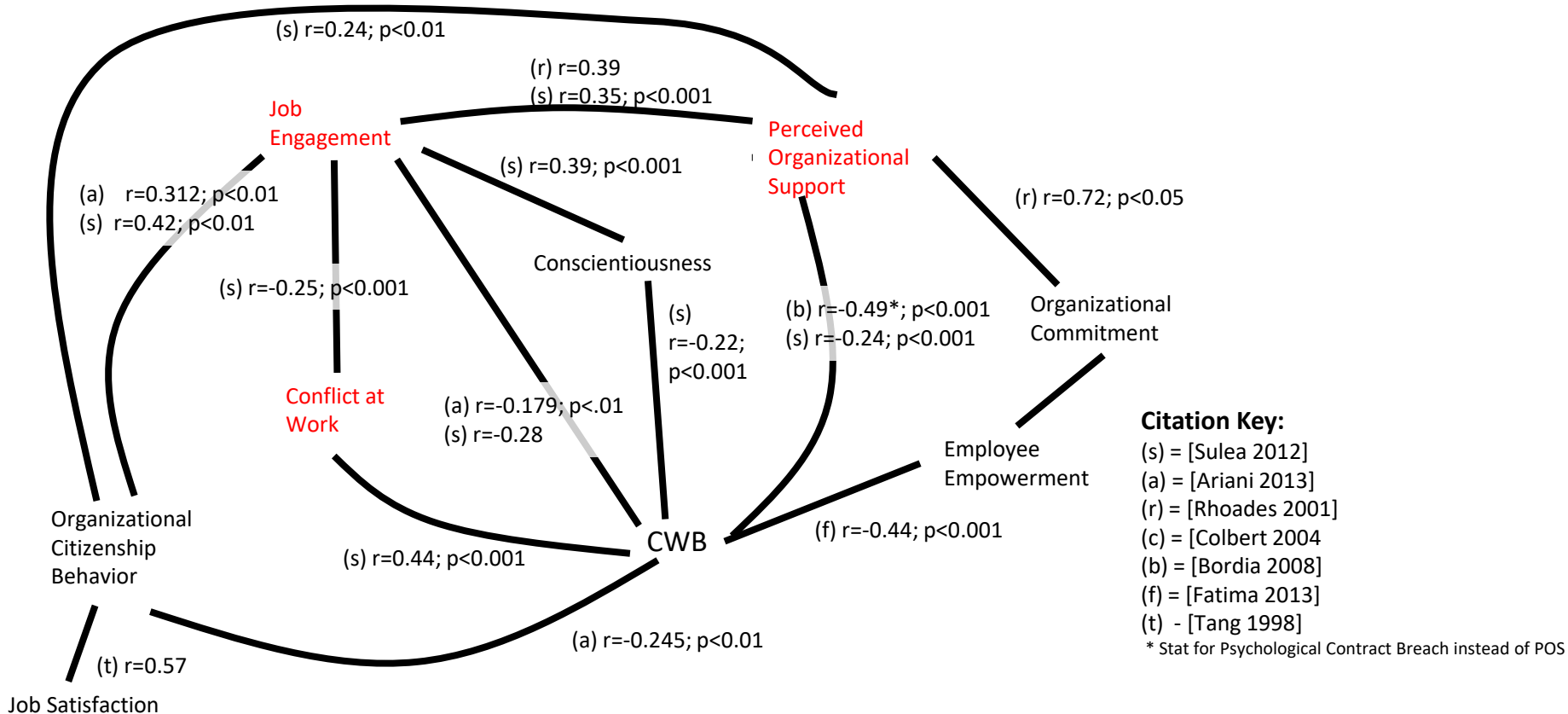
Job Engagement

## Organization



Perceived Organizational  
Support (POS)

# Previous Studies in the Organizational Behavior Literature



# Previous CERT study relating POS and Insider Risk\*

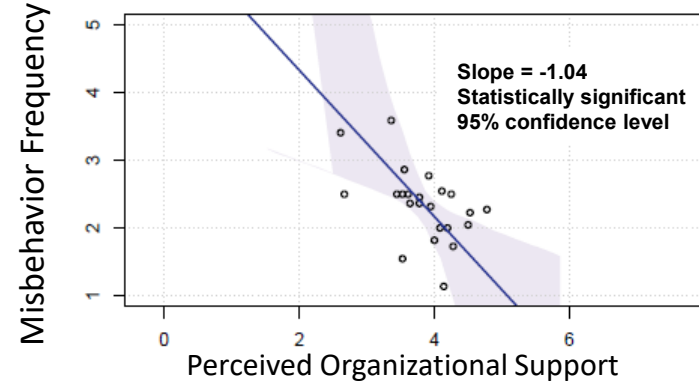
**POS:** the degree to which employees believe that their organization values their contributions and cares about their well-being

**Research Question:** How much does POS influence insider cyber misbehavior?

**Method:** Exploratory survey of Open Source Insider Threat (OSIT) Information Sharing Group

- Independent variable on existing 5-point scale
  - *Perceived organizational support* (36 quest.)
- Dependent variable on 5-point frequency scale
  - *Cyber misbehavior* from case data (22 quest.)

