Measuring and Mitigating Organizational-Culture Vulnerabilities to Reduce Insider Risk

RESEARCH FOCUS

Insider risk management typically focuses on potential risk indicators (PRIs) of individual workforce members for measuring risk and omits an analysis of the organizational-culture vulnerabilities present at the time of the incident. Our analytical approach identifies ***measures*** of organizational-culture vulnerability associated with bundled deterrence ***mitigators*** to enable evidence-based insider risk management.

Definitions

- Bundled Deterrence: Combination of positive and negative deterrence mitigators to reduce the likelihood workforce members will engage in insider threat behaviors.
- Organizational-Culture Vulnerabilities: Factors associated with an organization's norms and behaviors which make it susceptible to insider incidents .

METHODOLOGY

Case Study Analysis: Investigated 1,500 cases of prosecuted insider threat incidents to find organizational/cultural vulnerabilities which can be measured and mitigated.

Literature Review: Surveyed multiple resources to find measures of organizational culture vulnerabilities linked to insider threat observables and to find positive and negative deterrence practices associated with mitigating insider threats. Research examined literature around Perceived Organizational Support (POS), Counterproductive Workplace Behaviors (CWBs), and Employee Deviance.

References

[1] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes. Addison-Wesley.

[2] Clayton, S. J. (2019, December 5). 6 Signs Your Corporate Culture is a Liability. Harvard Business Review.

[3] DeConinck, J. B. (2010). The effect of organizational justice, perceived organizational support, and perceived supervisor support on marketing employees' level of trust. Journal of Business Research, 1349 – 1355.

[4] Eisenberger, R., and Stinglhamber, F. (2011). Perceived organizational support: Fostering enthusiastic and productive employees. American Psychological Association.

[5] Moore, A. P., Miller, S., Horneman, A., & Rousseau, D. (2021). Shaping Organizational Culture through Balanced Deterrence. SBS Summit.

[6] National Insider Threat Center. (2018). Common Sense Guide to Mitigating Insider Threats, 6th Edition. Carnegie Mellon University Software Engineering Institute.

[7] Rousseau, D. (1990). Assessing organizational culture: The case for multiple methods. In Organizational Culture. Frontiers of Industrial and Organizational Psychology. San Francisco: Jossey-Bass.

TAKEAWAYS: MEASURES & MITIGATORS

Measures

- How **efficient** and **effective** is the employee complaint process?
- How **supportive** and **fair** is management perceived?
- How **diverse** and **inclusive** is the organization perceived to be?
- How **ethical** and **values-based** is the organization perceived to be?
- How **competitive** is the organization perceived to be?
- How **clear** and **organized** is the management structure?
- How **valued** do workforce members feel?
- How **accountable** is the organization perceived to be?

Fig 2: Measures of organizational-culture vulnerabilities (Clayton, 2019) (Eisenberger, 2011). Measures can be assessed via surveys, focus groups, interviews, and via operational process timing (e.g., response times).

Organizational-culture vulnerabilities are manageable factors that can be measured and mitigated to protect against insider risk.

Mitigators

Negative Deterrence		Positive Deterrence
Incident Stories in Awareness Training	+	Wellness Stories in Awareness Training
Technical Constraints	+	Team Building Initiatives
Suspicious Activity Reporting	+	Performance-Based Recognition
Detections/Sanctions Policy	+	Workforce Satisfaction Survey
Confirming Evidence	+	Disconfirming Evidence

Fig 3: Mitigators of bundled deterrence (Moore, 2021). Negative deterrence attempts to force the workforce to act in the interests of the organization, whereas positive deterrence attempts to attract the workforce to act in the interests of the organization.

CASE EXAMPLES

Unresolved Concerns

*The insider was employed as a systems administrator by the victim organization, which provided unified messaging services to customers. The insider discovered a security flaw in the email system and reported it, and then **became disgruntled when the organization failed to fix the bug**. The insider resigned to work for another company. After leaving they used a valid email account, which had not been disabled, to email the victim organization's customers about the security flaw.*

- Perceived inefficient and ineffective complaint resolution.
- Establish a culture of accountability from the top down *(Clayton, 2019).*

Lack of Accountability

*The insider was a foreign currency trader for a financial institution. An acquisition of the company made the insider's **supervision ambiguous**. Their responsibilities were to collect and trade assets in order to generate profits. The yearly bonus was tied to the profit produced. They **executed a complex fraud scheme** convincing other employees not to track the insider's trades and validate them. The **company did not record trading phone calls and remote access was used to continue the fraud**.*

- Perceived ambiguous management.
- Clearly document and consistently enforce policies and access controls *(National Insider Threat Center, 2018).*

Harassment and Hostility

*A foreign national employed as a systems analyst, database administrator, and project manager for a government entity **filed a complaint with Human Resources (HR) against their supervisor for harassment and discrimination**. The insider's **work performance declined and they resigned**, taking a position with another government entity. Their **negative performance reviews were sent to their new employer**. They remotely dialed in to the former employer's systems and altered the database.*

- Perceived hostile and discriminatory work environment.
- Document and enforce anti-harassment policies. Amplify Diversity, Equality, and Inclusion (DEI) initiatives *(Clayton, 2019).*

Carnegie Mellon University
Software Engineering Institute

Hui-Chen Betty Liu & Isabel Gardner | hliu@cert.org / isgardner@sei.cmu.edu
Under supervision of Carrie Gardner and Andrew P. Moore

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.

DM21-0787