Best Practices for Building an Effective Insider Risk Management Program Hub

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Commerce 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 sponsored by the United States Department of Defense.

DM22-0904

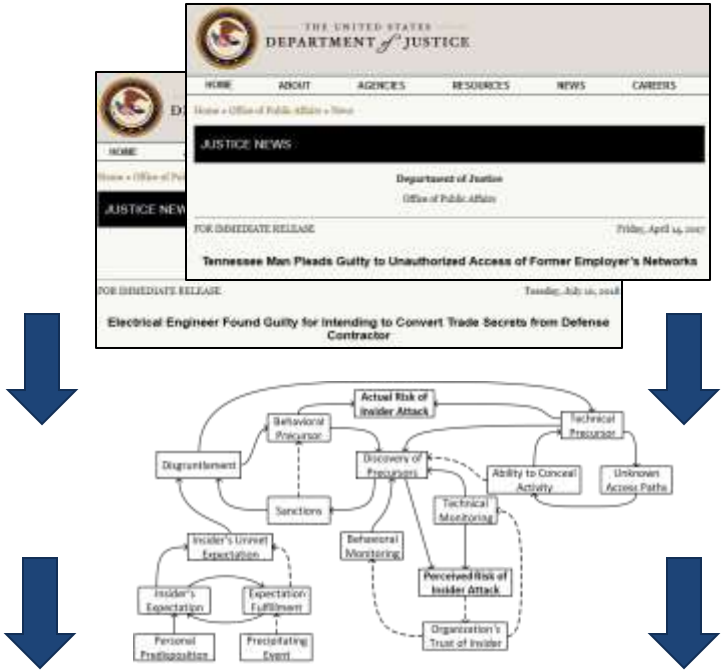
Agenda

Insider Risk Overview – Scope and Scale

Insider Risk Management Program Hub Introduction

Best Practices for Insider Risk Management Hub Building

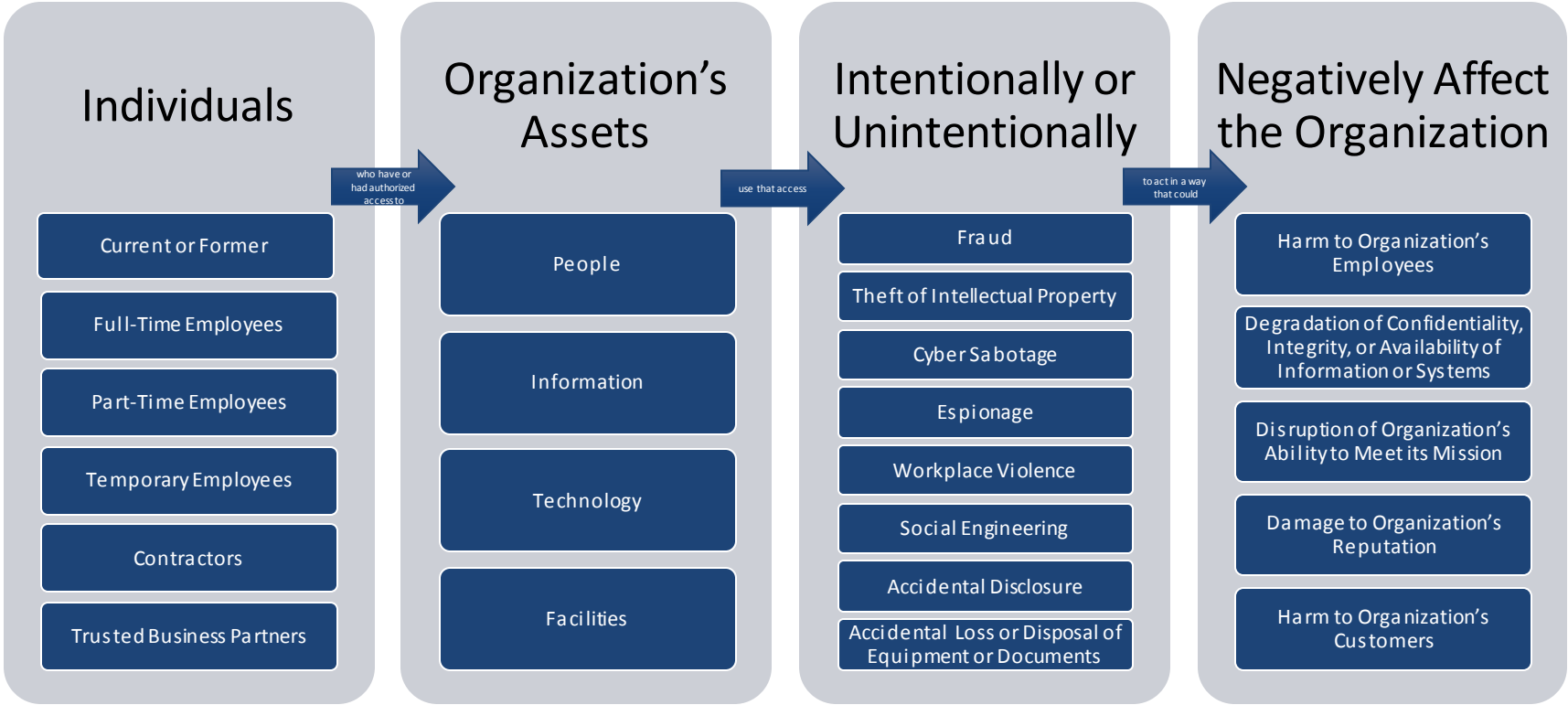
Insider Risk Research at the SEI




```
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 data collection, modeling, analysis, and outreach to develop socio-technical solutions to help organizations more effectively manage insider risk

Scope of the Insider Risk



Scale of the Insider Risk

1 in 3 cybercrimes are perpetrated by insiders

Insider incidents have increased by 47% since 2018 (Source: Ponemon 2022 Cost of Insider Threat Global Report)

1 in 4 insider incidents are perpetrated by trusted external entities

1 in 3 insider incidents are committed with malicious intent

Insider Risk Management Program Hub Overview

A centralized capability for data collection, correlation, analysis and response

Common hub capabilities

- Collect, correlate, and aggregate data from disparate sources.
- Develop, deploy, and refine indicators of potential insider activity.
- Evaluate detected instances of potential insider activity.
- Provide supporting information to incident investigators and responders.

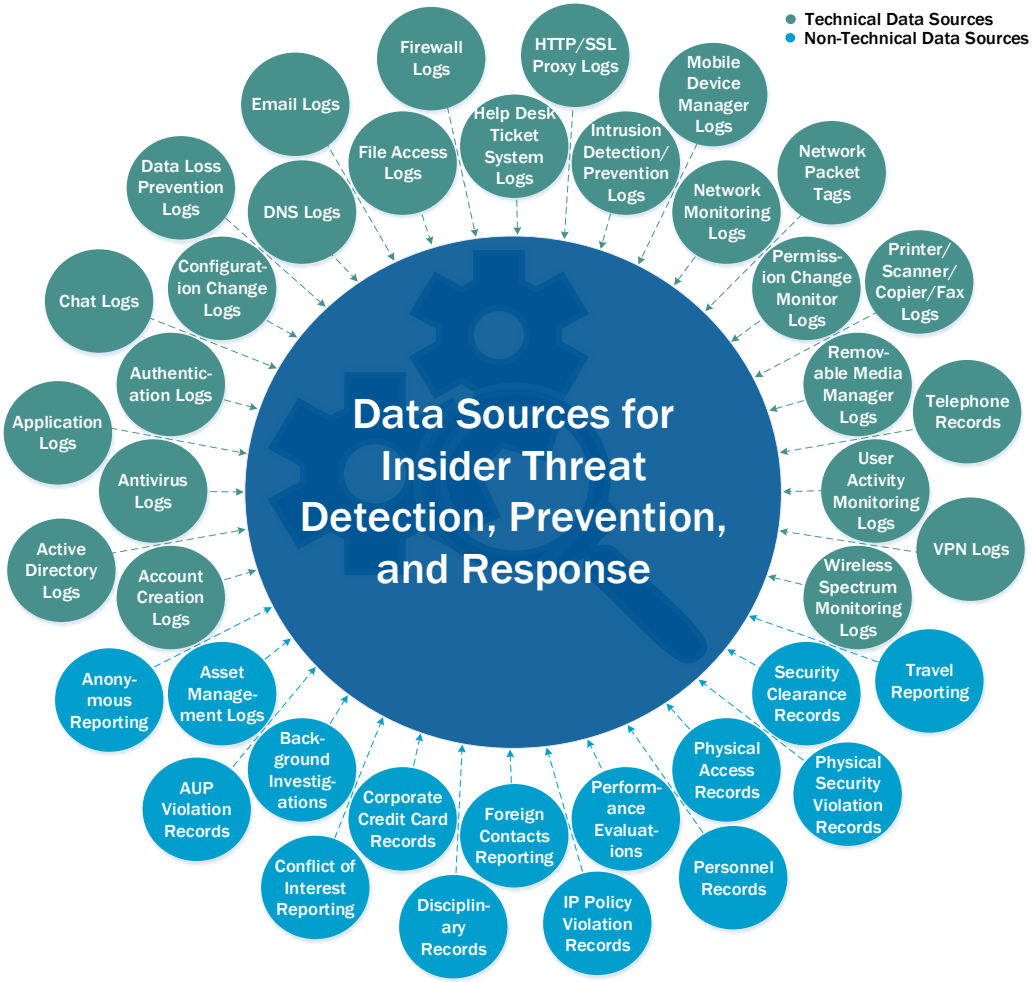
A hub is NOT a specific tool, but typically a collection of technical and administrative tools, data, capabilities, and authorities

Hub Benefits

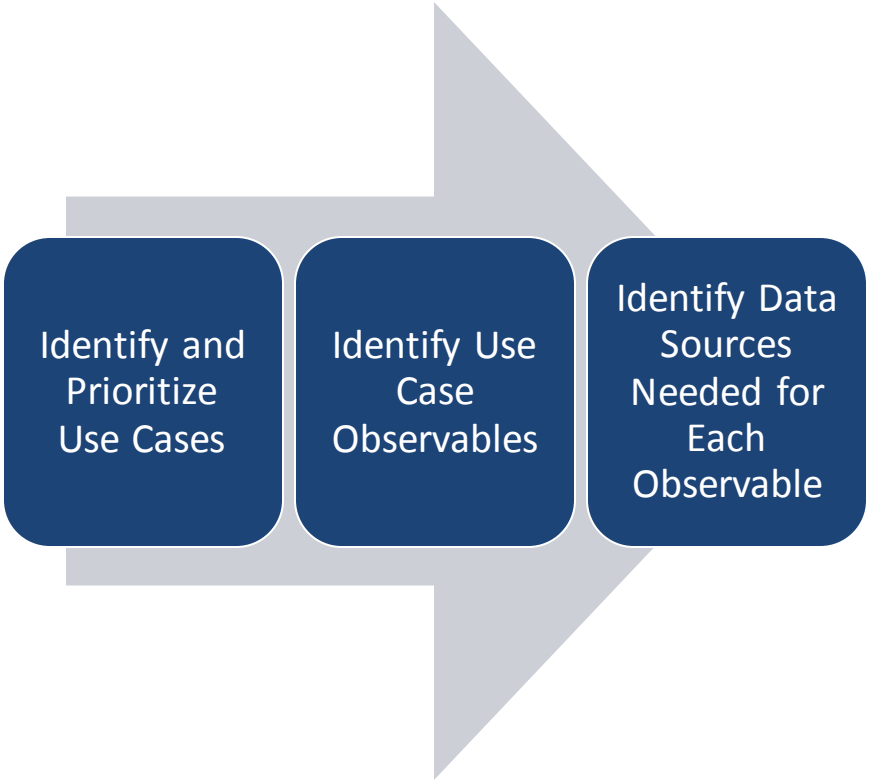
Allows the organization to discreetly identify anomalies and analyze potential insider risk activity

