Understanding Insider Risk

Bob Ditmore

rmditmore@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

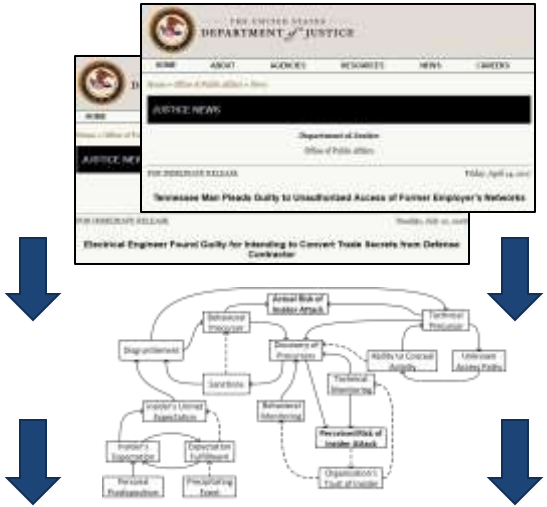
Document Markings

DM22-0508

The Software Engineering Institute

- A United States Department of Defense Federally Funded Research and Development Center (FFRDC)
- Vision: leading and advancing software engineering and cybersecurity to solve the nation's toughest problems
- Mission: to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

Insider Risk at The CERT Division of Carnegie Mellon University's Software Engineering Institute




```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *"
| eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address,
recipient_address, message_subject, total_bytes'
```

Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats since 2001

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

The Insider Threat Defined

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Untangling Insider Taxonomy

Insider: An *insider* of an organization is an employee, contractor, or other business partner who *has or had* authorized access to the organization's critical assets.

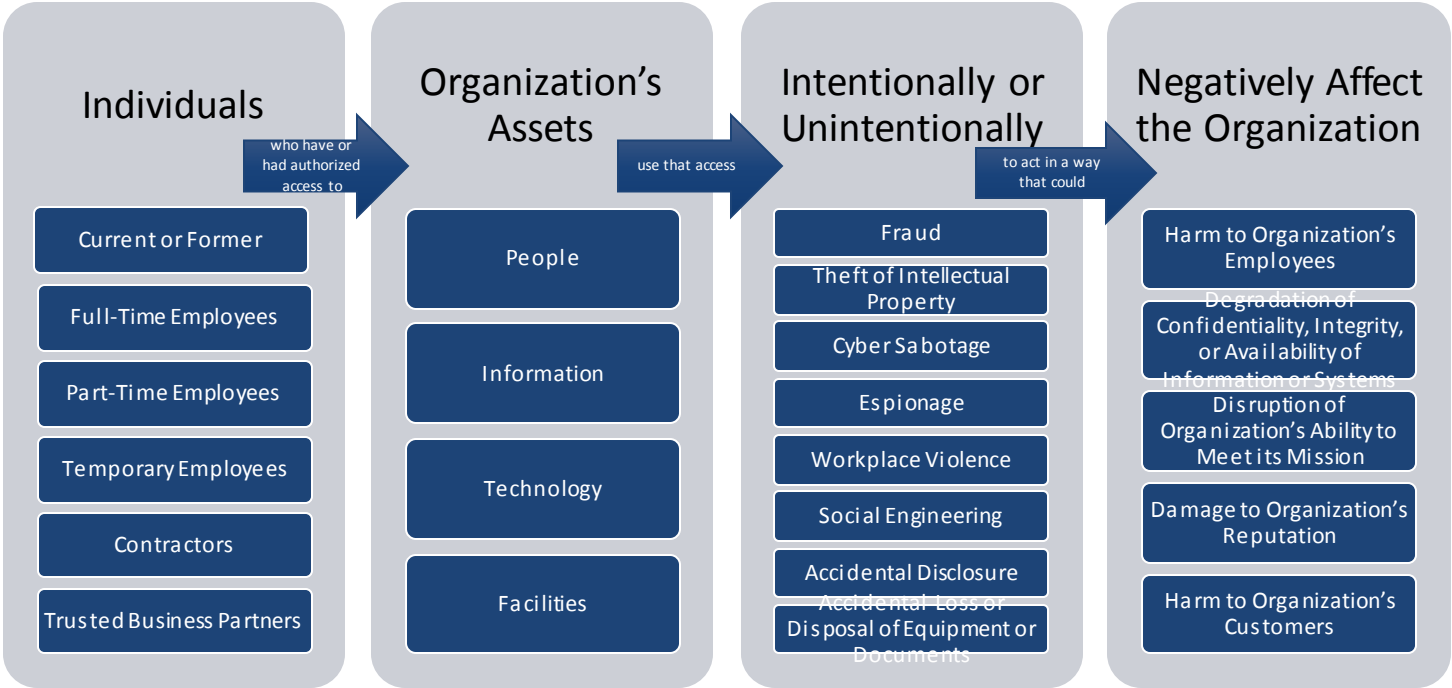
Insider Threat: *Insider threat* for an organization is the potential for an insider to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Insider Risk: *Insider risk* is the potential for loss associated with the realization of an insider threat.

