



Positive Deterrence and its Role in Countering Extremist Acts against Organizations

Andrew P. Moore

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2021 Carnegie Mellon University.

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.

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.

DM21-1080

Overview of Presentation

Goal: Argue for insider risk management programs (IRMPs) to adopt evidence-based workforce management practices that we call **positive deterrence** as a complement to existing command-and-control approaches to reduce insider risk.

Outline:

- Characterize positive deterrence
- Identify why positive deterrence is a needed complement to command-and-control
- Discuss how positive deterrence can help counter extremist acts against the organization
- Discuss areas of possible future research
- Identify what IRMPs can do now to start implementing positive deterrence

I Will Be Connecting the Dots of Many Great Thinkers

Primary contributors to the dots:

- Prof. Herbert Kelman (Types of influence)
- Prof. Henri Tajfel (Social identity theory)
- 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. Dominic Packer (Normative conflict model)
- Prof. Denise Rousseau (Psychological contract theory)
- Dr. Katherine Herbig (Characterization of espionage)
- Dr. Eric Shaw (Critical path and organizational influences)
- Dr. Frank Grietzer (Expansion of organizational factors)
- Dr. Kris Veenstra (Loyalty, social identity, and insider threat)
- SEI colleagues, including M. Theis, D. Costa, C. Gardner, L. Osterritter, S. Perl, R. Trzeciak, J. Cowley, D. Mundie

...



Three Types of Influence of the Workforce*

Compliance (exchange with organization)

- Influence due to desire to gain specific rewards
- Maintained with surveillance by the organization

Identification (affiliation with organization)

- Influence due to desire to establish or maintain a satisfying relationship with the organization
- Maintained because of attractiveness of the relationship to the individual

Internalization (goals/values shared with organization)

- Influence due to congruence of individual and organization's goals and values
- Maintained because of credibility of those goals and values to the individual

Command
and Control



Positive
Deterrence

Depends on

- Extrinsic motivation
- Organization's monitoring and response

Depends on

- Intrinsic motivation
- Individual's instinctive response

* Kelman "Social Influence and Linkages between the Individual and the Social System," in *Perspectives on Social Power*, 1974.
O'Reilly and Chatman "Organizational Commitment and Psychological Attachment," *Journal of Applied Psychology*, 1986.
Tyler "Promoting Employee Policy Adherence and Rule Following in Work Settings-The Value of Self-Regulatory Approaches." BLR, 2004.

Relevance of Motivational Focus Theory (MFT)*

Motivational Focus Theory posits two independent orientations that people instinctively use to determine how they go about making decisions

- Promotion-focused: individual focus on advancement and accomplishment, aka gains
- Prevention-focused: individual focus on security and responsibility, aka non-losses

MFT provides measures for identifying the extent of each when approaching a given task

