Positive Deterrence and its Role in Countering Extremist Acts against Organizations

Andrew P. Moore (apm@sei.cmu.edu)

Keynote Presentation

6th Workshop on Research for Insider Threats (WRIT)

8 December 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM21-1080

Overview of Presentation

Goal: Argue for insider risk management programs (IRMPs) to promote 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 organizations 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
- 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 organization's goals and values

Command and Control

Depends on
- Pressure through extrinsic motivation
- Organization's monitoring and response

Positive Deterrence

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

* 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

An individual may have different orientations depending on the context

Command-and-Control defenses

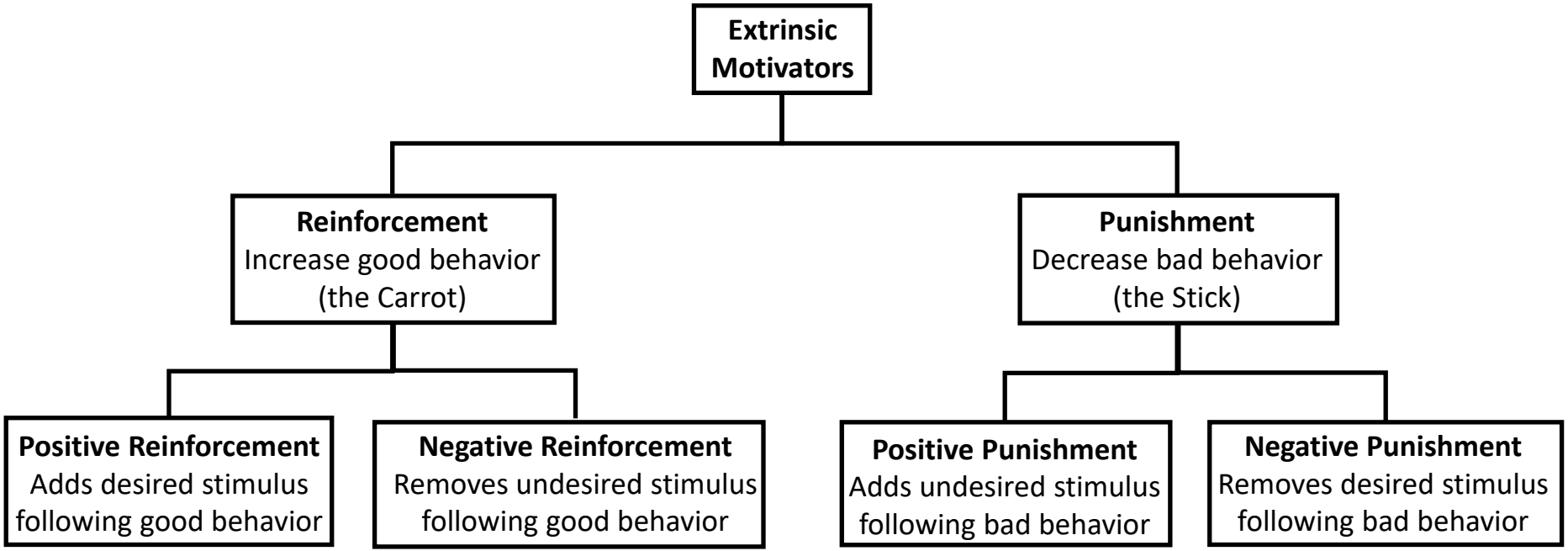
- Good fit for prevention-focused individuals
- Hinderance or irritation to promotion-focused individuals

