Reducing Insider Risk Through Positive Deterrence

Andrew P. Moore (apm@sei.cmu.edu)
Carrie Gardner (cgardner@sei.cmu.edu)
Software Engineering Institute

Denise M. Rousseau (denise@cmu.edu)
Heinze College and Tepper School of Business

Carnegie Mellon University
Pittsburgh, PA 15215

Abstract

Most organizations approach insider risk management with a command-and-control focus, pressuring employees to act in the interests of the organization through external controls. Positive deterrence complements the command-and-control approach by aligning and reinforcing the mutual interests of the individual and the organization in ways that further reduce insider risk. This brief report describes why and how insider risk management programs should consider augmenting their command-and-control strategies with positive deterrence. Programs that embrace positive deterrence can unlock greater potential to minimize insider risk and employees' negative perception of the command-and-control approach. We provide actionable guidance on how organizations can combine positive deterrence and command-and-control of insider threat in a balanced way to take advantage of the reduced insider risk that it affords. As a complement to command-and-control, positive deterrence creates a work environment that reinforces the bond between the organization and its workforce, contributing to the well-being of both.

Introduction

In this article, we describe why and how insider risk management programs (IRMPs) should consider promoting a set of evidence-based management practices that we call *positive deterrence*. Positive deterrence practices align and reinforce the mutual interests of the individual and the organization in ways that reduce insider risk. Positive deterrence complements the *command-and-control* approach that most IRMPs take. Command-and-control approaches pressure employees to act in the interests of the organization through external controls including rules, regulations, technical constraints, monitoring, and response.[1] In contrast, positive deterrence promotes constructive behavior and attitudes by aligning employees' interests with those of the organization.

We describe a specific type of positive deterrence: Practices that bolster employee *perceived organizational support* (POS) (Eisenberger & Stinglhamber, 2011). POS-related practices can increase employee commitment to and trust in the organization by increasing the perception that the organization values their contributions, cares about their well-being, supports their socioemotional needs, and treats them fairly. POS-boosting practices include work flexibility, work/family balance, employee assistance, fair compensation, and constructive supervision. For insider risk management, these positive deterrence practices defend against intentional (malicious) insider threats, especially those motivated by employee disgruntlement such as insider sabotage, theft, and espionage.

Reasons to Augment Command-and-Control with Positive Deterrence

There are four primary reasons why an IRMP should promote positive deterrence as a complement to existing command-and-control practices.

1. *Organizational practices and managerial processes can create a working environment conducive to insider threats by undermining goodwill on the part of employees.*

Employee goodwill is essential for maintaining acceptable levels of insider risk and for organizational success generally. Most insider incidents are perpetrated by individuals who started out as loyal employees. Yet as professional and/or personal stressors emerged, their motives shifted toward acting against the organization's interests (Shaw & Sellers, 2015). How organizations respond to these stressors can mitigate or exacerbate the disgruntlement the employee may feel.[2] Organizations can reduce the frequency of insider misbehavior and its

---

1 Command-and-control approaches rely on traditional forms of (negative) deterrence, which focus on a negative response to violations. References to employees in this article includes workforce members that are managed directly by the organization, whether they are full-time, part-time, or are contracted through a third party.

2 This insight does not imply that the organization is at fault in insider compromise—most insider threat incidents are violations of the law or agreements with the organization that are prosecutable in court.

associated costs by implementing practices that directly increase POS especially in stressful personal and professional situations (Moore et al., 2016).

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

Organizations cannot continue increasing the strength of command-and-control without eventually undermining employee goodwill (Moore, Novak, Collins, Trzeciak, & Theis, 2015). There is a natural limit to the security an organization can achieve through command-and-control alone. Positive deterrence—in the form of practices that increase workforce perceptions of organizational support—promotes a sense of organizational justice, shared goals and values, and helps ensure that individuals act to benefit the organization (Eisenberger and Stinglhamber, 2011 chap. 7; Moore 2018). Employees who identify with the organization and internalize its goals and values tend to display pro-social organizational behavior, including adhering to organizational rules beyond the levels observed with compliance-based approaches (Tyler, 2004; O'Reilly & Chatman 1986; Kelman 1958). Although external controls remain essential to IRMPs, inattention to positive deterrence leads to higher than necessary insider incident base rates and the recurrence of damaging incidents over time.