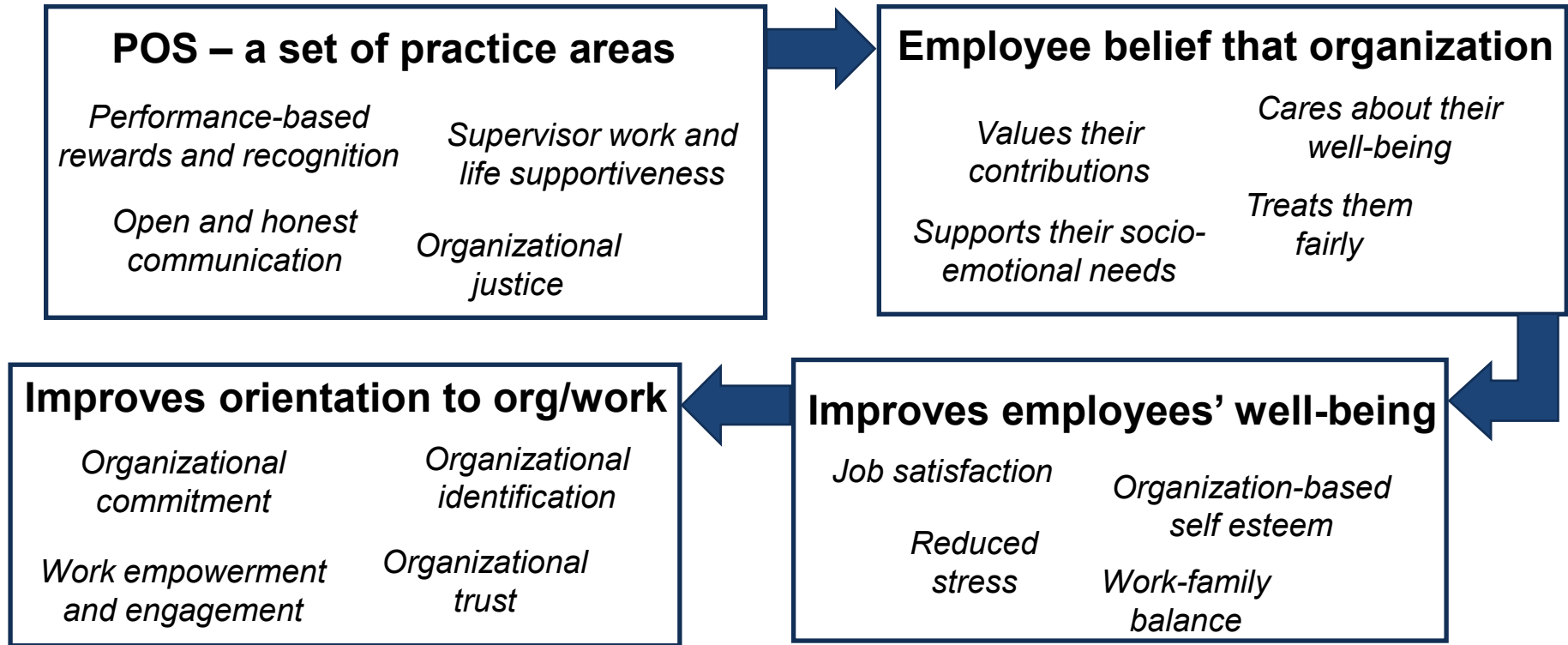
**Results:** 23 responses (out of 90)



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

\* [Moore 2018]

# Perceived Organizational Support (POS) as Positive Deterrence\*



\* [Eisenberger 2011] "Perceived Organizational Support: Fostering Enthusiastic and Productive Employees"