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

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

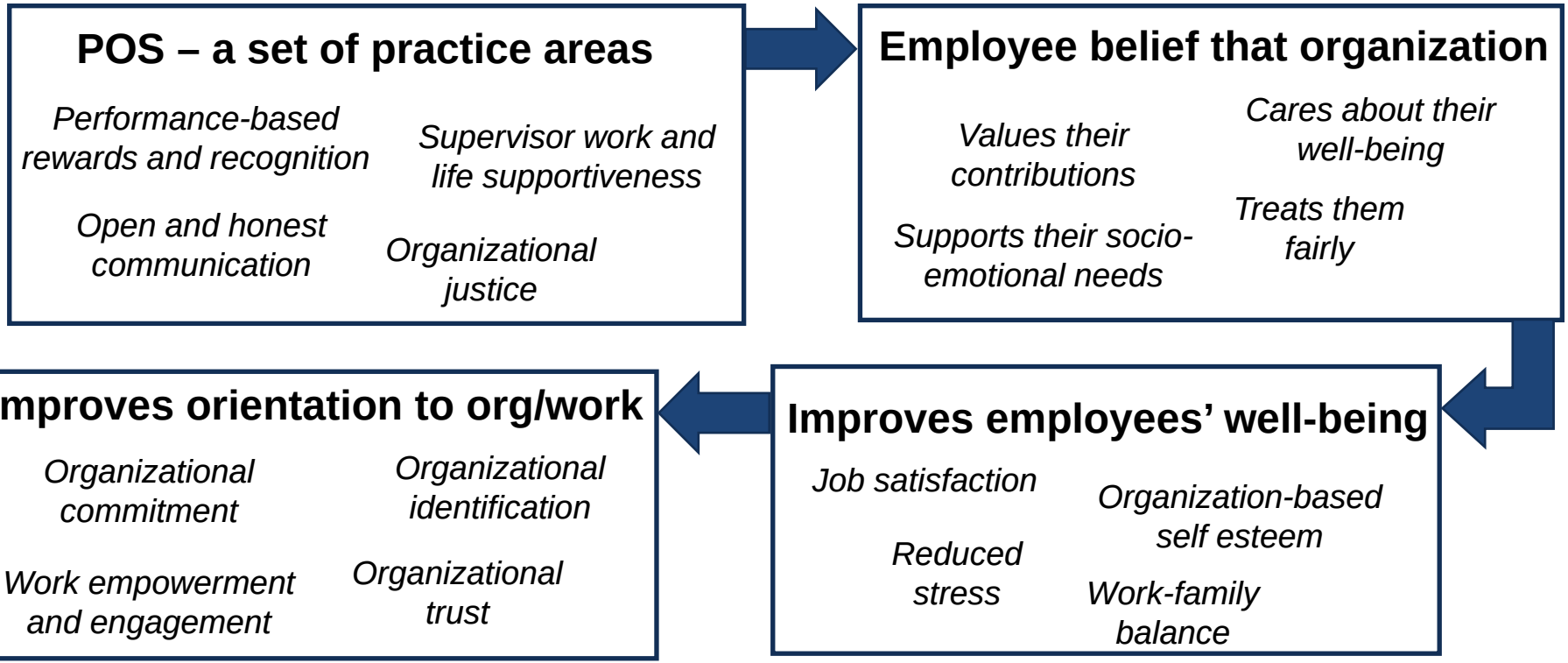
- Halvorson and Higgins. *Focus: Use different ways of seeing the world for success and influence*. Penguin, 2013. aka Regulatory Focus Theory.