3. *Promoting positive deterrence practices significantly enhances achieving the IRMP mission.*

An exclusive focus on command-and-control strategy can pit the organization against its workforce, undermining the trust between management and employees. Positive deterrence creates a work environment that reinforces the bond between the organization and its workforce, contributing to the well-being of both. Positive deterrence also can help employees view command-and-control approaches as more legitimate and appropriate through the enhanced relationship POS-boosting practices promote (Martin, Wellen, & Martin, 2016). The proper balance of positive deterrence and command-and-control creates a net positive for both the employee and the organization. By improving employee working conditions and well-being, an IRMP can move from a "big brother" program to a "good employer" program.

4. *Positive deterrence can increase the desirable employee feelings and attitudes that improve general job performance.*

Research in Organizational Psychology demonstrates that while some (prevention-focused) employees are responsive to command-and-control approaches, that approach makes other (promotion-focused) employees feel stifled (Park, Hinsz, & Nick, 2015; Motyka et al., 2014). Fortunately, evidence-based positive deterrence practices that improve POS are shown to promote employee well-being and positive orientation toward the organization and work (Eisenberger & Stinglhamber, 2011, chap. 7) - outcomes that reflect a consequential array of employee attitudes and behavior:

- Employee subjective well-being: job satisfaction, organization-based self-esteem, reduced stress, work-family balance, and positive mood
- Positive orientation toward the organization and work: organizational commitment and identification, creativity and innovation, work engagement, trust, empowerment, and reduced cynicism

Improved organizational performance, and employee job performance, retention, and well-being are primary outcomes demonstrated in Organizational Psychology research (Pfeffer, 2018-a); these outcomes are a virtuous side effect of positive deterrence too.

Although research is continuing, the Organizational Psychology literature provides a convincing body of evidence that positive deterrence-related practices can be adopted *now* for the reduction of insider risk (Dalal & Gorab, 2016). We next describe how to leverage POS practices for positive deterrence.

Strategies to Augment Command-and-Control with Positive Deterrence

Five operational strategies help organizations use positive deterrence as part of insider risk management.

1. *Build quality relationships with organizational stakeholders, including line managers and members of human resources (HR) teams.*

IRMP leaders cannot implement positive deterrence by themselves: good working relationships with other organizational *stakeholders* are required. Many aspects of positive deterrence overlap with the work that line managers and HR teams do. Implementing positive deterrence necessitates joint action by line managers working with HR practitioners to create the supportive work settings that align employee interests with those of the organization. At present, few line managers or HR specialists recognize their own role in managing insider risk.

Organizational leadership should avoid tying the hands of the IRMP by restricting its scope to external controls. IRMPs must advocate for broader recognition of how company employment practices contribute to levels of insider risk. Taking on positive deterrence is not the expansion of scope it might first seem, but it does demand advocacy of supportive employment practices by IRMPs wherever insider risk exists. This proactive threat management perspective needs to be considered as part of the overall governance of the IRMP.

2. *Work with stakeholders to identify and implement workforce management practices that increase perceived organizational support.*

An employee's positive perceptions of the organization and its employment practices reduce risk of misbehavior. Here are some examples of workforce management practices that can increase employee POS:

- Organizational justice (e.g., treating employees with dignity, and compensating them equitably inside the organization and in line with industry standards)
- Performance-based rewards and recognition (e.g., using transparent criteria for promotions and rewards, and basing these rewards on project performance and other contributions)
- Honest and respectful communication (e.g., setting clear expectations, offering regular feedback and mentoring)
- Personal and professional support (e.g., offering employee assistance programs, promoting employee development, and empowering them on the job)

It is also important to hire employees with values congruent with those of the organization. (For more detail on organizational support principles and practices see Eisenberger & Stinglhamber 2011, chap. 8; Moore et al., 2016, chap. 5.) We advise organizations to focus on practices targeting their own challenge areas - areas that can be identified via on-going assessment (see strategy #3 below).

3. Regularly seek out and assess employee perspectives regarding the IRMP and the work environment; redesign practices accordingly.

Organizations benefit greatly from keeping up to date on how employees feel about their working environment generally and IRMP practices specifically. To learn more about employee perceptions, organizations can conduct surveys and focus groups. U.S. Federal Government organizations can take advantage of results from the annual Federal Employee Viewpoint Survey (OPM, 2020) and then conduct more in-depth follow-on assessments to probe various issues (e.g., POS or IRMP practices). Private organizations can leverage previously conducted employee climate and job satisfaction surveys in much the same way. Since even small pockets of problematic management practices or supervisory behaviors can increase insider risk, analyzing employee feedback requires drilling down into negative responses regardless of how well the organization performed overall.

