Applying Text Analytics to Insider Threat Detection

Dan Costa

Carrie Gardner

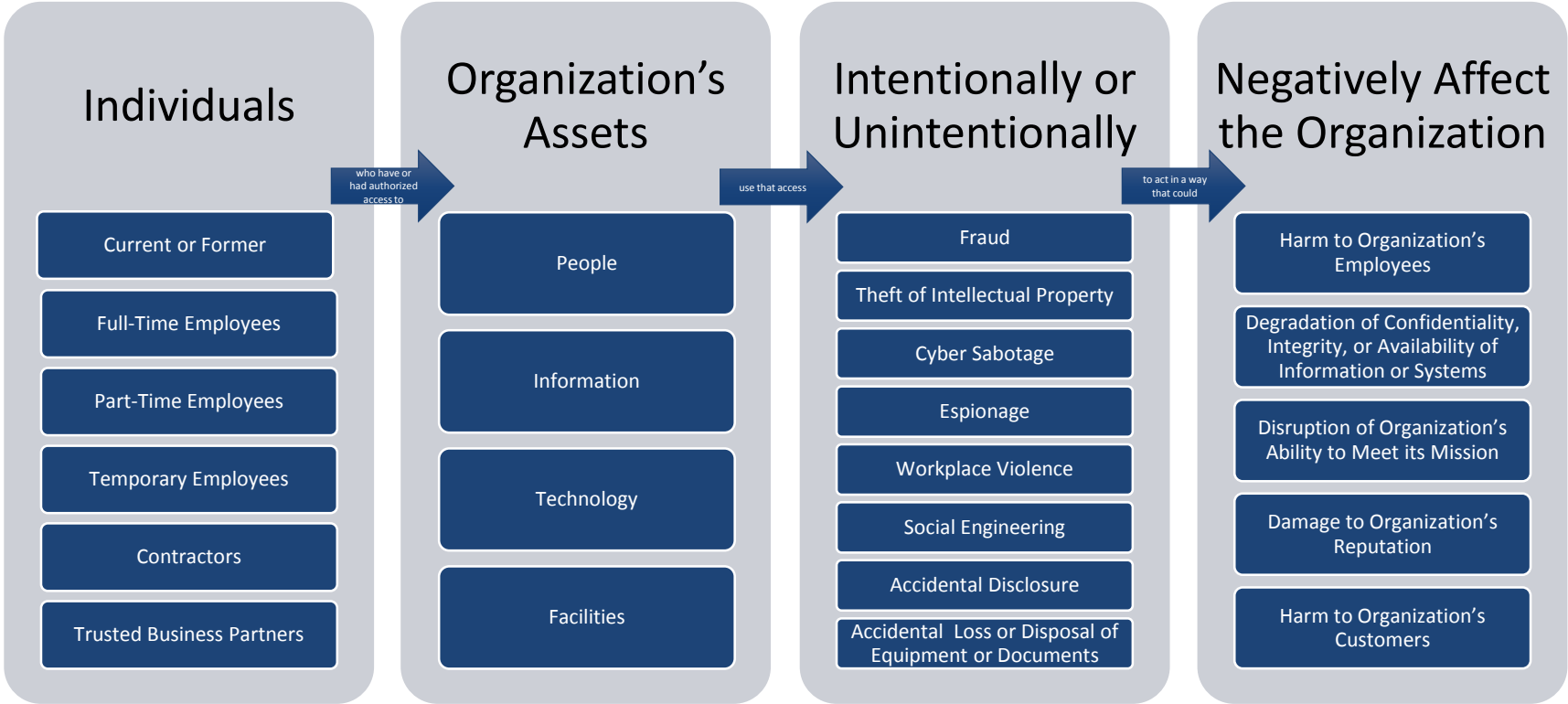
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