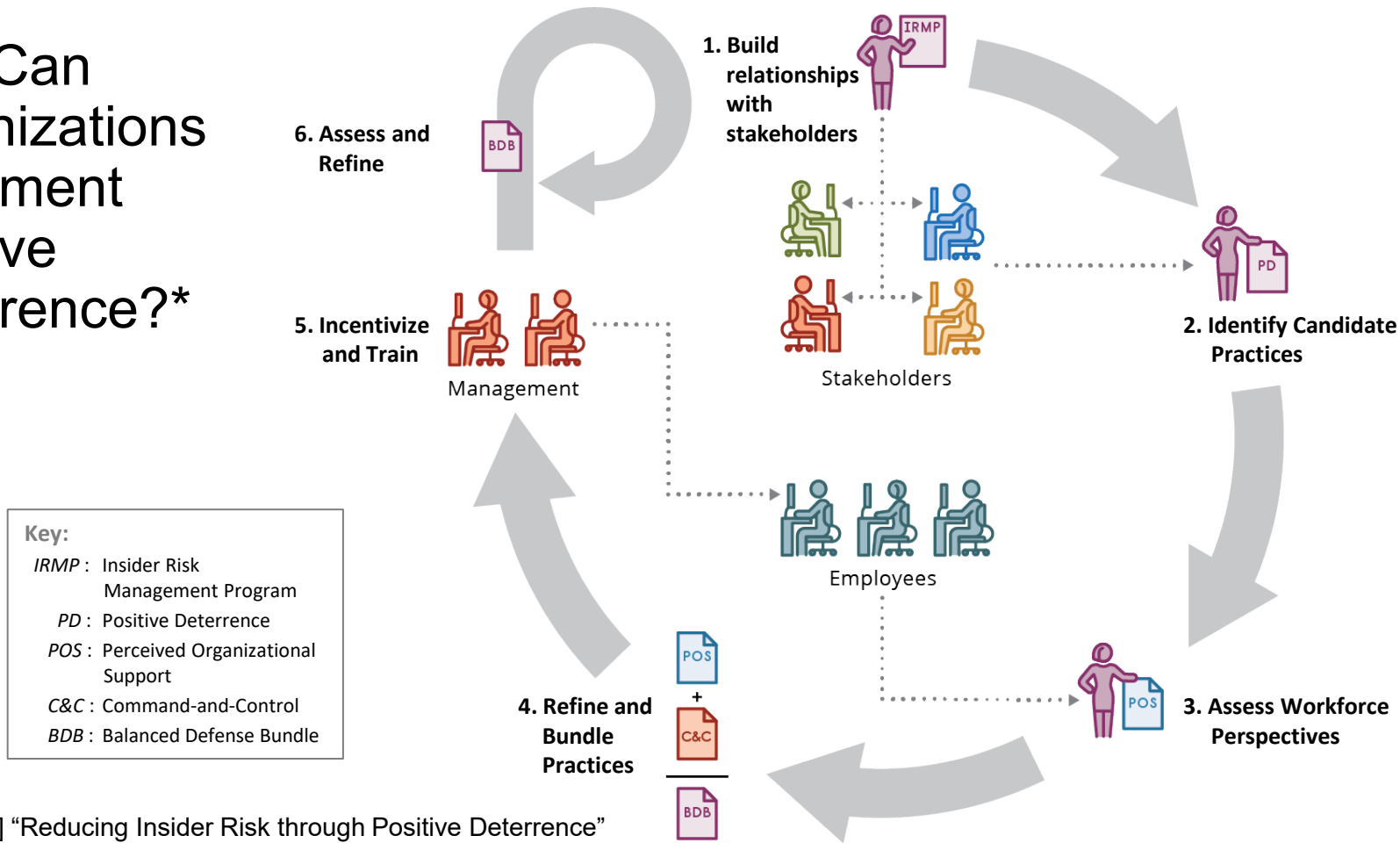


# Why Augment Command-and-Control with Positive Deterrence?\*

1. Exclusive or excessive reliance on command-and-control can undermine workforce goodwill
2. Positive deterrence combined with command-and-control can reduce insider incident rates over command-and-control alone
3. Promoting positive deterrence significantly enhances the Insider Risk Management Program (IRMP) mission
4. Positive deterrence improves job performance generally

\* [Moore 2022] “Reducing Insider Risk through Positive Deterrence”

# How Can Organizations Implement Positive Deterrence?\*



\* [Moore 2022] "Reducing Insider Risk through Positive Deterrence"

# Balanced Defense Bundles

# Management Complementarities\*

Bundles exploit the notion of complementarities in the organizational management literature

- Complementary activities are ones for which “increases in the level of some activities raises the marginal profitability of the others.”

Complementarity is created when different practices

- make different contributions to attain a common outcome
- possibly through different psychological and social mechanisms

Evidence indicates that organizations exploiting complementarities are performance leaders.

\* [Milgrom 1992, Ennen 2010, Chadwick 2010, Subramony 2009]

# Example Human Resource Management (HRM) Bundles\*

## Empowerment-Enhancing Bundles

- Employee involvement in influencing work process
- Formal grievance procedure and complaint resolution
- Job enrichment (variety and responsibility)
- Self-managed or autonomous work groups
- Employee participation in decision making
- Systems to encourage feedback from employees

## Motivation-Enhancing Bundles

- Formal performance appraisal process
- Incentive plans (bonuses, profit-sharing, etc.)
- Linking pay to performance
- Opportunities for internal career mobility and promotions
- Health care and other employee benefits

*Meta-analysis provides evidence that these HRM bundles “have stronger <positive and synergistic> relationships with <positive> business outcomes than their individual HRM practices.”*

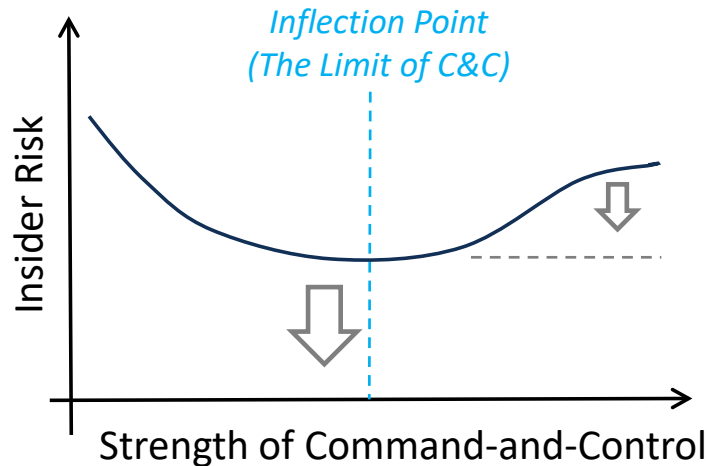
- *Outcomes: retention, operational performance, financial performance.*

\* [Subramony 2009] – “A Meta-Analytic Investigation of the Relationship Between HRM Bundles and Firm Performance”

# The “Too Much of a Good Thing” Effect in Management\*

Effect across many organizational management domains in which good management practices

- pushed to a limit become much less effective (the inflection point)
- and possibly start exhibiting negative outcomes



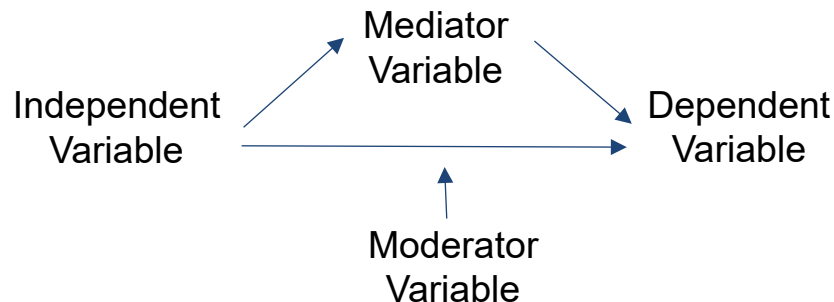
Data exhibits curvi-linearity with moderating variables influencing inflection point and shape of curve

Moderators (e.g., PD) can dampen the relationship between good practice (e.g., C&C) and negative outcomes

\* [Pierce 2011] “The Too-Much-of-a-Good-Thing Effect in Management”

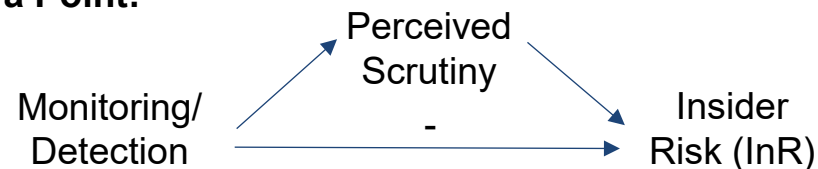
# Mediators and Moderators in Statistics