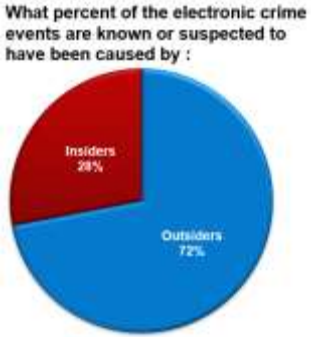
Insider risk is unique in organizational security in that the potential threat agents play fundamental roles in accomplishing the organization's mission.

- Insider goodwill is essential to both keeping intentional insider risk to a minimum and ensuring organizational success generally.

Scope of the Insider Threat

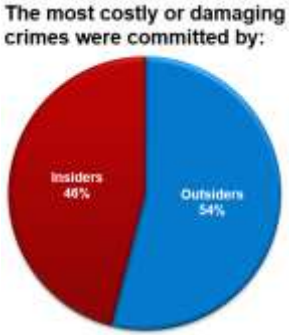


Scale of the Insider Threat



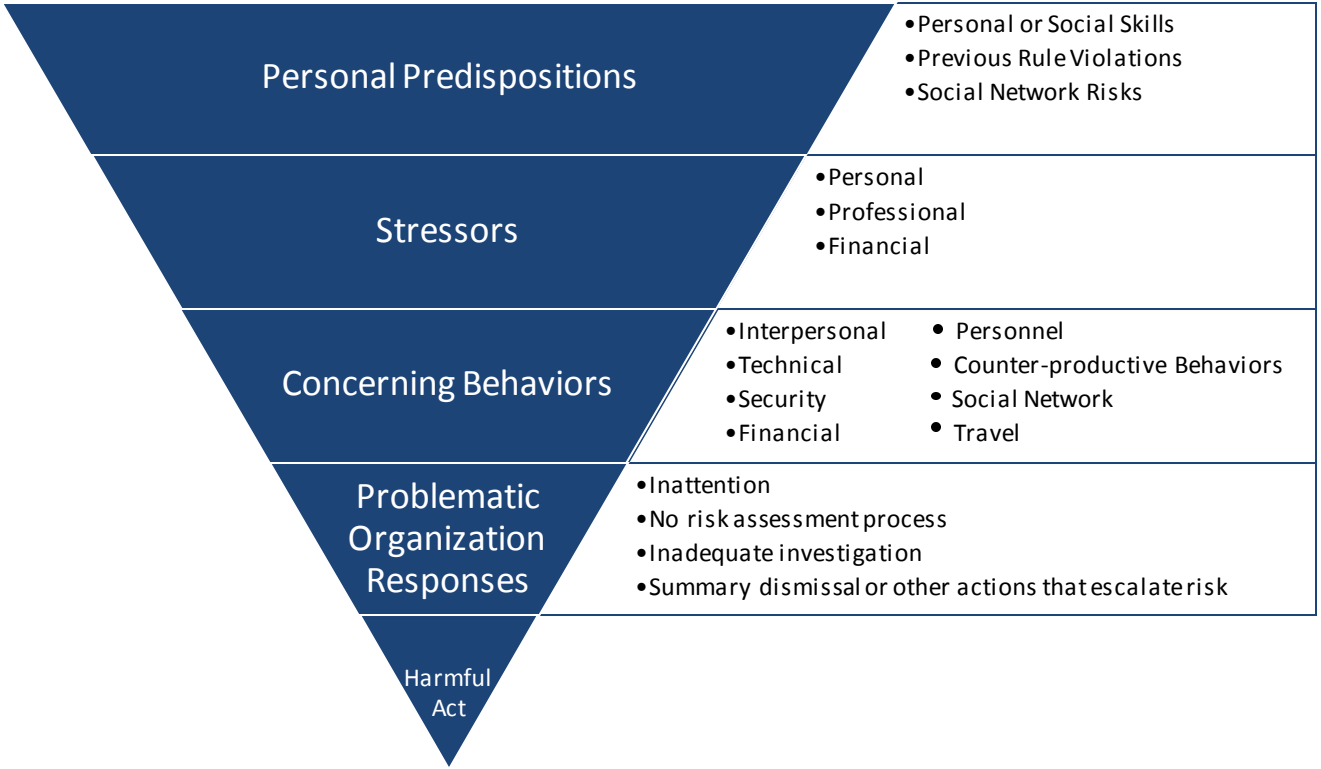
What percentage of certain types of security incidents were perpetrated by insiders?