External Motivation in the Light of Operant Conditioning*



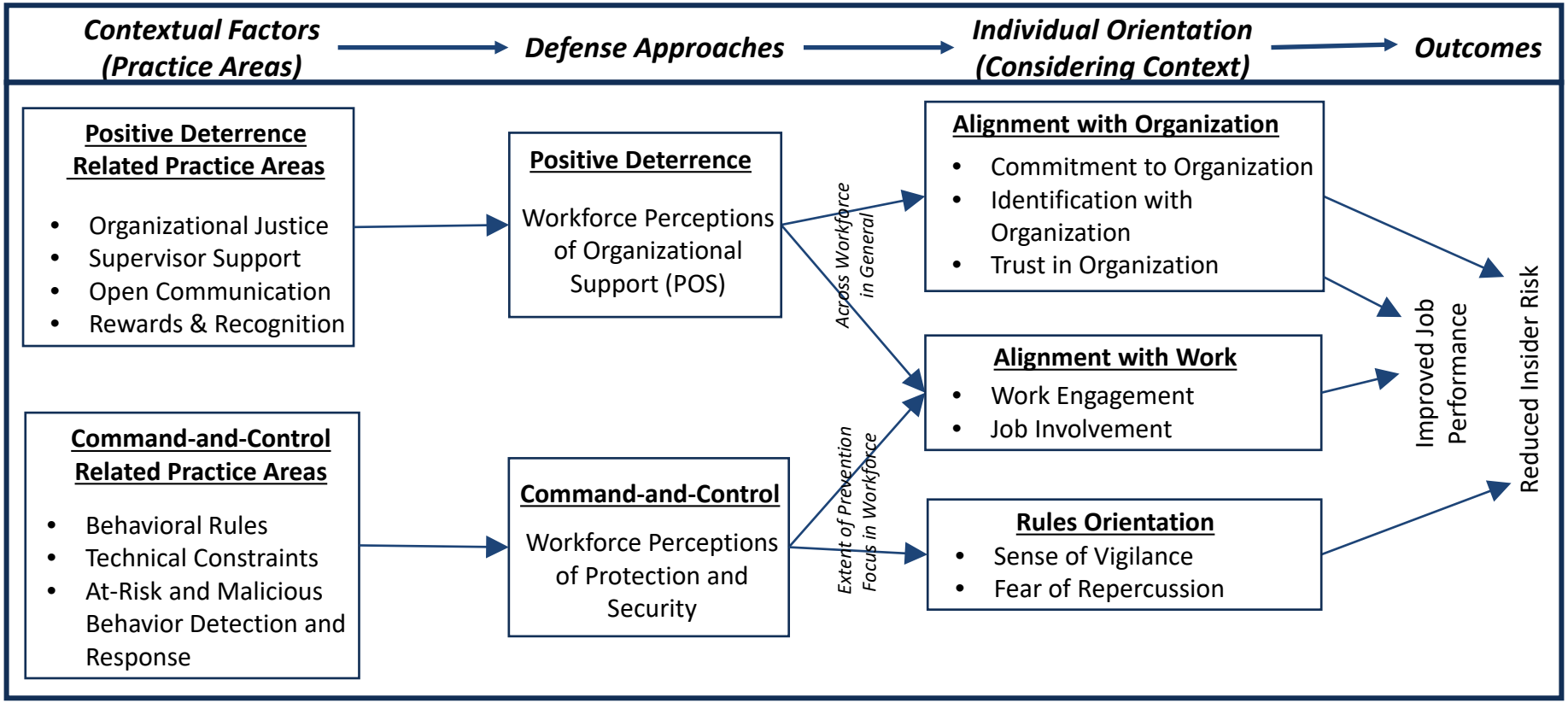
* Adapted from Wikipedia: Operant conditioning involves a voluntary behavior in the face of an external stimulus.

Perceived Organizational Support (POS) as Positive Deterrence*



* Eisenberger and Stinglhamber, Perceived Organizational Support: Fostering Enthusiastic and Productive Employees, APA, 2011.

Balanced Insider Risk Management



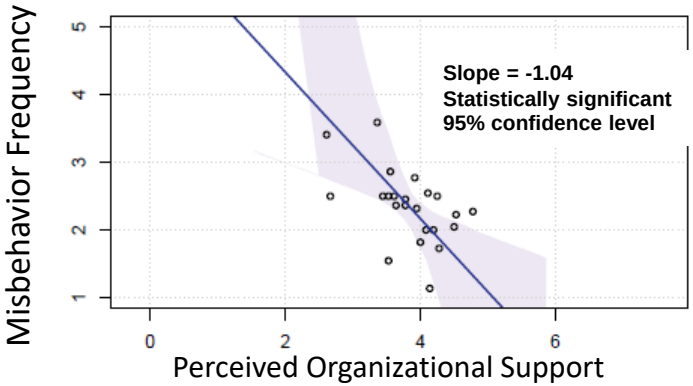
Previous CERT study relating POS and Insider Threat*

Research Question: How much does organizational support 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)**



* Moore, et al. “Balancing Organizational Incentives,” WRIT 2018.