## Notation\*

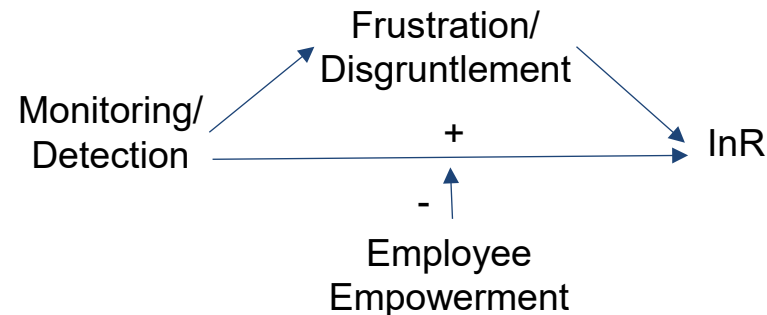


## Example\*\*

### Up to a Point:



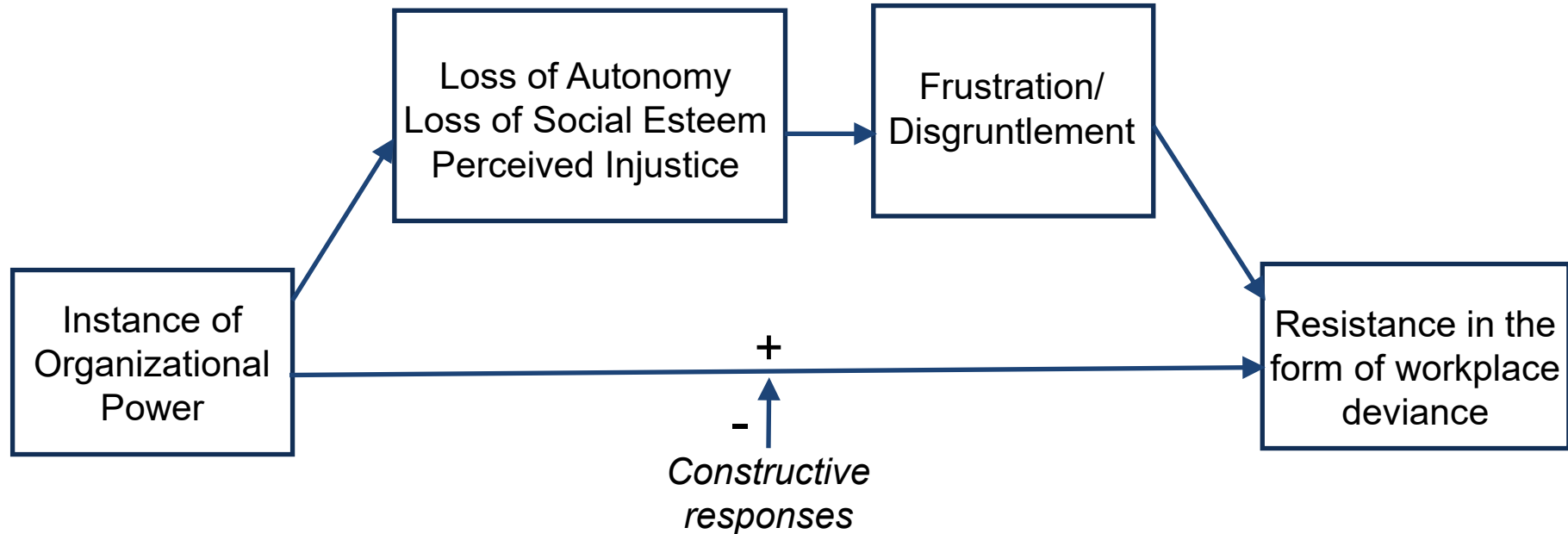
### Beyond that Point:



\* For a description of graphical notation for mediators and moderators see <https://www.scribbr.com/methodology/mediator-vs-moderator/>.

\*\* [Martin 2016] – “An Eye on Your Work: How Empowerment Affects the Relationship Between Electronic Surveillance and and Counterproductive Work Behaviors”

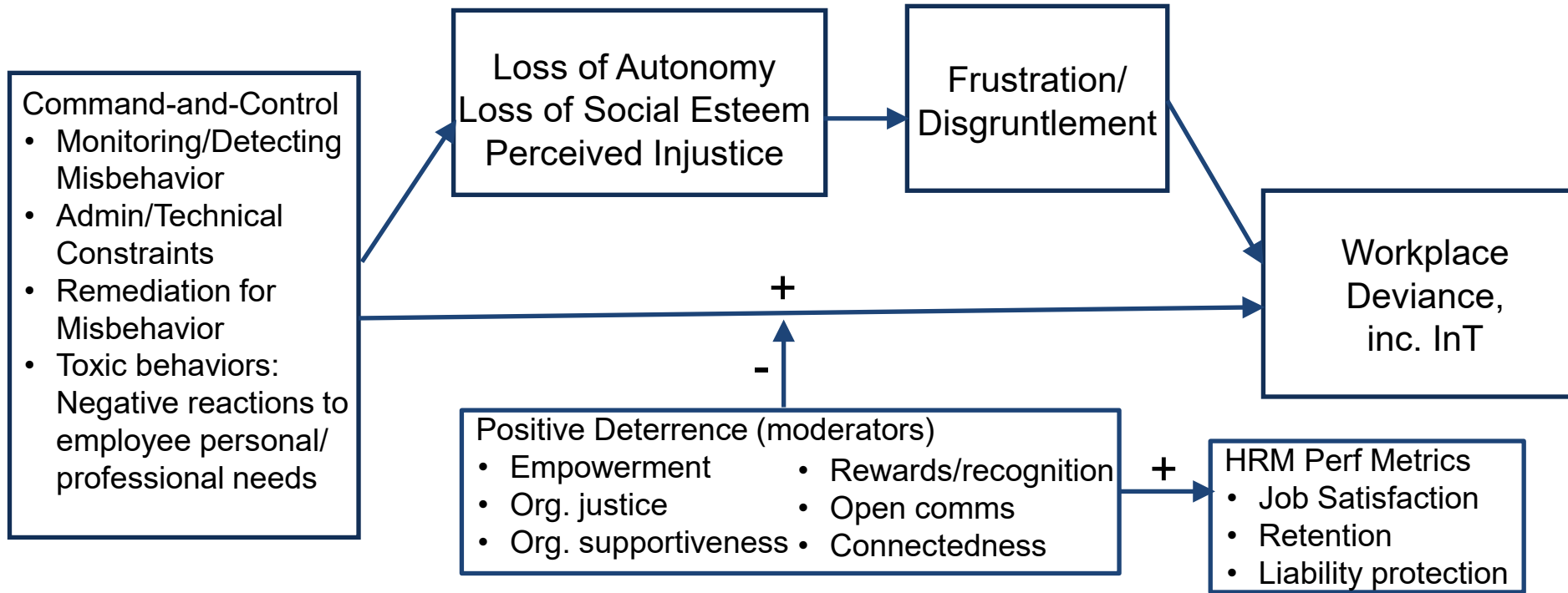
# Substantiated Relationships between Power and Deviance\*