Produces a better “whole person” picture and provides contextual information to potential insider risk activity

Can facilitate information sharing across previously stove-piped groups within an organization



Data Source Selection



A use case-based approach is the key to success.

- Enables effective prioritization of limited resources
- Facilitates development of clear data access request justifications
- Aligns with risk management processes
- Promotes effective participation of InTP stakeholders

Use-Case Based Data Source Prioritization Example

Use Case	Use Case Priority	Observable	HR System	DLP Logs	Help Desk Tickets	Active Directory Logs	Windows Event Logs
Departing Employee IP Theft	HIGH	Employee Termination	X				
	HIGH	Data Exfiltration		X			
Unauthorized Account Creation	MEDIUM	Account Creation				X	
	MEDIUM	Job Role of Account Creator	X				
	MEDIUM	No Associated Help Desk Ticket			X		
Clearing Security Logs	LOW	Windows Security Logs Cleared					X
…							
Data Source Priority Score			**5**	**3**	**2**	**2**	**1**

Hub Analysis Workflow

Analytics are run over hub data.

Alerts that correspond to indicators of insider activity are generated.

Hub analysts review alerts, using contextual data where applicable, and determine appropriate *next steps*.

Alert is determined to be a false positive

- Dismiss alert, potentially update analytics.

Alert is determined to be a legitimate concern

- Follow policies and procedures for opening and conducting inquiries/ investigations.
- Refer to other group (HR, legal, management, insider threat program manager) for further action.

More information is needed to discern between false positive and legitimate concern

- Gather additional data (in hub or elsewhere).

Hub Management – Data Access Process

Develop standardized process for requesting and integrating new data sources, which includes					