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

Why Augment Command-and-Control with Positive Deterrence?

1. Workforce management and security practices can undermine workforce goodwill
2. Positive deterrence can reduce insider incident rates over command-and-control alone
3. Promoting positive deterrence can significantly enhance the IRMP mission
4. Positive deterrence improves job performance generally

Role of Positive Deterrence in Countering Extremist Acts against the Organization

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 employed.

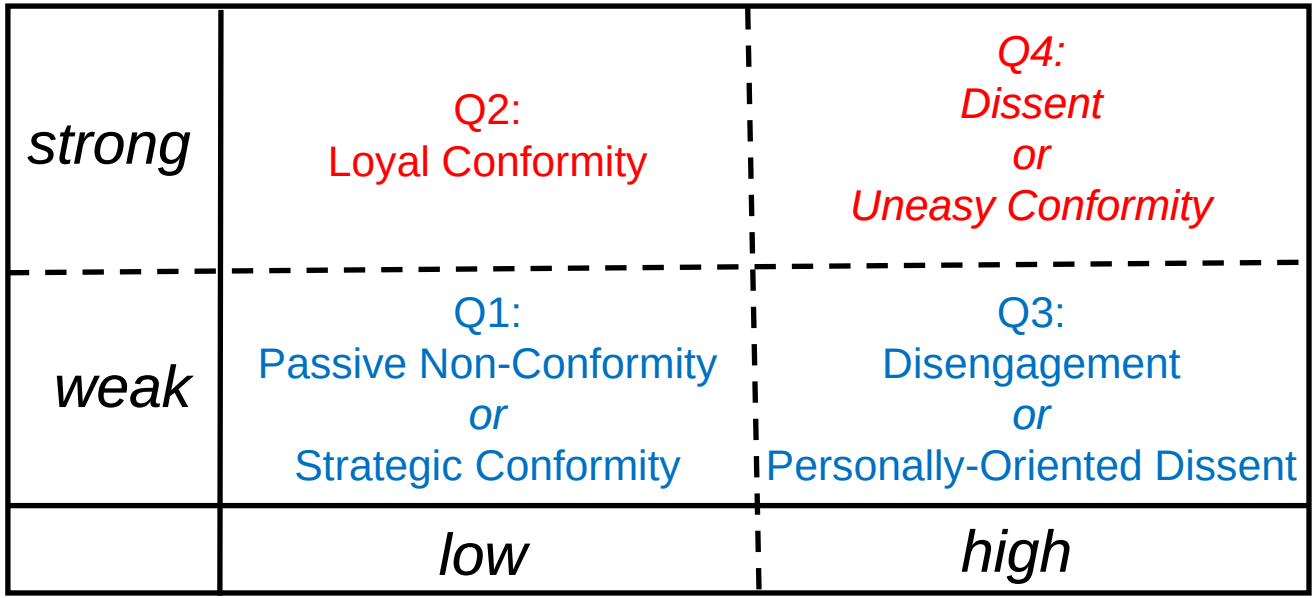
Normative Conflict: discrepancy between the current (perceived) behavioral norms of the organization and another standard (possibly the attributed norms of the organization)

When Identification is high, dissent is possible response to normative conflict in 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.