An individual may have different orientations depending on the context

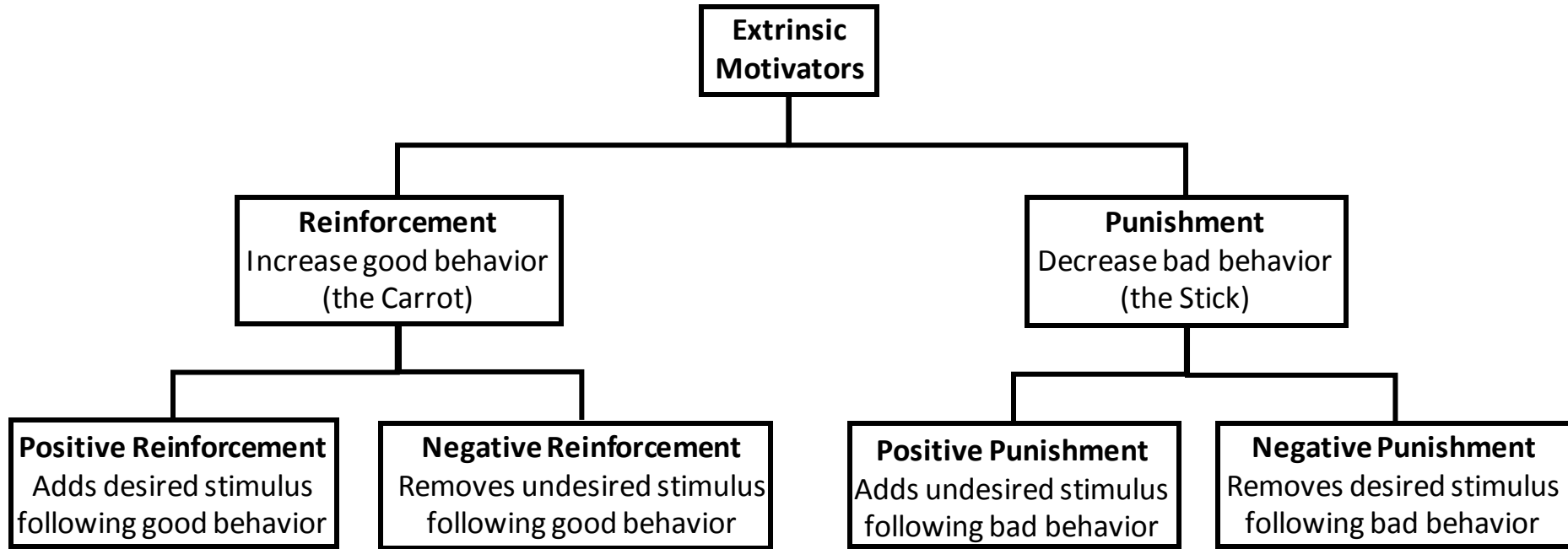
Command-and-Control defenses

- Good fit for prevention-focused individuals
- Hinderance to promotion-focused individuals

Positive deterrence provides a better fit for a promotion-focused orientation.

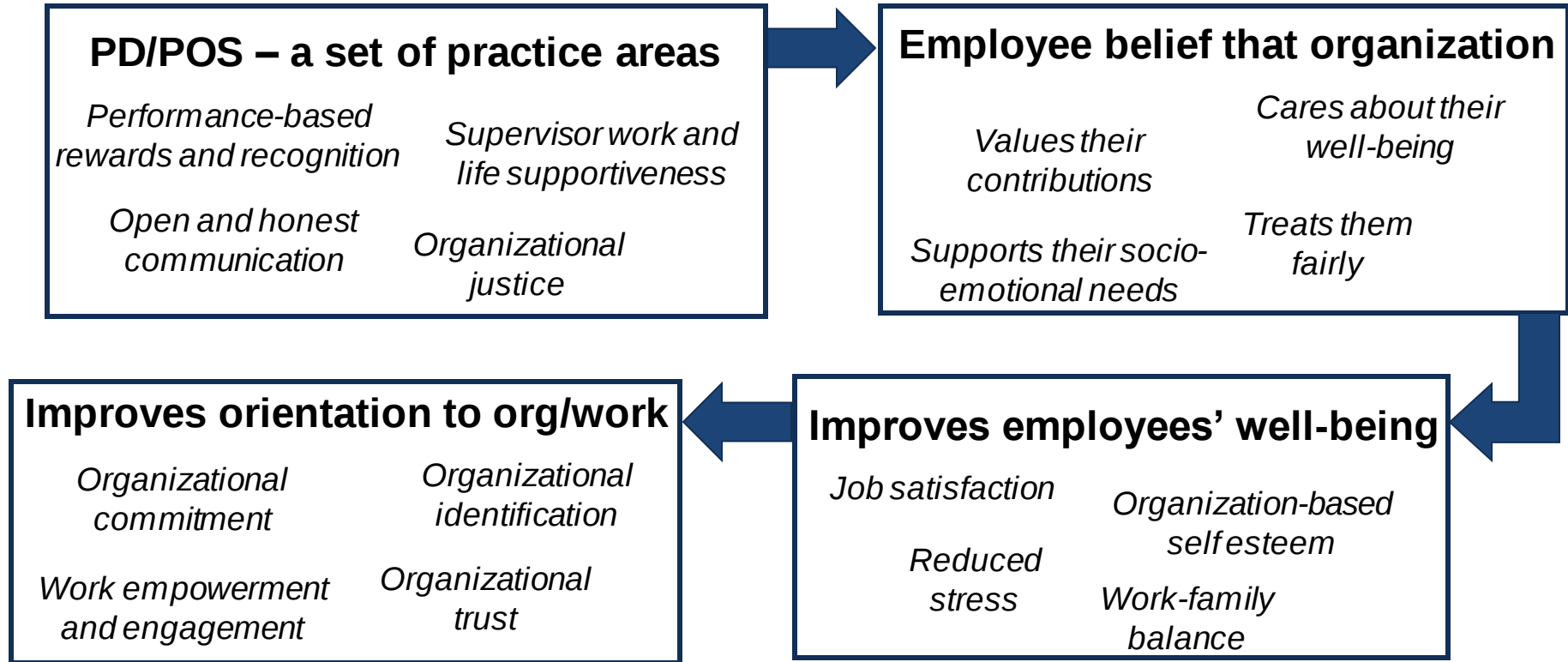
- Halvorson and Higgins. *Focus: Use different ways of seeing the world for success and influence*. Penguin, 2013.
aka Regulatory Focus Theory.

External Motivation in the Light of Operant Conditioning*

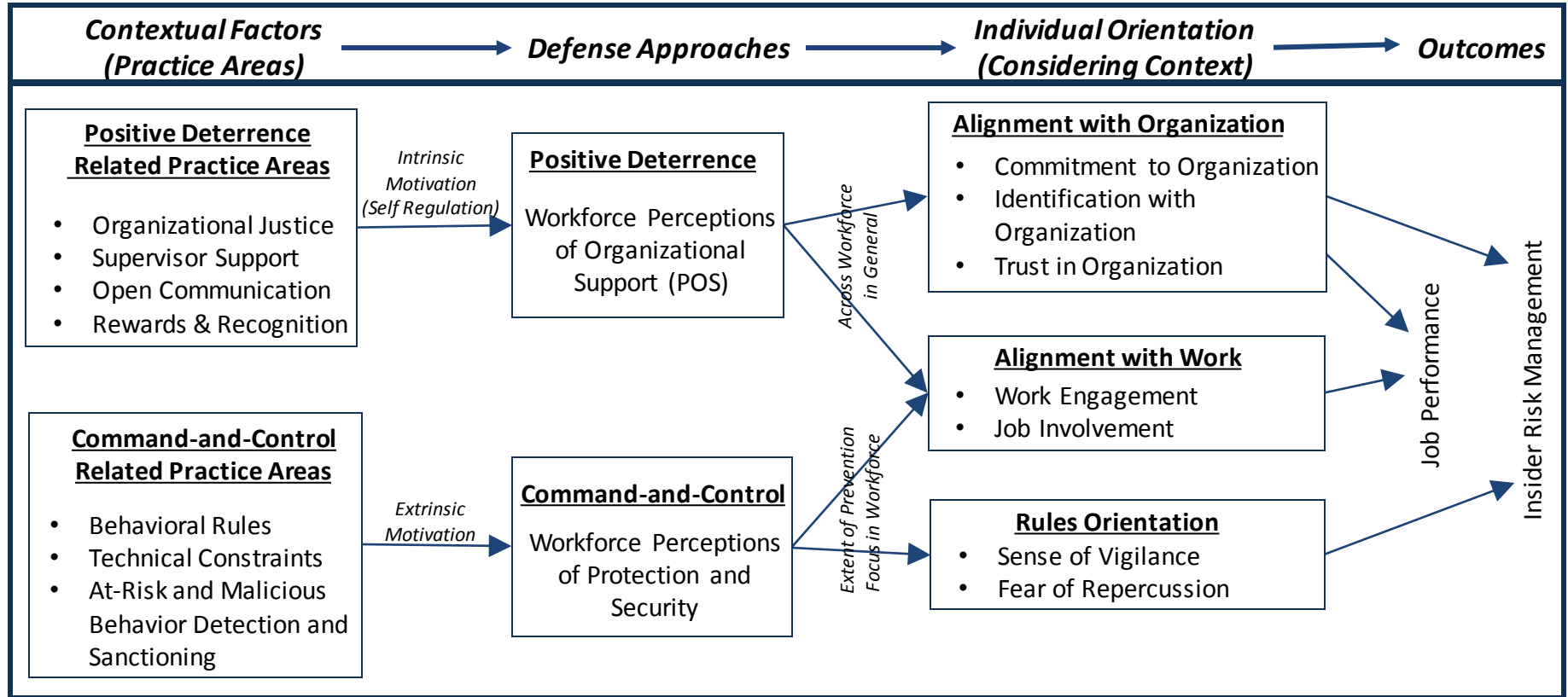


* Adapted from Wikipedia: Operant conditioning involves a voluntary behavior in the face of an external stimulus.

Perceived Organizational Support (POS) as Positive Deterrence*



Balanced Insider Risk Management

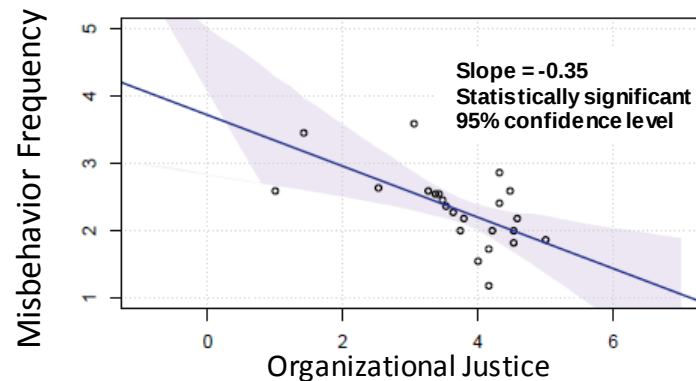
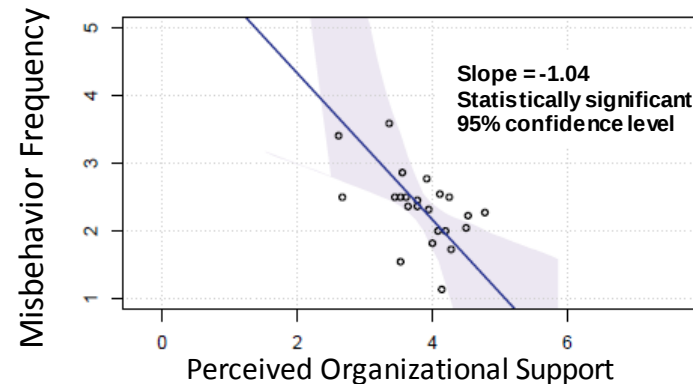


POS and Insider Threat

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.

Why Augment Command-and-Control with Positive Deterrence?

Workforce management and security practices can undermine workforce goodwill

Positive deterrence can reduce insider incident rates over command-and-control alone

Promoting positive deterrence can significantly enhance the IRMP mission

Positive deterrence improves job performance generally

Relating Organizational Identification and Normative Conflict

Social Identity: “that part of an individual’s self-concept which derives from his knowledge of his membership in a social group (or groups) together with the value and emotional significance attached to that membership.”*

Organizational Identification: The value placed on being a part of an organization with which one has self-categorized.

Normative Conflict: discrepancy between the current (perceived) norms of a group and another standard (possibly the ascribed norms of the group)

Dissent is one possible response to normative conflict in the Normative Conflict Model:

- The model author does not view dissent as inherently good or bad:
 - “There is nothing intrinsically moral or righteous about the dissenter; indeed, from the perspective of other group members, as well as outside observers, dissent may often appear to be motivated by blatantly misguided or immoral principles.”**
- Effective whistleblower program or grievance procedures can allow dissent to be handled productively
- BUT, Dissent can lead to heightened insider risk.

* Tajfel, H. *Human Groups and Social Categories*, Cambridge Univ. Press, 1981.

** Packer, D.J. “On Being Both With Us and Against Us: A Normative Conflict Model of Dissent in Social Groups,” PSPR, 2008.