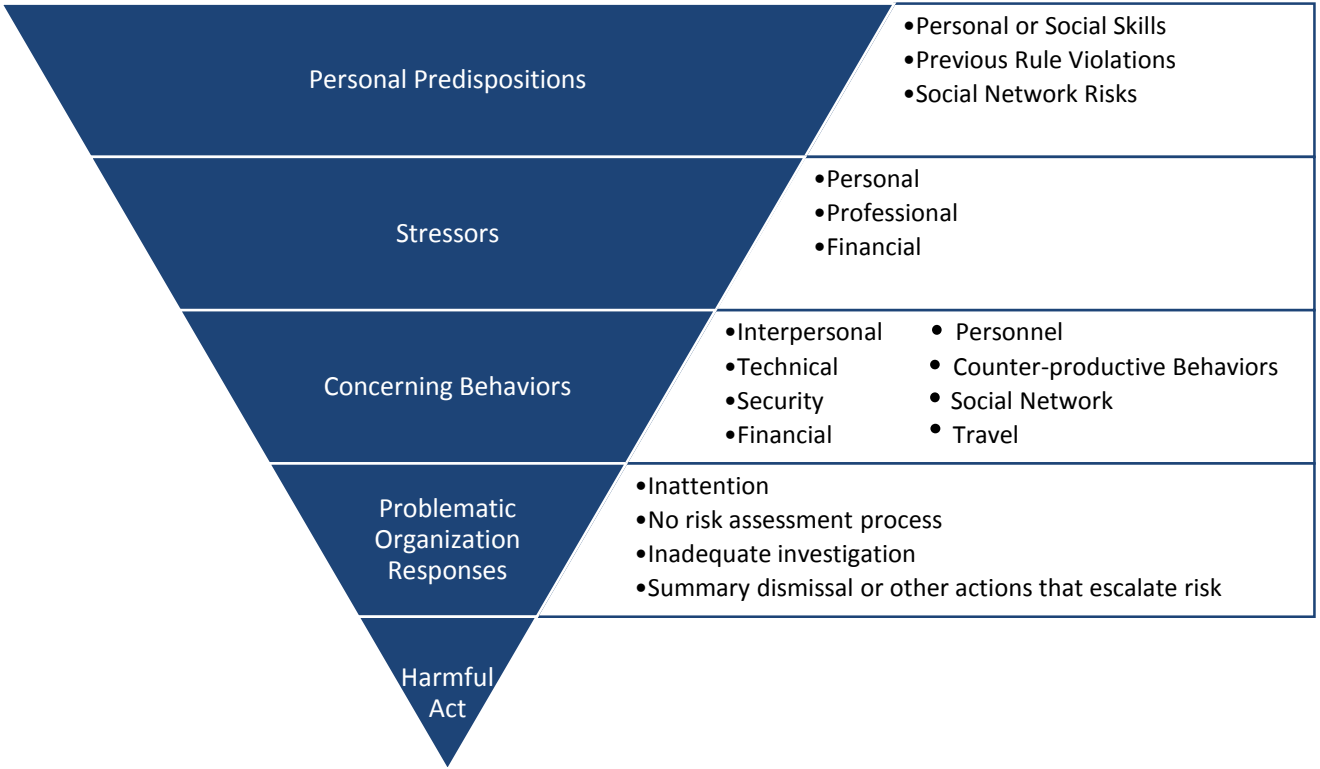
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-1182

Scope of the Insider Threat



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)

Text Analytics Tasks

Recognize Entities

Classify & Tag "Documents"

