Spotlight On: Insider Threats in the Supply Chain

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 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.

DM21-0495

Prevalence of the Problem

For the finance and insurance sector, **38%** of insider incidents were known to be perpetrated by trusted business partners

https://insights.sei.cmu.edu/blog/patterns-and-trends-in-insider-threats-across-industry-sectors-part-9-of-9-insider-threats-across-industry-sectors/

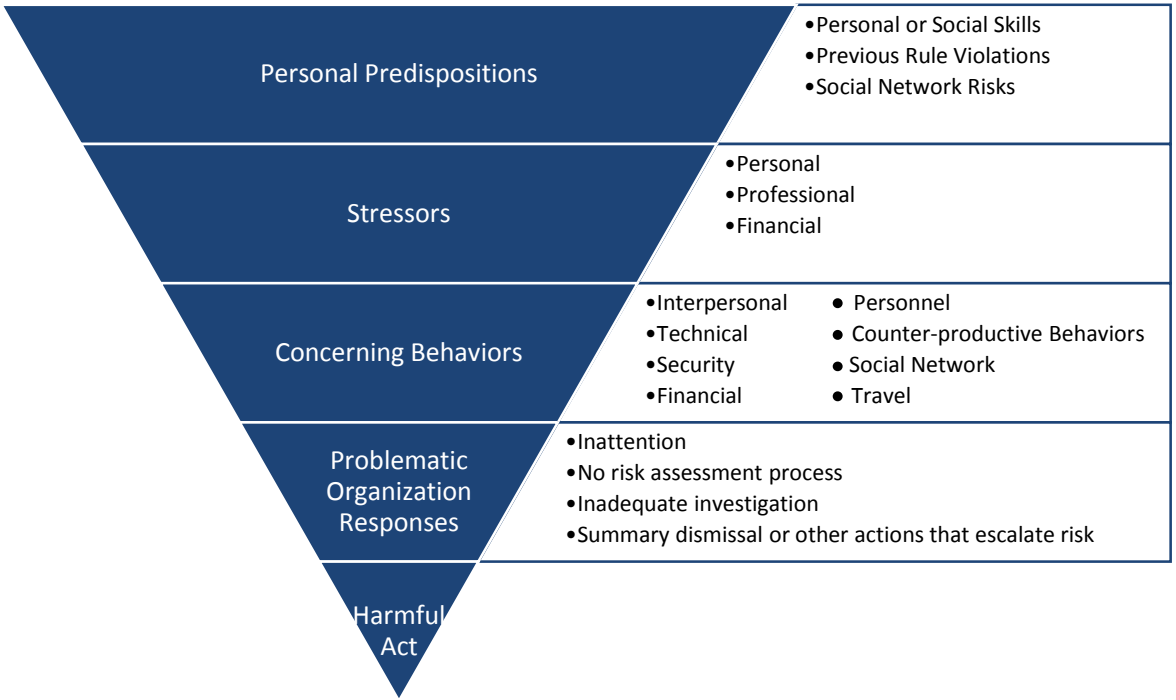
Scope of the Challenge

How extensive is the challenge of achieving each of the following for insider risk programs?

Challenge	Respondent Count	Low	Medium Low	Medium	Medium High	High
Coordinating and communicating across business / operational units	50				✓	
Establishing the insider threat program scope and organizational structure	50			✓		
Ensuring compliance with all applicable legal requirements	50			✓		
Developing policy and formalizing the program	50			✓		
Incorporating insider threat controls for trusted business partners	49				✓	
Obtaining adequate funding for program operation	50				✓	
Developing and administering insider threat awareness training	50			✓		
Hiring and retaining qualified insider threat program personnel	48			✓		
Sharing information across the organization's departments / units, including Human Resources (HR)	50				✓	

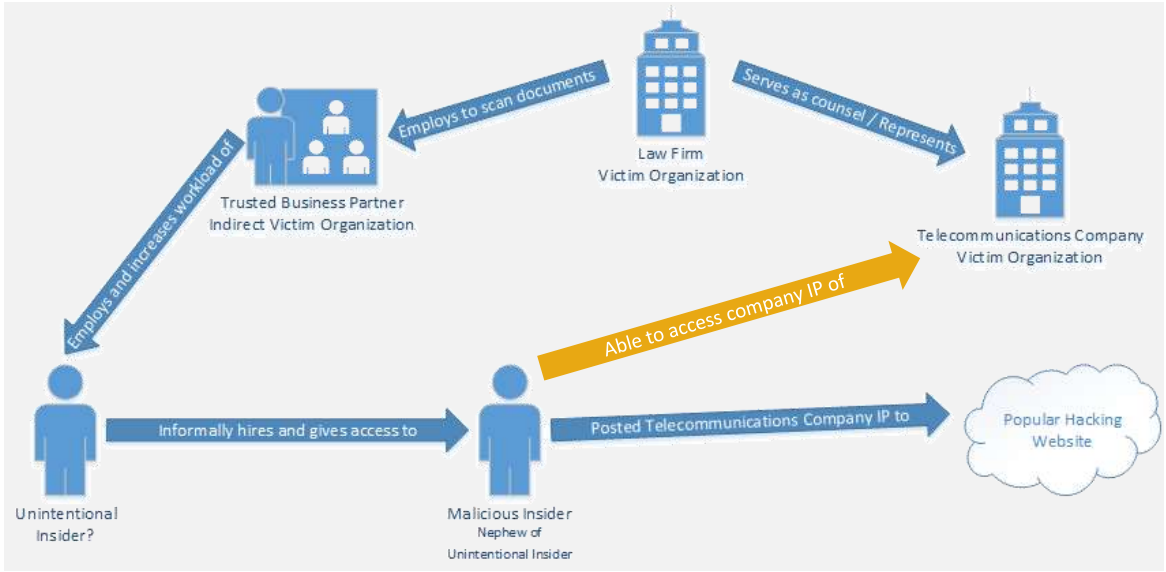
https://www.cylab.cmu.edu/_files/documents/irm-survey-results-20210331.7.pdf

Insider Incident Progression



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)

A Case Study



A contractor was unofficially working for the company's TBP, a document imaging company.

The victim organization was a high technology company. The TBP was hired to copy trade secrets in preparation for litigation. The insider was hired informally by a family member, to assist with the high workload.

The insider stole and posted trade secrets, design notes, and correspondence between the victim organization and a collaborator. The incident related loss was approximately $25 million.

Best Practices for Supply Chain Insider Risk Management

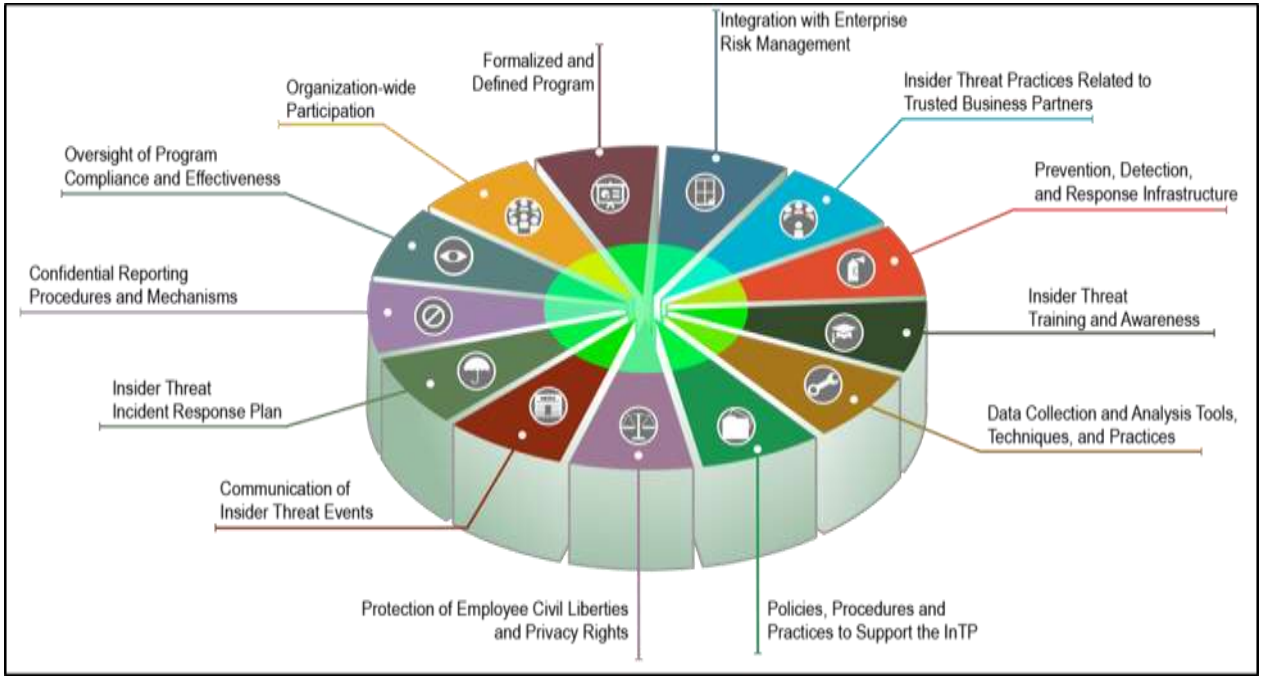
Policies, practices, and procedures – yours and your trusted business partners

- Non-disclosure and intellectual property agreements
- Background screening
- Concerning behavior reporting

Contractual agreements that “raise the bar” for technical controls and information sharing

Goal: apply security controls and risk management activities based on levels of access, not employment status

Components of a Successful Insider Risk Management Program



Q&A

For More Information

- CERT Common Sense Guide to Mitigating Insider Threats
- Spotlight On: Insider Threat From Trusted Business Partners
- Insider Threats in the Finance and Insurance Sector
- Additional Inquiries: insider-threat-feedback@cert.org