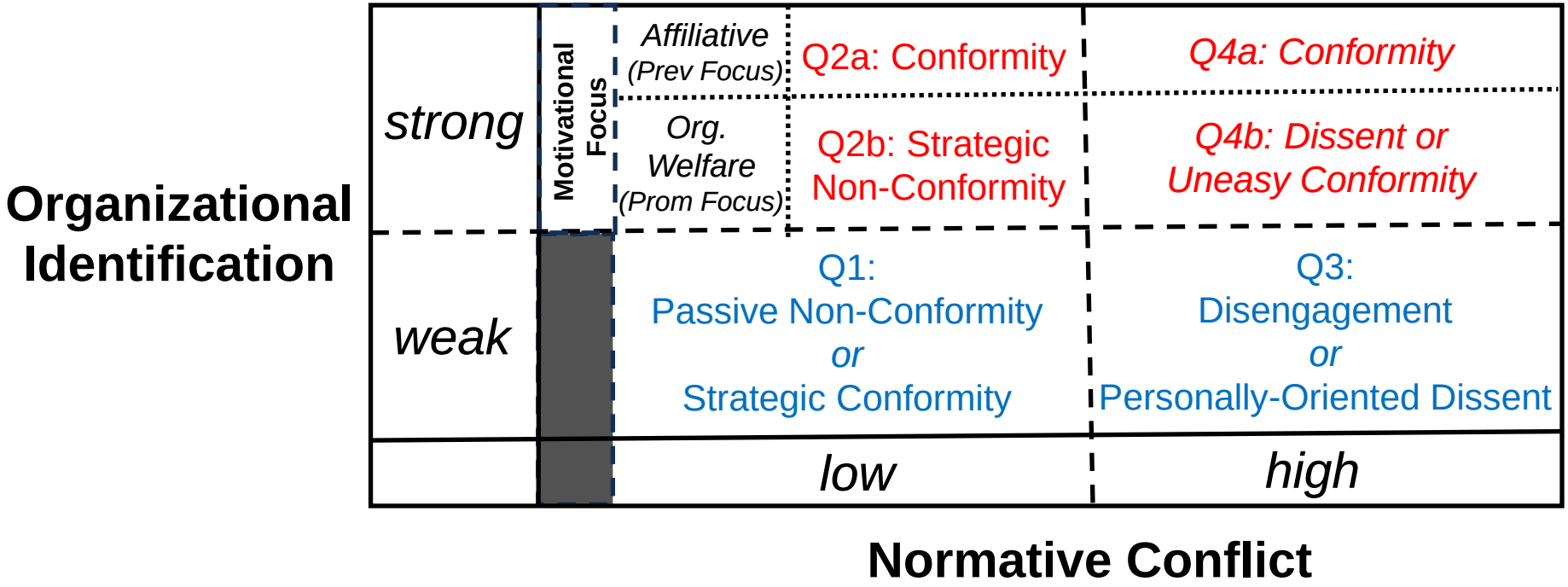
* Veenstra, K. ‘Loyalty, Social Identity and Insider Threat,” Aust. Crime Commission, 2015.
** Tajfel, H. *Human Groups and Social Categories*, Cambridge Univ. Press, 1981.
*** Packer, D.J. “On Being Both With Us and Against Us: A Normative Conflict Model of Dissent in Social Groups,” PSPR, 2008.