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

Balancing command-and-control with positive deterrence is an effective strategy of insider threat reduction. It requires ensuring that combinations of practices work well together. "Working well" can mean that the advantages of practices in one area counter the disadvantages of practices in the other area.[3] Evidence suggests that external controls implemented consistently, with clear messaging and supportive training can reinforce rather than undermine the positive relationship promoted by organizational support. Motivational focus theory is useful in identifying the appropriate balance of prevention and promotion strategies at an individual or a team level. This balance can be promoted by bundling command-and-control and positive deterrence practices. Examples include:

- Combining practices that empower employees with those that implement employee monitoring. Evidence suggests that employee empowerment can mitigate dissatisfaction associated with employee monitoring policies (Martin et al., 2016).
- Bundling sanctions for rule violations with confidential grievance procedures to help ensure organizational justice.
- Ensuring investigations consider disconfirming as well as confirming evidence to reduce confirmation bias and increase perceptions of fairness (Tetlock, 1985).

[3] While the potential negative consequences of excessive command-and-control have been elaborated (Moore et al., 2015), positive deterrence practices can have negative consequences as well. Examples include heightened insider risk due to employees' excessive empowerment or over identification with the organization (Veenstra 2015).

These practices are not new for most organizations, but considering their combination explicitly in insider risk management may be. Importantly, IRMPs associated with introducing positive deterrence practices into workforce management can increase employee goodwill toward both the IRMP and the organization.

5. Train and incentivize management to deliver positive deterrence practices effectively.

Positive deterrence management practices often require supervisor training to reinforce needed change in management behavior (e.g., supervisor supportiveness). Such behavioral changes may require shifts in the organization's management culture along these dimensions. The best way to instill such change is to (1) align supervisors' goals and incentives with the practice intent and (2) train supervisors on how to execute those practices effectively (Rousseau, 1990). This process gradually helps supervisors internalize values and beliefs consistent with those behaviors, thus promoting the required dimension of cultural change (Eisenberger & Stinglhamber, 2011; Skarlicki & Latham, 2005).

Here is a roadmap for establishing positive deterrence as part of an IRMP:

- Coordinate with HR and other stakeholders to review management practices, including current or planned insider risk management command-and-control practices.
- Identify a candidate set of positive deterrence practices, bundled with command-and-control practices where appropriate, to establish a proper balance for the organization.
- Assess employee attitudes and perceptions. Using this as feedback regarding whether the set of practice bundles create the intended balance, redesign the set of practices accordingly.
- Specify organization-wide goals and incentives to instill positive deterrence as a foundation of insider risk management.
- Coordinate with stakeholders across the organization to implement the positive deterrence practices identified and train management to execute those practices effectively.
- Periodically assess, monitor, and adjust management practices, revisiting previous steps as appropriate.

This roadmap can be adapted as needed but on-going assessment and redesign is essential to ensure effective implementation.

Vision for the Future of Insider Risk Programs

Traditional IRMPs focus narrowly on command-and-control activities instead of incorporating proactive threat prevention into their efforts. IRMPs should become advocates of a supportive organizational climate to better balance command-and-control with positive deterrence.

Figure 1 illustrates the balanced defense resulting from combining positive deterrence and command-and-control. We combine the illustration Straub and Welke (1998) provide of a command-and-control approach with our representation of positive deterrence to show how the two complement each other. In addition to perceived organizational support as one avenue for