\* [Lawrence 2007, Sims 2010, Faldetta 2021] – ‘Workplace Deviance as Organization Resistance’



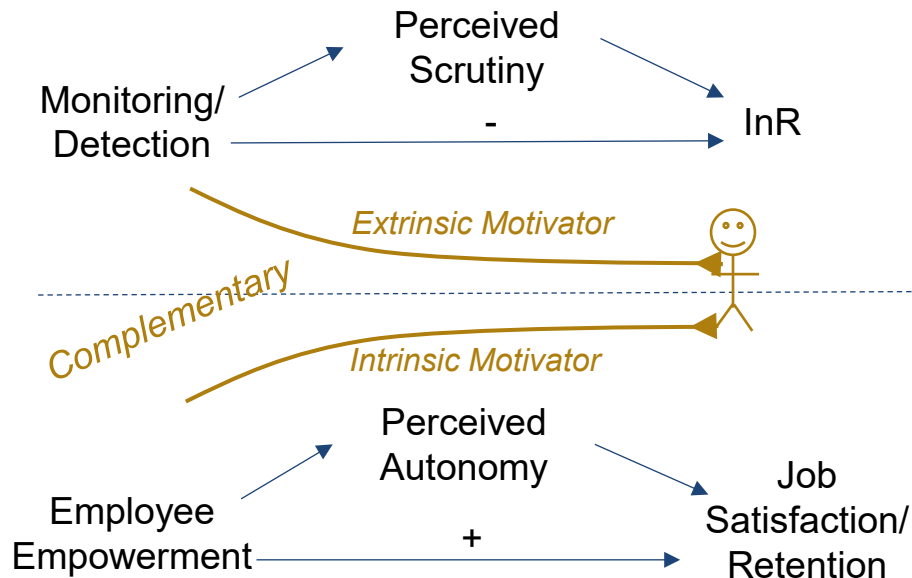
# Applying this to the Insider Risk Domain



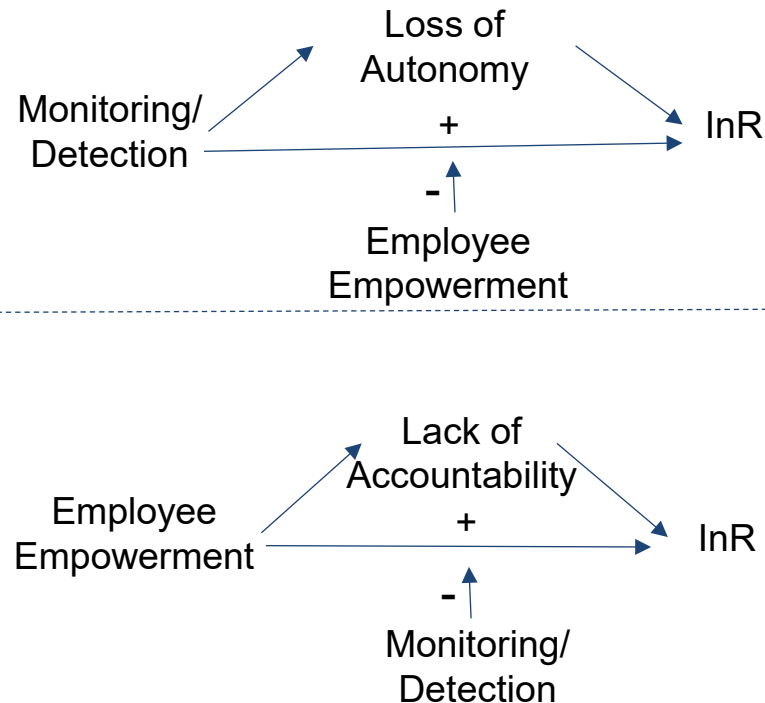
“Balanced Defense Bundles” combine C&C practice areas with moderating PD practice areas

# Bundling C&C and PD : Monitoring vs Empowerment\*

## Up to a Point:



## Beyond that Point:

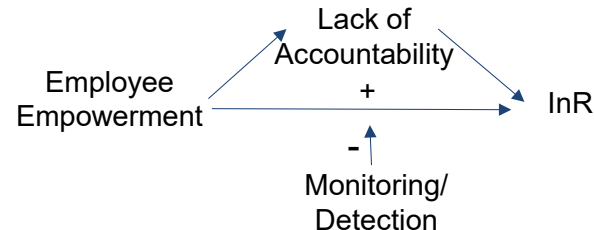
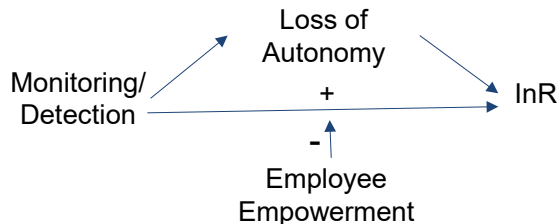


\* [Martin 2016] – ““An Eye on Your Work: How Empowerment Affects the Relationship Between Electronic Surveillance and and Counterproductive Work Behaviors”

# Efficient Complementarities\*

*“Complementarities commonly give rise to a variety of coherent strategies. Individual managers all acting with the firm’s interest in mind may get stuck with a coherent strategy that is not the best one for the firm. It takes conscious effort and centralized decision making in these cases to determine and focus attention on the proper strategy.”*

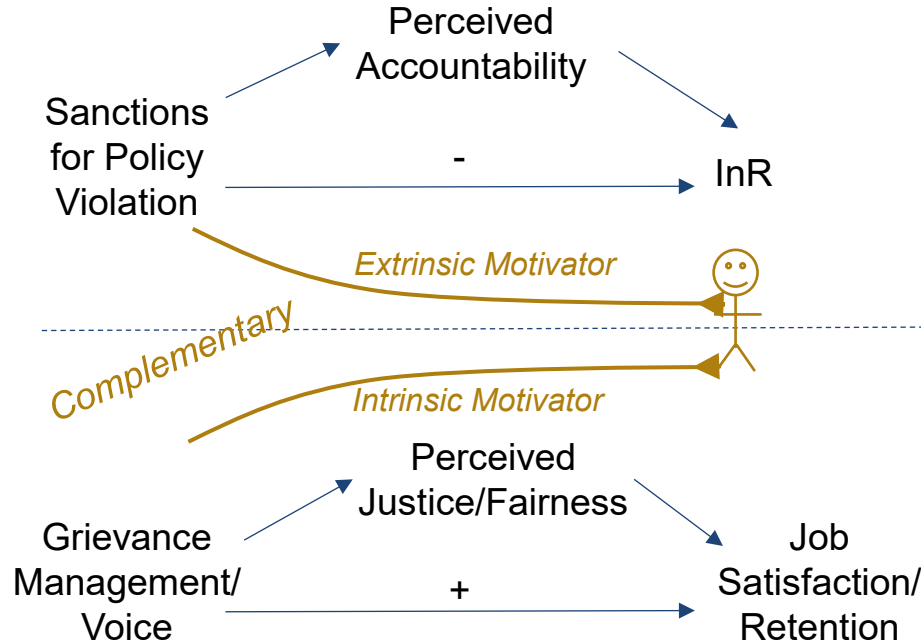
- Efficient complementarities enable “a more than a sum of it’s parts” benefit
  - Balanced Defense Bundles can have these properties
- Efficient complementarity occurs when “the effects of component HRM practices on system outcomes both moderate and are moderated by the effects of the other HRM practices in the system.”



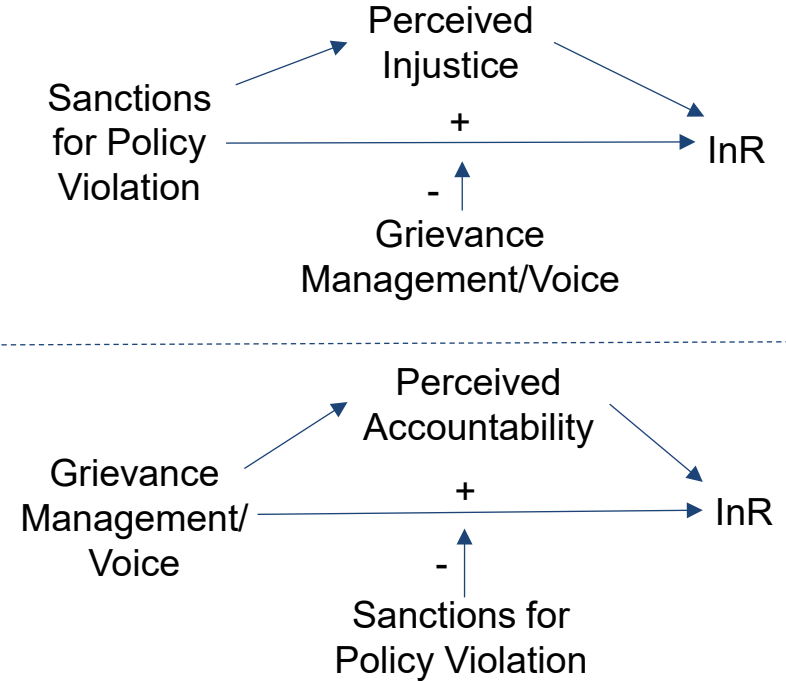
\* [Milgrom 1992, Chadwick 2010, Ennen 2009]

# Another Example : Sanctions vs. Grievance Management\*

## Up to a Point:



## Beyond that Point:

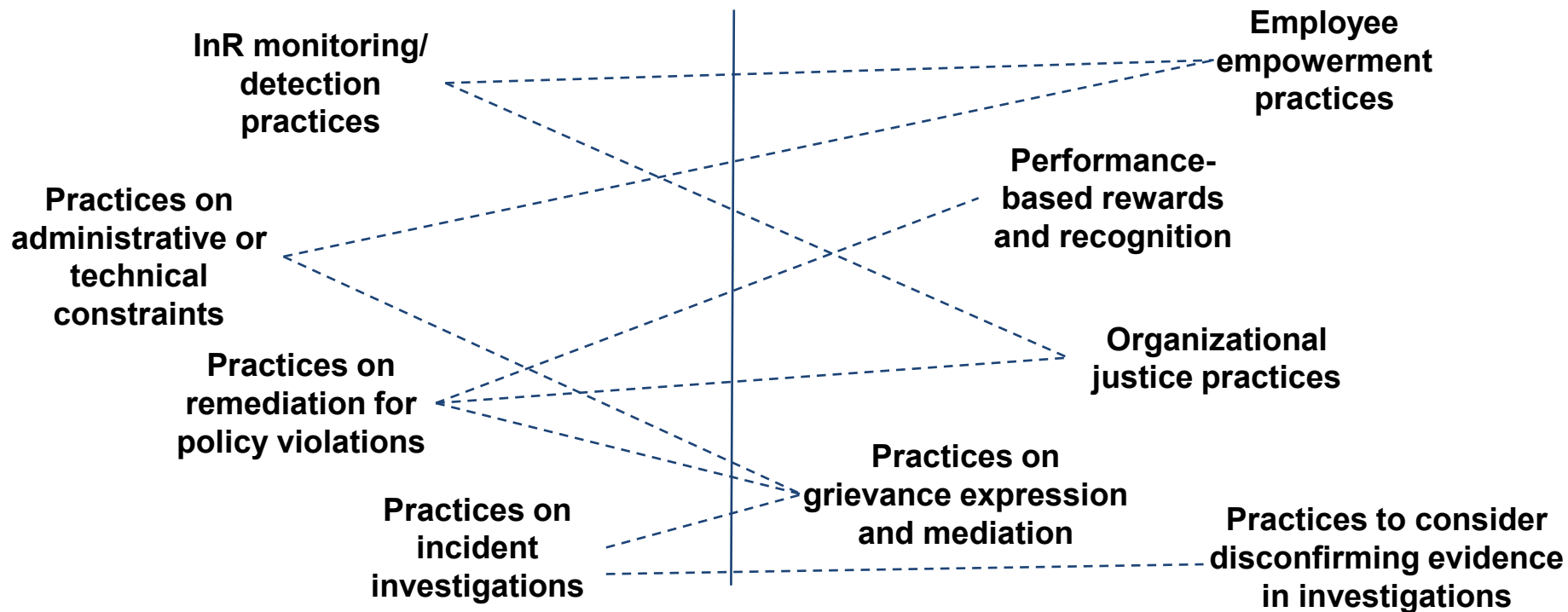


\* [Jiang 2021, Wang 2020, Withey 1989] – “Does a Stick Work? A Meta-Analytic Examination of Curvilinear Relationships between Job Insecurity and Employee Workplace Behaviors”

# Balanced Defense Bundles for Exploration

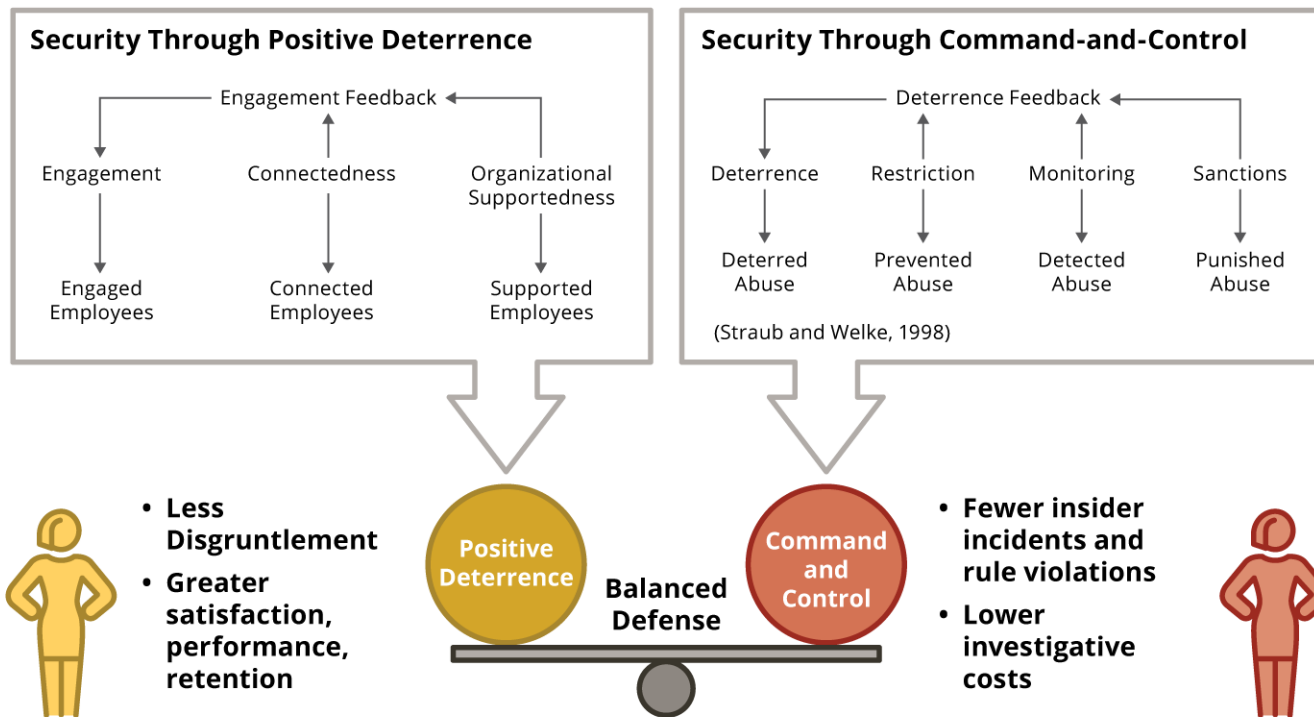
## C&C Practice Areas

## PD Practice Areas



# Conclusion

# Extending the Traditional Security Paradigm



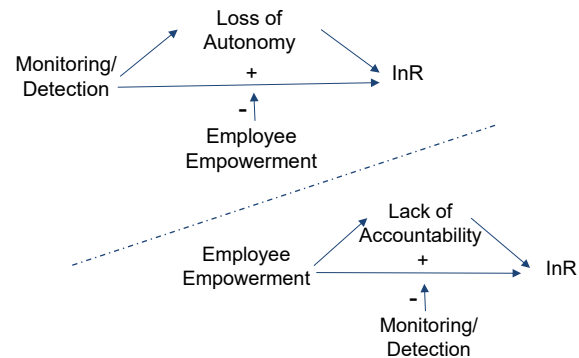
# Potential Implications

## Research

- Investigate balanced defense bundles described here and propose others for reducing insider risk and improving organizational performance
- Conduct studies to collect empirical evidence to support or refute the efficacy of balanced defense bundles