Model of Normative Conflict*

Organizational Identification	<i>strong</i>	Q2: Loyal Conformity	Q4: Dissent or Uneasy Conformity
	<i>weak</i>	Q1: Passive Non-Conformity or Strategic Conformity	Q3: Disengagement or Personally-Oriented Dissent
		<i>low</i>	<i>high</i>

- Packer, D.J. "On Being Both With Us and Against Us: A Normative Conflict Model of Dissent in Social Groups," PSPR, 2008.
- Veenstra, K. 'Loyalty, Social Identity and Insider Threat,' Aust. Crime Commission, 2015.

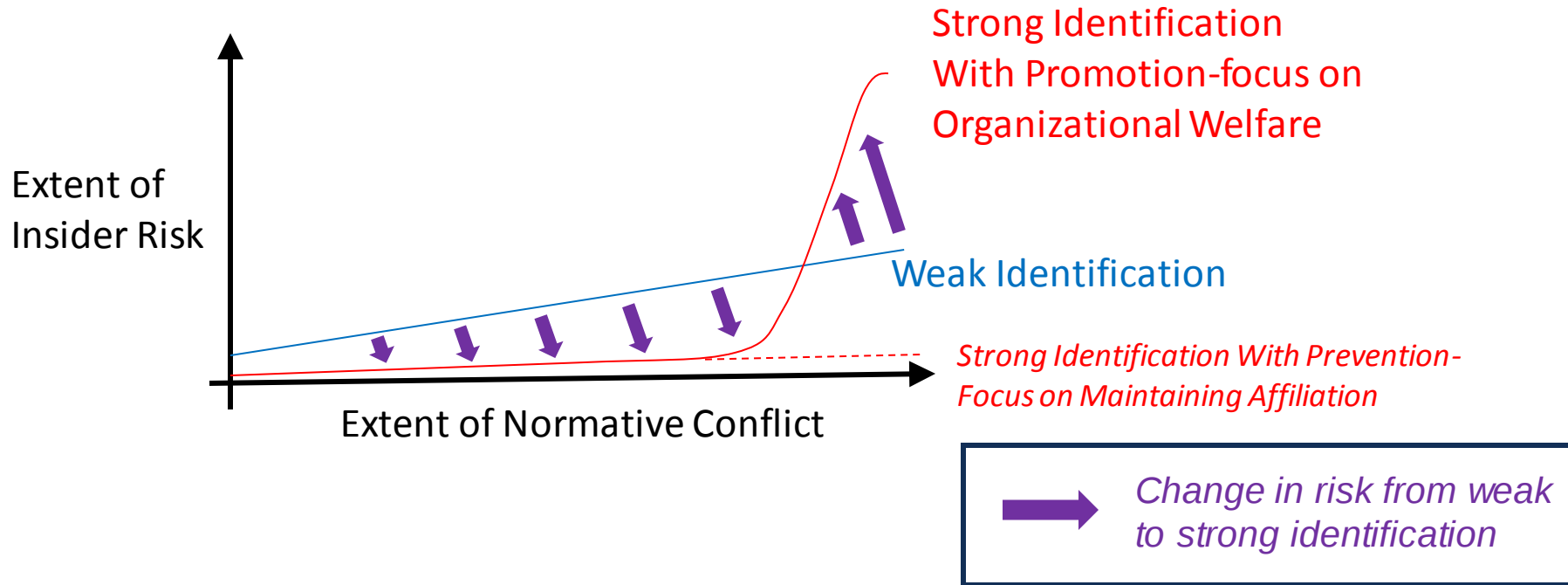
Model of Normative Conflict*

Organizational Identification	<i>strong</i>	Motivational Focus	Affiliative (Prev Focus)	Q2a: Conformity	Q4a: Conformity
			Org. Welfare (Prom Focus)	Q2b: Strategic Non-Conformity	Q4b: Dissent or Uneasy Conformity
	<i>weak</i>			Q1: Passive Non-Conformity or Strategic Conformity	Q3: Disengagement or Personally-Oriented Dissent
				<i>low</i>	<i>high</i>

Normative Conflict

- Packer, D.J. "On Being Both With Us and Against Us: A Normative Conflict Model of Dissent in Social Groups," PSPR, 2008.
- Veenstra, K. 'Loyalty, Social Identity and Insider Threat,' Aust. Crime Commission, 2015.
- Blader, S.L. et al. "Organizational Identification and Workplace Behavior: More Than Meets the Eye," Elsevier, 2017.

Notional Representation of Risk Posed by Organizational Identifiers Given Normative Conflict



Research Areas

Empirical studies to validate aspects of the normative conflict model for insider risk

- Refining measures of organizational identification and normative conflict along continuum
- Relating the level of insider risk associated with various levels of normative conflict and organizational identification

Identification of tipping point of heightened risk along identification/conflict continuum

As a result of the above findings:

- Characterization of properties of effective grievance procedures and whistleblower programs
- Refinement of
 - Potential risk indicators
 - Personnel security vetting procedures

Value of Positive Deterrence

Evidence exists showing that POS increases organizational identification

But there are research areas that remain to be investigated:

- Extent that positive deterrence (POS specifically) reduces normative conflict and balances organizational identification (self orientation vs group orientation)
- Can POS inoculate against disinformation-induced normative conflict?

As pointed out by Veenstra: James Turner, the chair of the Australian Information Security Association claims that in regard to the Snowden compromise

The lesson that they should be taking from this one is taking care of their people. It's not enough to vet a person, it's not enough to interview them well, it's not enough to know their background. You've actually got to take an ongoing interest in who they are and what they're dealing with on a ongoing basis. If someone had been interested in Snowden all through this period of time, the flags would have been raised.

This same sentiment could be applied to the insider extremist threat as well.

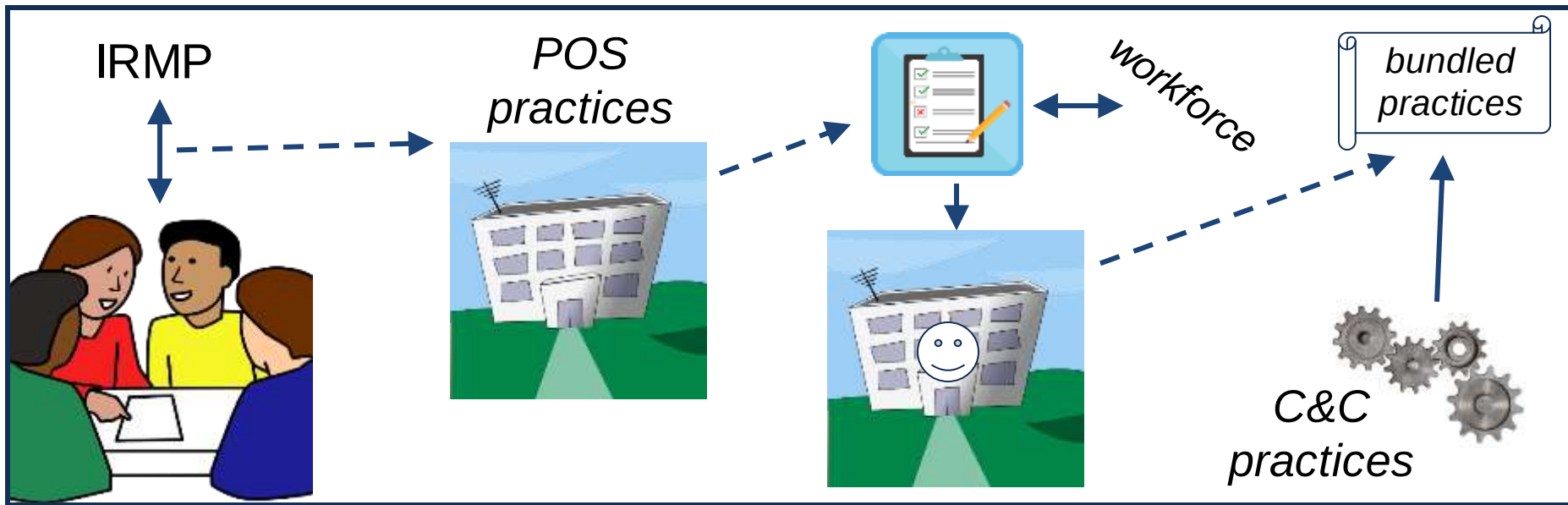
What Can Orgs Do Now to Implement Positive Deterrence

Engage and coordinate with stakeholders across the organization, especially HR

Work with stakeholders to implement practices proven to increase organizational support

Fine-tune practices by eliciting employee perspectives on IRMP and working environment

Bundle positive deterrence with command-and-control practices



Three Categories of Positive Deterrence-Related Practices

People



Connected @ Work

Job



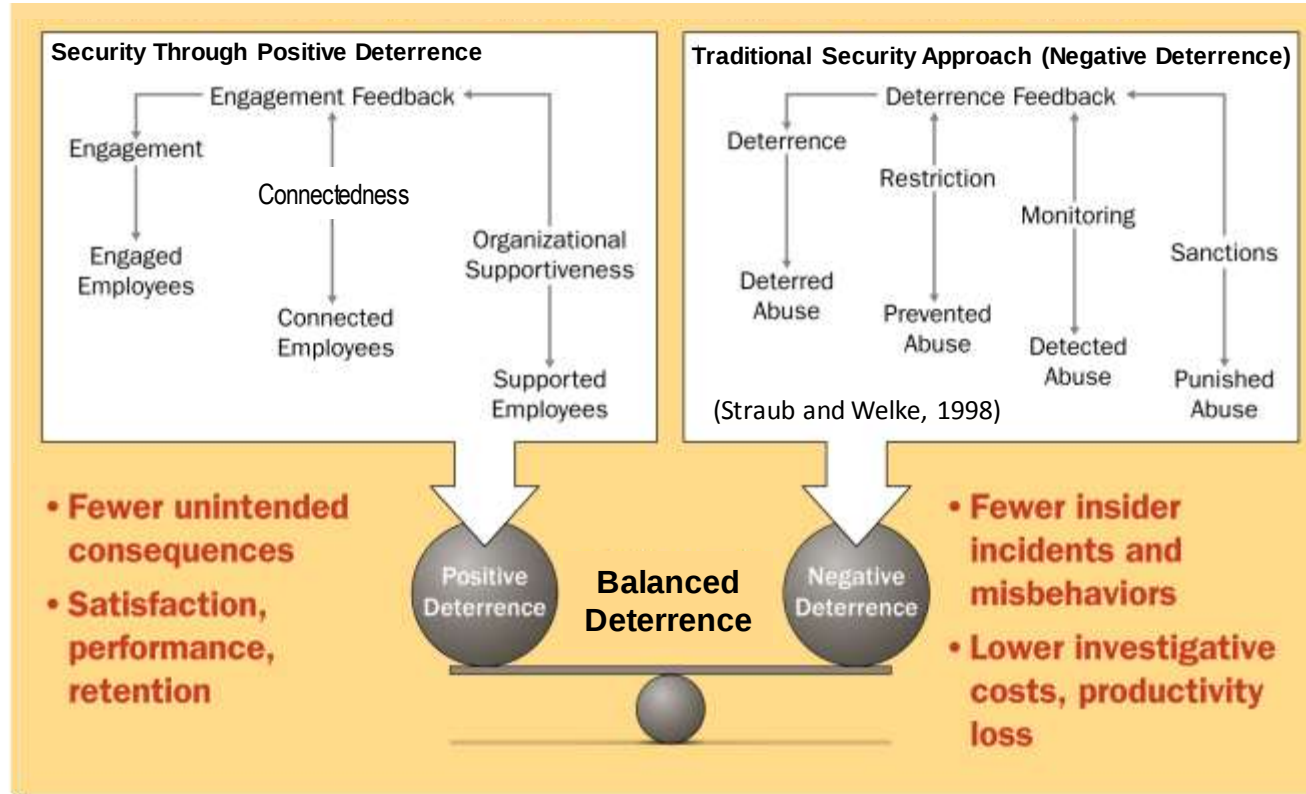
Job Engagement

Organization



Perceived Organizational Support

Extending the Traditional Security Paradigm*



* Adapted from Moore et al. "Balancing Organizational Incentives to Counter Insider Threat," Proc. IEEE Workshop on Research in Insider Threat (WRIT), 2018.

Picture after we continue to connect the dots (and conduct more research...)



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