Model of Normative Conflict*



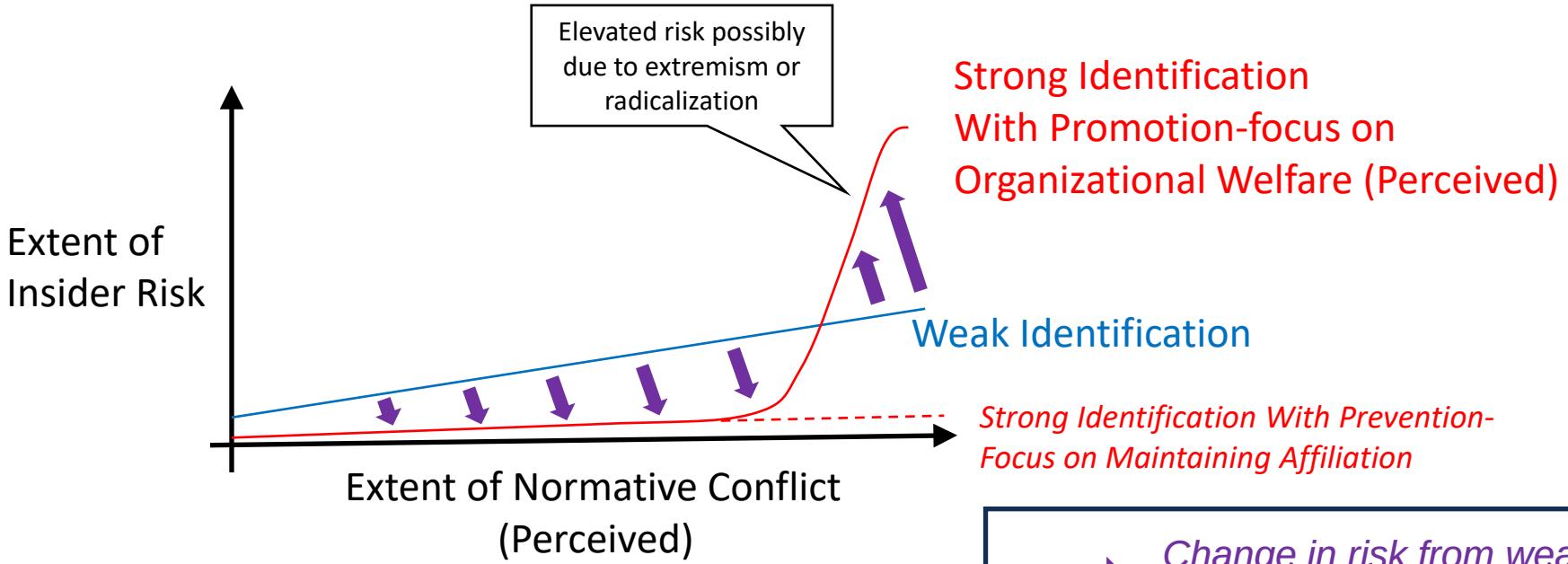
- Packer, D.J. “On Being Both With Us and Against Us: A Normative Conflict Model of Dissent in Social Groups,” PSPR, 2008.
  Veenstra, K. ‘Loyalty, Social Identity and Insider Threat,” Aust. Crime Commission, 2015.

Extended Model of Normative Conflict*



* 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

Understanding the Value of Positive Deterrence

Additional research areas

- Assessing extent that positive deterrence reduces normative conflict and balances organizational identification
- 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 an 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.