## Practice

- Consider the positive deterrence implementation process presented here for use within your organization
- Use proposed balanced defense bundles as a starting place for thinking about what balance means for your organization





# Foundational Contributors of Positive Deterrence

## Acknowledgements to:

- Prof. Herbert Kelman (Types of influence)
- Prof. S. Alexander Haslam (Organizational identification)
- Prof. E. Tory Higgins (Motivational Focus/Fit Theory)
- Prof. Robert Eisenberger (Perceived organizational support)
- Prof. Tom Tyler (Self regulation and rule following)
- Prof. Denise Rousseau (Psychological contract theory)
- Dr. Eric Shaw (Critical path and organizational influences)
- Dr. Frank Grietzer (Expansion of organizational factors)
- SEI colleagues, including D. Bauer, P. Buttles, T. Cassidy, W. Claycomb, M. Collins, D. Costa, J. Cowley, R. Ditmore, C. Gardner, A. Horneman, S. Miller, D. Mundie, W. Novak, L. Osterritter, S. Perl, D. Spooner, M. Theis, R. Trzeciak, N. VanHoudnos

# Questions?

## Contact Information:

Andrew P. Moore  
Software Engineering Institute  
Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA 15215  
412-225-4048  
apm@sei.cmu.edu

# References

**[Ariani 2013]** Ariani, “The Relationship between Employee Engagement, Organizational Citizenship Behavior, and Counterproductive Work Behavior *International Journal of Business Administration*, 4, 2013.

**[Bordia 2008]** Bordia, Restubog, and Tang, “When employees strike back: investigating mediating mechanisms between psychological contract,” breach and workplace deviance. *Journal of Applied Psychology*, 93(5), 1104, 2008.

**[Chadwick 2010]** Chadwick, “Theoretic Insights on the Nature of Performance Synergies in Human Resource Systems: Toward Greater Precision,” *HRM Review*, 2010.

**[Colbert 2004]** Colbert, Mount, Harter, Witt, and Barrick, “Interactive effects of personality and perceptions of the work situation on workplace deviance,” *Journal of Applied Psychology*, 89(4), 599, 2004.

**[Eisenberger 2011]** Eisenberger and Stinglhamber, *Perceived Organizational Support: Fostering Enthusiastic and Productive Employees* American Psychological Association.

**[Ennen 2010]** Ennen and Richter, “The Whole is more than the Sum of its Parts – or is it?: A Review of the Empirical Literature on Complementarities in Organizations,” *Journal of Management*, 2010.

# References

- [Faldetta 2021]** Faldetta, “Abusive Supervision and Workplace Deviance: The Role of Negative Reciprocity,” *Int’l Journal of Organizational Analysis*, 2021
- [Fatima 2013]** Fatima, Iqbal, and Imran “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, 2013.
- [Jiang 2021]** Jiang, et al., “Does a Stick Work? A Meta-Analytic Examination of Curvilinear Relationships between Job Insecurity and Employee Workplace Behaviors,” *Academy of Management*, 2021.
- [Kelman 1958]** Kelman, “Compliance, Identification, and Internalization: Three Processes of Attitude Change,” *Journal of Conflict Resolution* 2(1), 51-60, 1958.
- [Lawrence 2007]** Lawrence and Robinson, “Ain’t Misbehavin: Workplace Deviance as Organizational Resistance,” *Journal of Management*, 2007.
- [Martin 2016]** Martin, et al., “An Eye on Your Work: How Empowerment Affects the Relationship Between Electronic Surveillance and Counterproductive Work Behaviors,” *Int. Journal HRM*, 2016.

# References

**[Milgrom 1992]** Milgrom and Roberts, Economics, Organization & Management, Prentice-Hall, 1992.

**[Moore 2022]** Moore, Gardner, and Rousseau, “Reducing Insider Risk through Positive Deterrence,” CITRAP 1(1), 2022.

**[Moore 2015]** Moore, Novak, Collins, Trzeciak, and Theis “Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls,” SEI report, 2015.

**[Pierce 2011]** Pierce and Aguinis, “The Too-Much-of-a-Good-Thing Effect in Management,” Journal of Management, 2011.

**[Rhoades 2001]** Rhoades, Eisenberger, and Armeli, Affective commitment to the organization: the contribution of perceived organizational support. *Journal of Applied Psychology*, 86(5), 825, 2001.

**[Schoenherr 2022]** Schoenherr, Lilja-Lolax, Gioe, “Multiple Approach Paths to Insider Threat (MAP-IT): Intentional, Ambivalent and Unintentional Insider Threats,” CITRAP 1(1), 2022.

**[Sims 2010]** Sims, “A Study of Deviance as a Retaliatory Response to Organizational Power,” Journal of Business Ethics, 2010.

# References

- [Subramony 2009]** Subramony, “A Meta-Analytic Investigation of the Relationship Between HRM Bundles and Firm Performance,” *Human Resource Management*, Vol 48, No 5, p. 745-768, Sept-Oct 2009.
- [Sulea 2012]** Sulea, Virga, Maricutoiu, Schaufeli, Dumitru, and Sava, F. A. Work as mediator between job characteristics and positive and negative extra-role behaviors. *Career Development International*, 17, 188-207, 2012.
- [Straub 1998]** Straub and Welke, “Coping with Systems Risk: Security Planning Models for Management Decision Making,” *MIS Quarterly*, 22(4), 1998.
- [Tang 1998]** Tang and Ibrahim, “Antecedents of organizational citizenship behavior revisited: Public personnel in the United States and in the Middle East,” *Public Personnel Management*, 27(4), 529-550, 1998.
- [Wang 2020]** Wang, et al., “Exploring the Relationships Between a Toxic Workplace Environment, Workplace Stress, and Project Success with the Moderating Effect of Organizational Support,” *RM&HP*, 2020.
- [Withey 1989]** Withey and Cooper, “Predicting Exit, Voice, Loyalty and Neglect,” *Administrative Science Quarterly*, 1989.