Confidential records (trade secrets or intellectual property) were compromised	79%
Customer records were compromised	79%
Private or sensitive information was intentionally exposed	70%
Theft of personally identifiable information (PII) (customer or partner data)	66%
Systems were sabotaged (deliberate disruption, deletion or destruction of information, systems or networks)	65%
Private or sensitive information was unintentionally exposed	56%



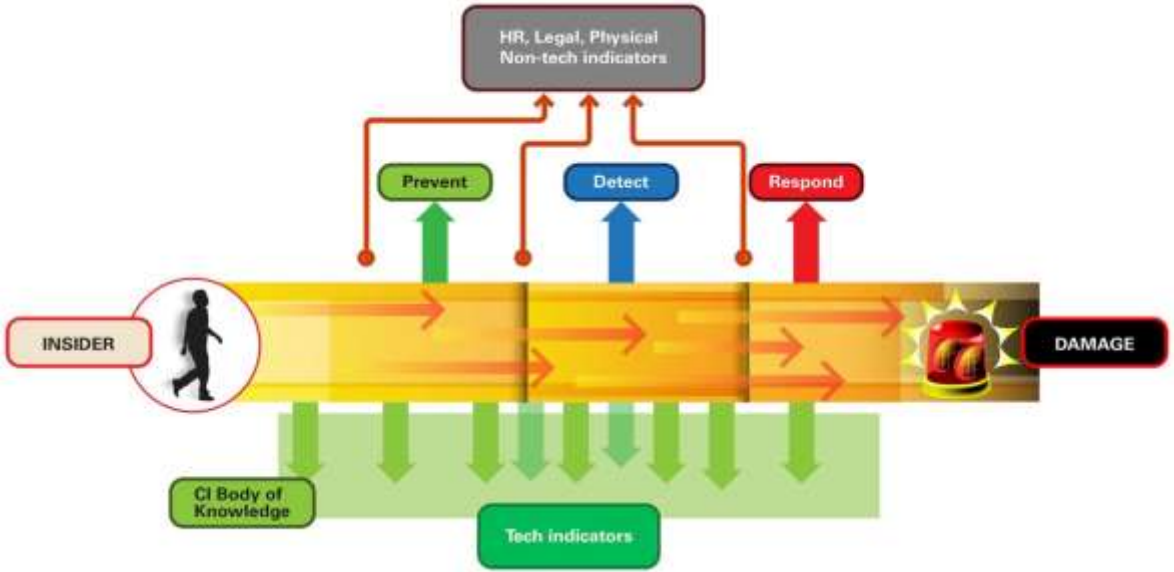
Sources: 2004-2018 U.S. State of Cybercrime Survey, in partnership with KnowBe4, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