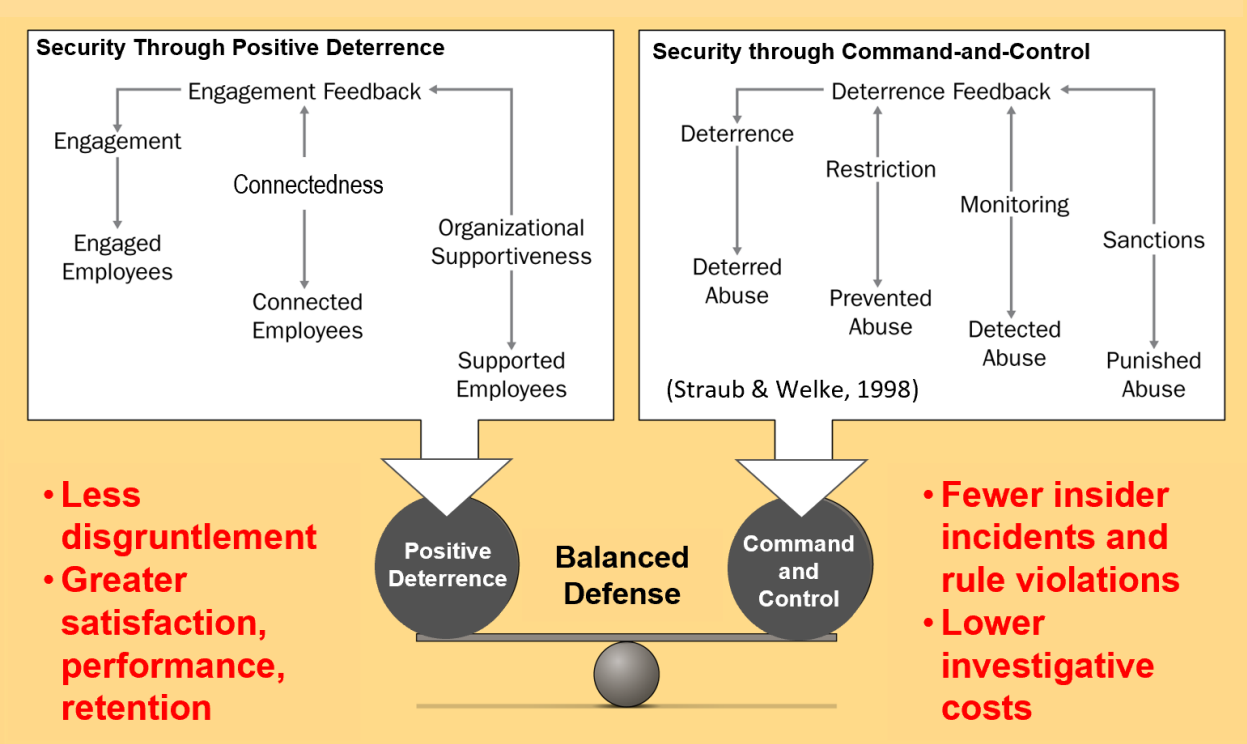
positive deterrence, organizations can consider two other Organizational Psychology concepts in the IRMP toolkit:

- job engagement—the extent to which employees are excited by and absorbed in their work (OPM, 2020; Schaufeli & Bakker, 2004)
- connectedness at work—the extent to which employees want to interact with, trust, and feel close to their co-workers (Brien et al. 2012; Malone, Pillow, & Osman, 2012)

These well-studied areas convey the many positive benefits of POS but in different ways (Pfeffer, 2018-b).

IRMPs that embrace positive deterrence can unlock greater potential to minimize insider risk and employees' negative perception of the command-and-control approach. Organizations that adjust management practices based on workforce attitudes send the message that they are an advocate for the workforce and strive to improve employee work and life. Such a message is valuable to all employees, particularly those who are turned off by programs focused strictly on discovering insider wrongdoing.

Figure 1: ***Extending the Traditional Security Paradigm with Positive Deterrence (Adapted from Moore et al., 2018)***



Acknowledgment

The authors would like to thank those who have helped to develop the area of work involving the positive deterrence of insider threat: Daniel Bauer, Tracy Cassidy, Mathew Collins, Daniel Costa, Jennifer Cowley Robert Ditmore, Susan Moore, David Mundie, Luke Osterritter, Michael Theis, Randall Trzeciak, and Nathan VanHoudnos. We would also like to thank the Software Engineering Institute technical editors: Barbara White and Sandy Shrum.

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.

References

Brien, M.; Forest, J.; Mageau, G. A.; Boudrias, J.; Desrumaux, P.; Brunet, L.; & Morin, E.M. (2012) “The Basic Psychological Needs at Work Scale: Measurement Invariance between Canada and France,” *Applied Psychology: Health and Well-Being*, 4(2), 167.

Dalal, R.S. & Gorab, A.K. (2016). Insider Threat in Cyber Security: What the Organizational Psychology Literature on Counterproductive Work Behavior Can and Cannot (Yet) Tell Us. In *Psychosocial Dynamics of Cyber Security* (pp. 122-140). Routledge.