Justification for access	Authorization from senior management	Sign-off from legal	Continued support to securely access the data source	Data access and retention policies	Determine handling and safeguarding requirements from the data owner

Don't compromise the security of the organization for the sake of having access to data

Hub Building Considerations

Start with collecting and aggregating existing data sources.

Start with developing potential risk indicators for most critical concerns.

Identify critical capability gaps, and incrementally address these gaps.

Leverage automation where possible to minimize manual efforts for aggregation, correlation, and triage.

Best Practices for Internal Risk Mitigation

1. Know and protect your critical assets	2. Develop a formalized insider risk management program
3. Clearly document and consistently enforce administrative controls	4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior
5. Anticipate and manage negative issues in the work environment	6. Consider threats from insider and trusted external entities in enterprise-wide risk assessments
7. Be especially vigilant regarding social media	8. Structure management tasks to minimize insider stress and mistakes
9. Incorporate insider threat awareness into periodic security training for all workforce members	10. Implement strict password and account management policies and practices
11. Institute stringent access controls and monitoring policies on privileged users	12. Deploy solutions for monitoring workforce member actions and correlating information from multiple sources
13. Monitor and control access from all end points, including mobile devices	14. Establish a baseline of normal behavior for both networks and workforce members
15. Enforce separation of duties and least privilege	16. Define explicit security agreements for clous services, especially access restrictions and monitoring capabilities
17. Institutionalize system change controls	18. Implement secure backup and recovery processes
19. Mitigate Unauthorized data exfiltration	20. Develop a comprehensive workforce member termination procedure
21. Adopt positive incentives to align the workforce and the organization	22. Learn from past insider incidents

https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

A Holistic Approach to Insider Risk Management

Summary

An effective insider risk management program hub requires a solid foundation.

- Existing infrastructure that follows cybersecurity best practices
- Organization-wide willingness to participate in data and information sharing, including senior leadership buy-in

Developing an effective insider risk management program hub involves tailoring existing policy and infrastructure to support.

- Data collection and analysis
- Incident response

An hub is an essential part of a formal Insider Risk Management Program.

For More Information

Insider Threats in the Software Development Life Cycle

Balancing Organizational Incentives to Counter Insider Threat

Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program

Insider Threats Across Industry Sectors

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

Analytic Approaches to Detect Insider Threats

Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments

Workplace Violence & IT Sabotage: Two Sides of the Same Coin?

An Insider Threat Indicator Ontology

Questions / Discussion

Presenter Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, Enterprise Threat and Vulnerability Management

CERT Division

Software Engineering Institute

Carnegie Mellon University

dlcosta@sei.cmu.edu

412-268-8006