The Critical Path to Insider Risk



Adapted from Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)

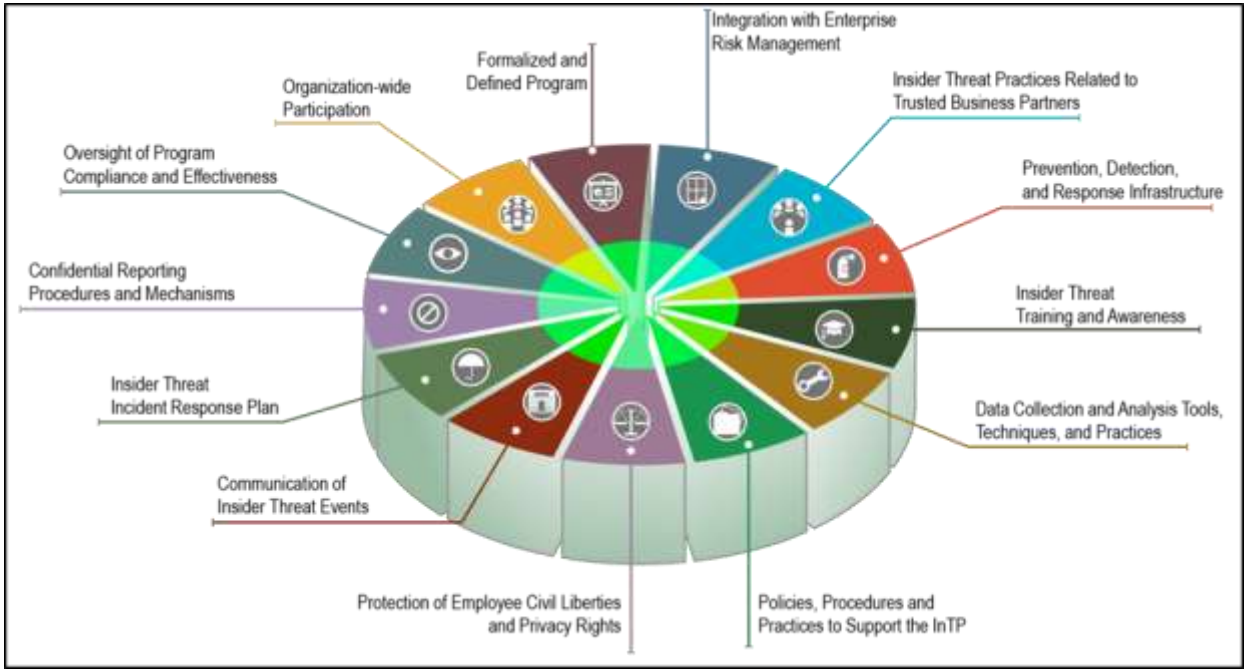
The Goal for an Insider Threat Program…



Is to reduce insider risks to critical assets to acceptable levels

https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html

Key Components of an Insider Threat Program



Best Practices from the CERT Common Sense Guide to Mitigating Insider Threats

1 - Know and protect your critical assets.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
2 - Develop a formalized insider threat program.	13 - Monitor and control remote access from all endpoints, including mobile devices.
3 - Clearly document and consistently enforce policies and controls.	14 - Establish a baseline of normal behavior for both networks and employees
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	15 - Enforce separation of duties and least privilege.
5 - Anticipate and manage negative issues in the work environment.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	17 - Institutionalize system change controls.
7 - Be especially vigilant regarding social media.	18 - Implement secure backup and recovery processes.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	19 - Close the doors to unauthorized data exfiltration.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	20 - Develop a comprehensive employee termination procedure.
10 - Implement strict password and account management policies and practices.	21 - Adopt positive incentives to align the workforce with the organization.
11 - Institute stringent access controls and monitoring policies on privileged users.	http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644