Eisenberger, R. & Stinglhamber, F. (2011). *Perceived Organizational Support: Fostering Enthusiastic and Productive Employees.* American Psychological Association.

Kelman, H.C. (1958). Compliance, Identification, and Internalization Three Processes of Attitude Change. *Journal of Conflict Resolution, 2*(1), 51-60.

Martin, A.J.; Wellen, J.M.; & Martin, R.G. (2016). An Eye on Your Work: How Empowerment Affects the Relationship between Electronic Surveillance and Counterproductive Work Behaviours. *The International Journal of Human Resource Management, 27*(21), 2635-2651.

Malone, G.P.; Pillow, D.R.; & Osman, A. (2012) "The General Belongingness Scale (GBS): Assessing Achieved Belongingness," *Personality and Individual Differences*, 52(3).

Moore, A.P.; Perl, S.J.; Cowley, J.; Colins, M.L.; Cassidy, T.M.; VanHoudnos, N.; Buttles, P.; Bauer, D.; Parshall, A.; Savinda, J.; & Monaco, E.A. (2016). *The Critical Role of Positive Incentives for Reducing Insider Threats.* Pittsburgh: Software Engineering Institute. doi:10.1184/R1/6585104.v1

Moore, A.P.; Cassidy, T.M.; Theis, M.C.; Bauer, D.; Rousseau, D.M.; & Moore, S.B. (2018). Balancing Organizational Incentives to Counter Insider Threat. *In 2018 IEEE Security and Privacy Workshops (SPW)* (pp. 237-246). San Francisco: IEEE Security. doi:10.1109/SPW.2018.00039

Moore, A.P.; Novak, W.E.; Collins, M.L.; Trzeciak, R.F.; & Theis, M.C. (2015). Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls Software Engineering Institute. *White Paper*. Pittsburgh: Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

Motyka, S.; Grewal, D.; Puccinelli, Nancy M.; Roggeveen, A.L.; Avnet, T.; Daryanto, A.; de Ruyter, K.; & Wetzels, M. (2014). Regulatory Fit: A Meta-Analytic Synthesis. *Journal of Consumer Psychology, 24*(3), 394-410.

Office of Personnel Management (OPM). (2020) *Federal Employee Viewpoint Survey Results: Empowering Employees. Inspiring Change.*, U.S. Office of Personnel Management.

O'Reilly, C.A. & Chatman, J. (1986). Organizational Commitment and Psychological Attachment: The Effects of Compliance, Identification, and Internalization on Prosocial Behavior. *Journal of Applied Psychology, 71*(3), 492.

Park, E.S.; Hinsz, V.B.; & Nick, G.S. (2015). Regulatory Fit Theory at Work: Prevention Focus' Primacy in Safe Food Production. *Journal of Applied Social Psychology, 45*(7), 363-373.

Pfeffer, J. (2018-a). Dying for a paycheck: How modern management harms employee health and company performance—and what we can do about it.

Pfeffer, J. (2018-b). The overlooked essentials of employee well-being. McKinsey Quarterly, 3(2018), 82-89.

Rousseau, D. M. (1990). Assessing Organizational Culture: The Case for Multiple Methods. *Organizational climate and culture*, *153*, 192.

Schaufeli, W.B. & Bakker, A.B. (2004) "Job Demands, Job Resources, and Their Relationship with Burnout and Engagement: A Multi-Sample Study," *Journal of Organizational Behavior, 25*(3), 293.

Shaw, E. & Sellers, L. (2015). Application of the Critical-Path Method to Evaluate Insider Risks. *Studies in Intelligence*, *59*(2), 1-8.

Skarlicki, D.P. & Latham, G.P. (2005). How Can Training Be Used to Foster Organizational Justice? In J. Greenberg, & J. A. Colquitt (Eds.), *Handbook of Organizational Justice* (p. Chapter 17).

Straub, D.W. & Welke, R.J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469. doi:10.2307/249551

Tetlock, P. (1985) Accountability: A Social Check on the Fundamental Attribution Error. *Social Psychology Quarterly*, 48, 227-236.

Tyler, T. R. (2004). *Promoting Employee Policy Adherence and Rule Following in Work Settings—The Value of Self-Regulatory Approaches.* Brooklyn Law Review 70.

Veenstra, K. (2015). Loyalty, Social Identity and Insider Threat. Paper prepared for the Australian Crime Commission. Available at: linkedin.com/in/kris-veenstra-phd-401a7110b