s

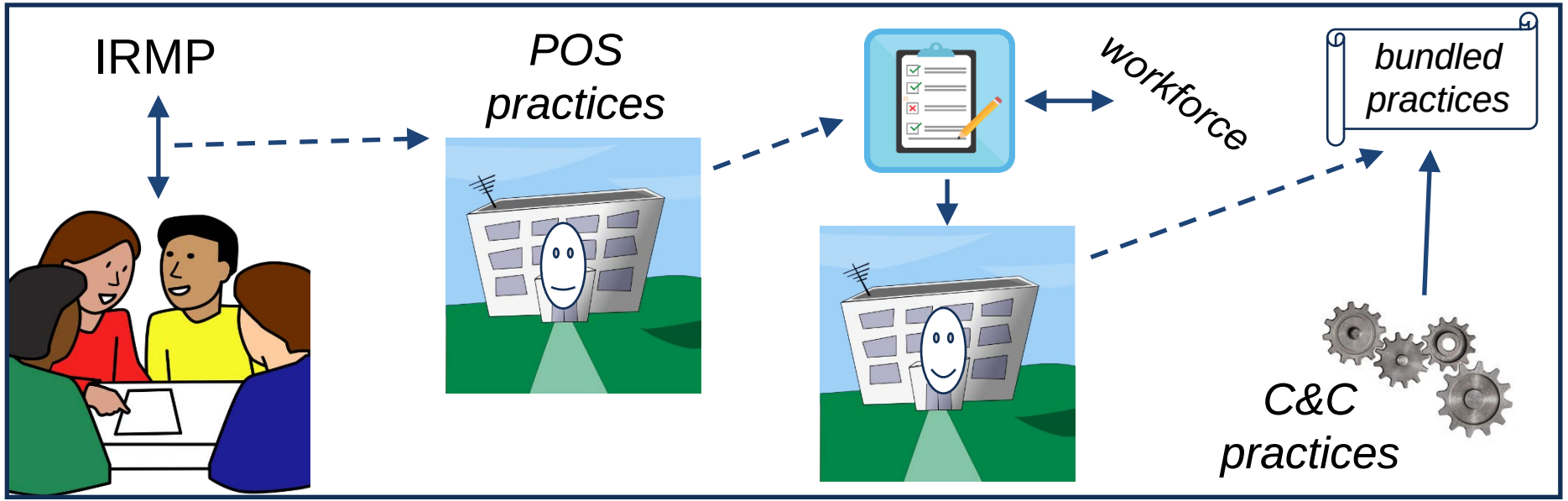
What Can Orgs Do Now to Implement Positive Deterrence

1. Engage and coordinate with stakeholders across the organization, especially HR

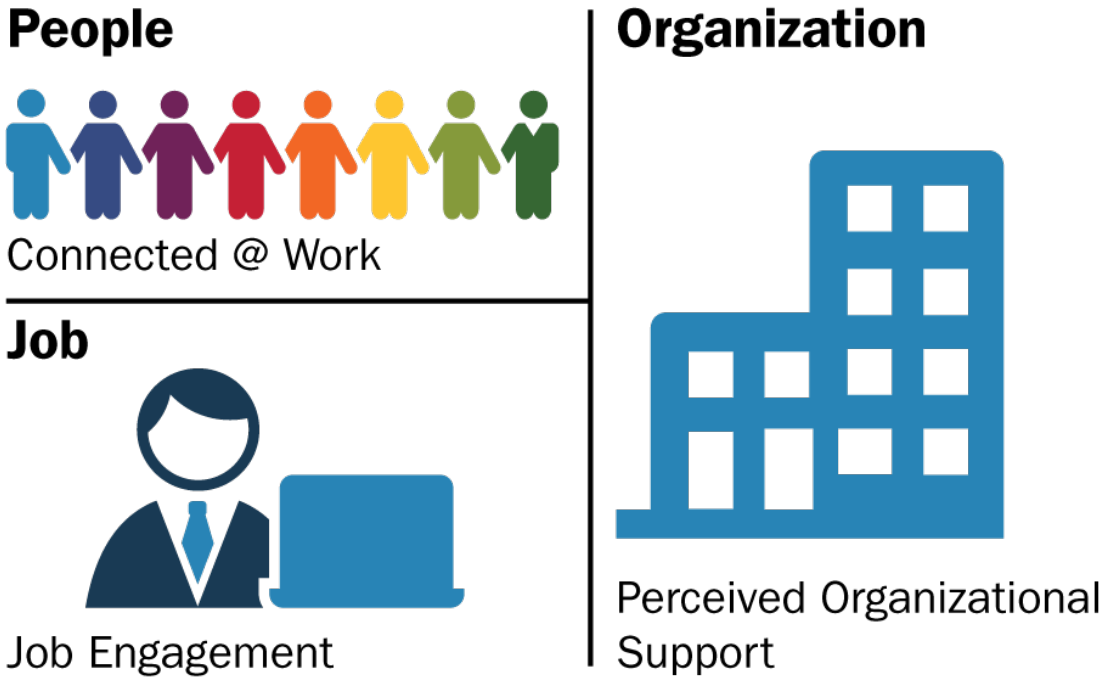
2. Work with stakeholders to implement practices proven to increase organizational support

3. Fine-tune practices by eliciting employee per-spectives on IRMP and working environment

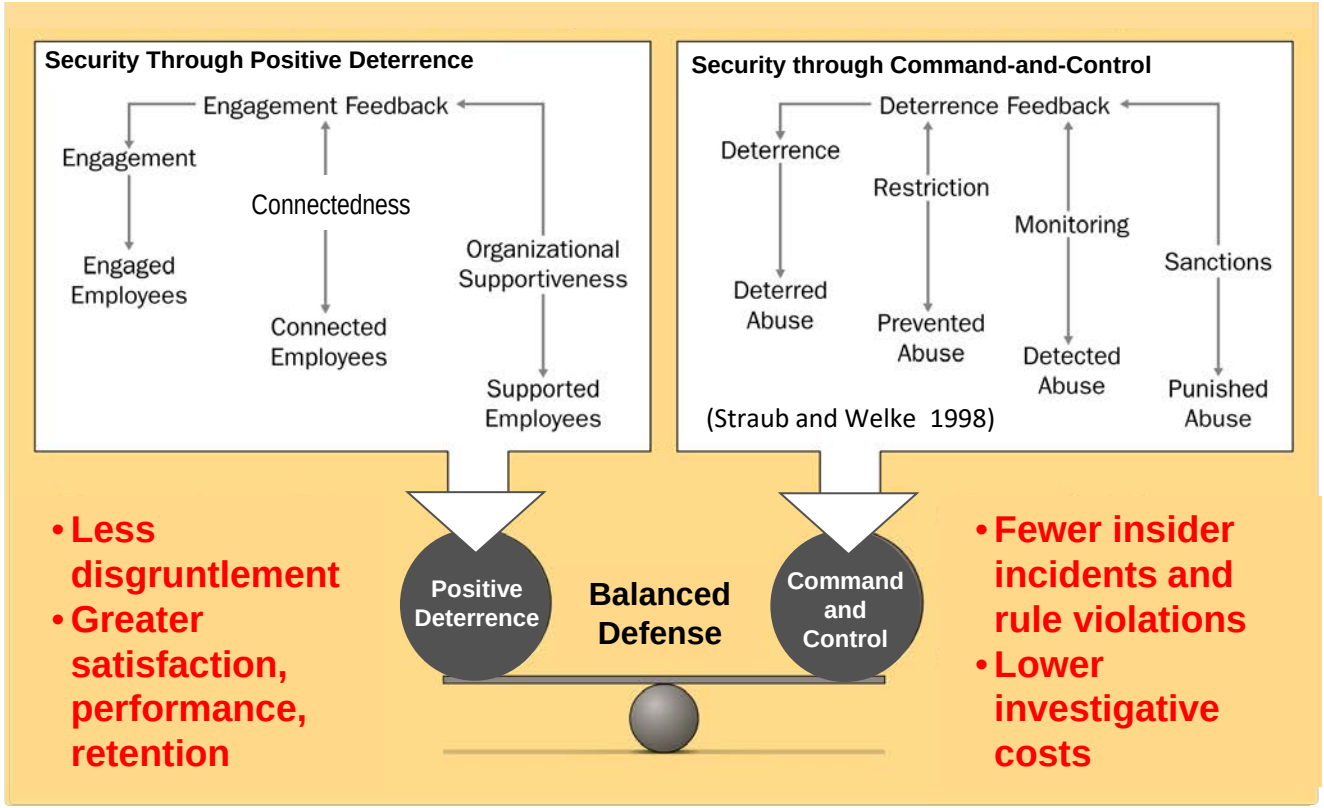
4. Bundle positive deterrence with command-and-control practices



Three Categories of Positive Deterrence-Related Practices



Extending the Traditional Security Paradigm*



* Adapted from Moore et al. "Balancing Organizational Incentives to Counter Insider Threat," WRIT 2018.

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