The Importance of Positive Deterrence to Insider Risk Management

Balanced Deterrence is Key

Balanced deterrence combines traditional security controls (command-and-control) with practices to increase employees' perceptions of organizational support (positive deterrence)

Command-and-Control

Workforce management practices that attempt to *force* employees to act in the interests of the organization

Employee Constraints, Monitoring, Punishment

Positive Deterrence

Workforce management practices that attempt to *attract* employees to act in the interests of the organization

Value Employee Contributions, Care about Well-Being, Treat Fairly

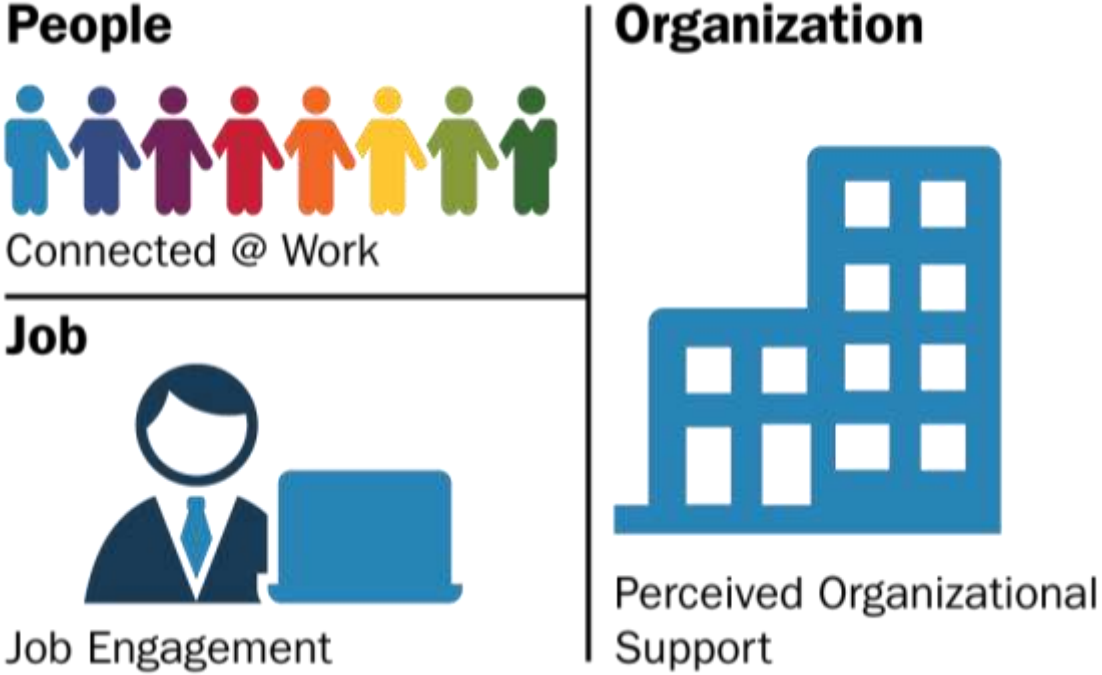
- Command-and-control *alone* can *exacerbate* the threat it is intended to mitigate
- Positive deterrence shown to reduce insider misbehavior through organizational justice, performance-based rewards/recognition, respectful communication, supervisor support
- ***Both*** positive and negative deterrence needed in *balance that is right* for organization

BUT organizational culture can be a significant barrier to adoption.

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

Three Categories of Positive Deterrence-Related Practices



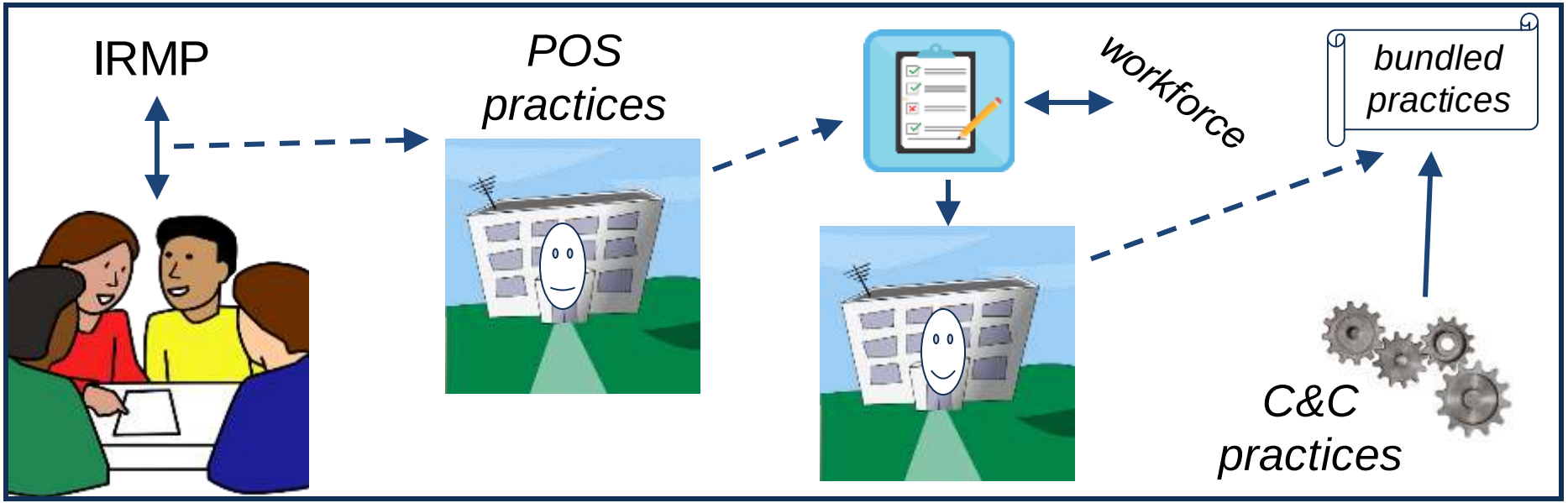
What Can Orgs Do Now to Implement Positive Deterrence

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 perspectives on IRMP and working environment

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



Keys for Successful Stakeholder Identification and Engagement

Keys to success include:

- Identifying stakeholders as early as possible
- Continually evaluating the list for needed additions
- Creating a communication strategy that is inclusive and bi-directional
- Meeting frequently, both as a group and in individual settings (where appropriate)

Establish Relationships and Engagement

Support and engagement can include:

- senior leader assigned as director/head of the insider threat program (*different than the InTP manager*)
- memos to key stakeholders, business process owners, and organizational senior management
- strategic meetings with key stakeholders
- stakeholder attendance at planning meetings
- ongoing references to insider threat issues in meetings, publications, and training

Keeping Stakeholders Engaged

Obtain continuous feedback.

Use incident scenarios as table-top discussions.

- use real incidents to discuss potential problems
- creatively use news articles affecting organizations similar to yours
- describe how insider activities can affect employees' jobs

Use secure forums to discuss lessons learned.

Contact Information

Bob Ditmore

Team Lead – Insider Risk, CERT Division

Software Engineering Institute

Carnegie Mellon University

rmditmore@sei.cmu.edu

https://www.sei.cmu.edu/our-work/insider-threat/index.cfm