Detect Sentiment

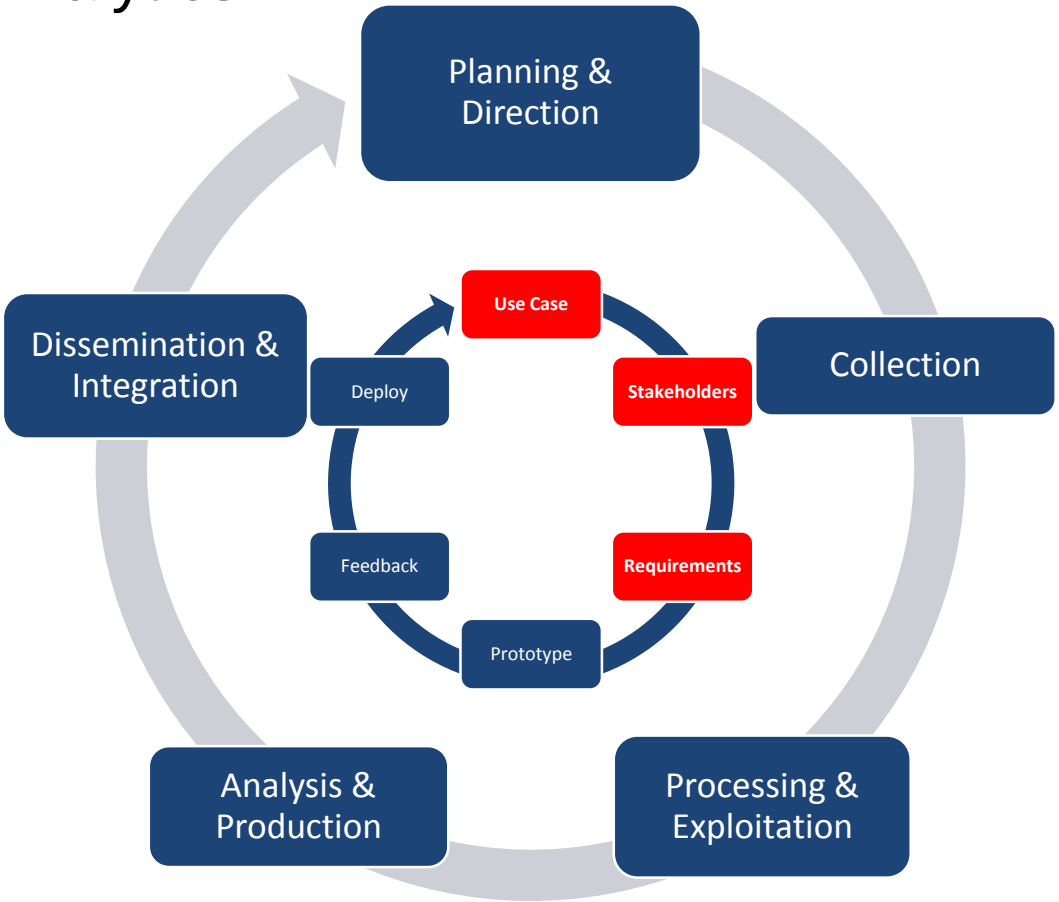
Detect Concepts

Generate Summaries

Applying Text Analytics to Insider Threat Use Cases

Use Case	Description	Advantages
Sensitive Document Tagging	Label intellectual propriety (IP), personally identifiable information (PII), or sensitive program references	• Automate process of labeling documents • Identify references to target labels that may be unmarked • Remove unnecessary references
Employee & Workforce Satisfaction/Disgruntlement	Monitor sentiment and emotion characteristics	• Observe workforce- or group wide swings • Observe individual-differences
Social Media Monitoring	Identify damaging or non-complaint statements made by employees on public forums	• Autonomously detect policy violations and potential indicators of counterproductive or insider threat activity
Event Prioritization	Label events, (anonymous) tips, or incidents with a priority classification	• Escalate and prioritize urgent or grave concerns • Filter through voluminous data

Using Text Analytics



Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

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

Carrie Gardner, CISSP, CIPP

Cybersecurity Engineer, CERT National Insider Threat Center

cgardner@sei.cmu.edu

https://insights.sei.cmu.edu/insider-threat/2018/07/considerations-for-deploying-a-text-analytics-capability-for-insider-threat-mitigation-part-1-of-3.html