Analytic Approaches to Insider Risk Quantification

Dan Costa

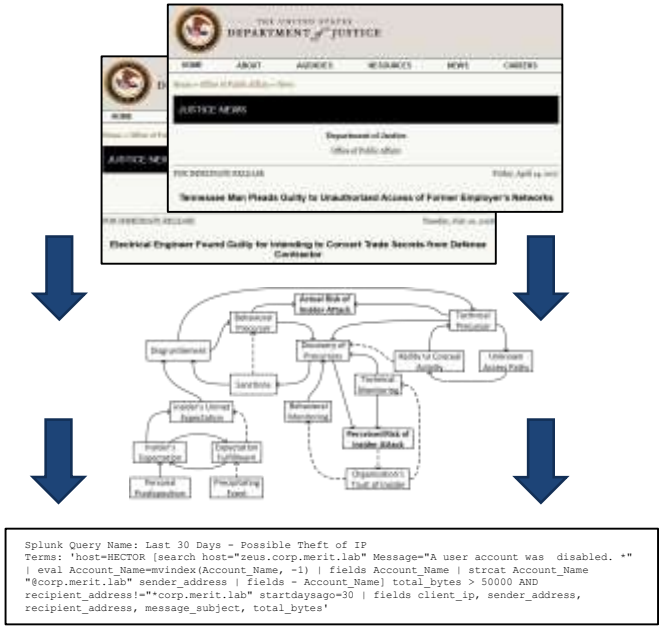
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

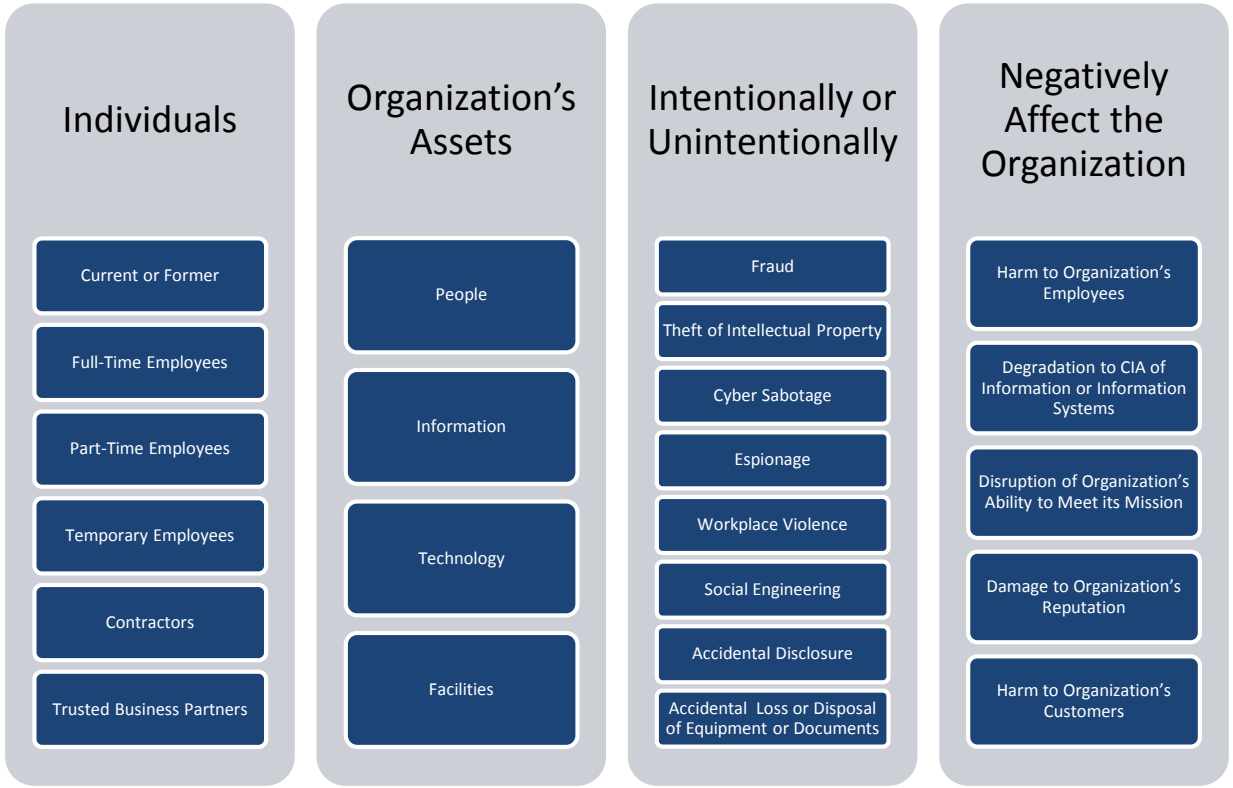
DM20-0828

The CERT National Insider Threat Center

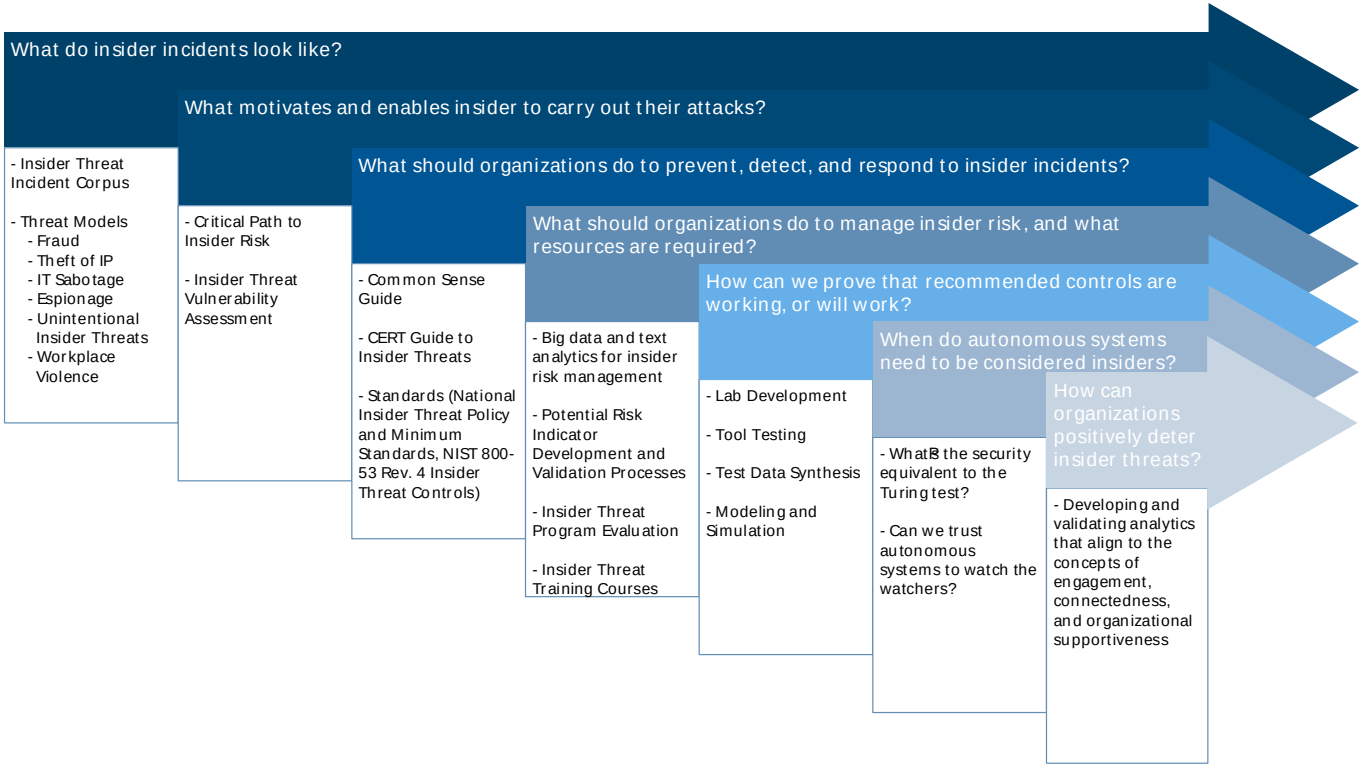


Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats since 2001

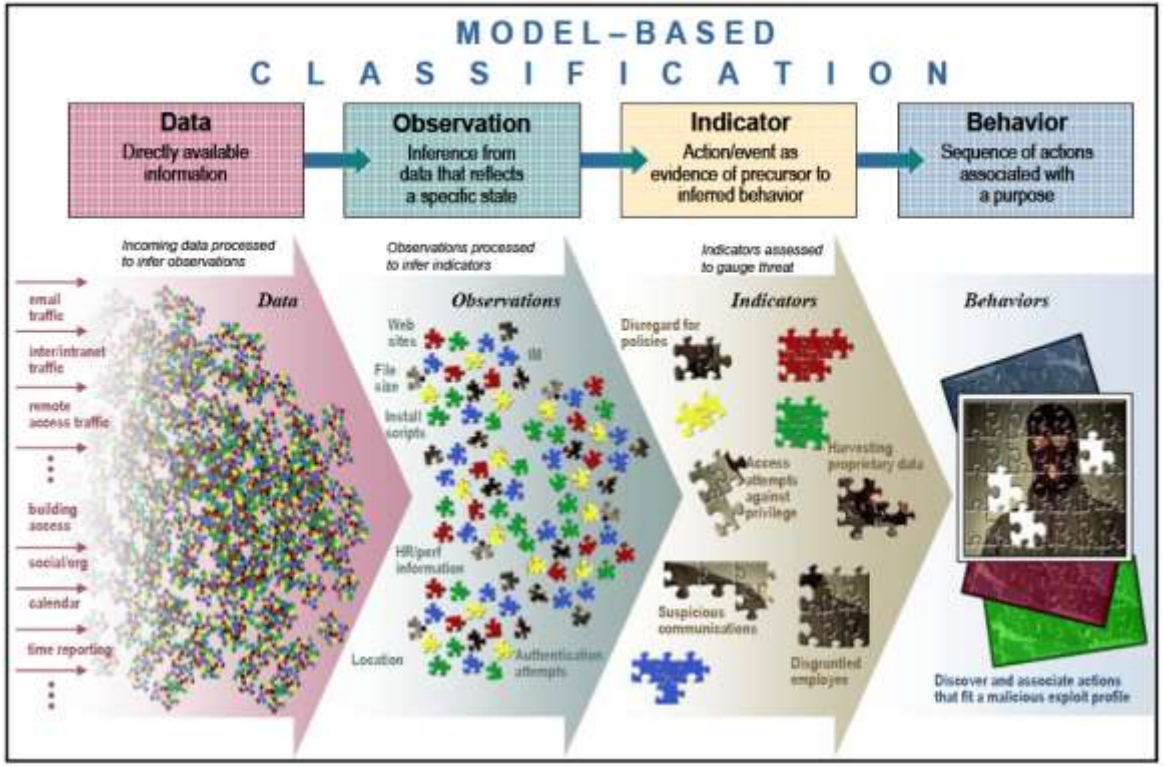
Scope of the Insider Threat



Past, Present, and Future Research



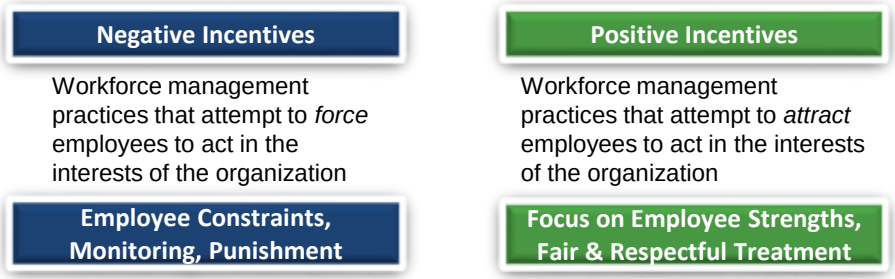
A Conceptual Model



Source: Greitzer, et al., “Predictive Modeling for Insider Threat Mitigation,” PNNL-SA-65204, April 2009.

A Balanced Approach to Insider Risk Management

Organizations typically focus their insider threat programs almost exclusively on negative incentives.



Negative incentives alone can exacerbate the threat they are intended to mitigate.*

Basic Tenet: Organizations should explicitly consider a mix of positive and negative incentives to build insider threat programs that are a net positive for employees and the organization.

* See “Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls,” SEI Digital Library, March 2015.

Research Highlights

Common Sense Guide to Mitigating Insider Threats, 6th Edition

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

Insider Risk Indicators Using Microsoft Telemetry

https://github.com/microsoft/Microsoft-threat-protection-Hunting-Queries

The Critical Role of Positive Incentives For Reducing Insider Risk

https://ieeexplore.ieee.org/abstract/document/8424655

Presenter Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu