Applying Text Analytics to Insider Threat Detection

Dan Costa

Carrie Gardner

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Document Markings

Copyright 2020 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

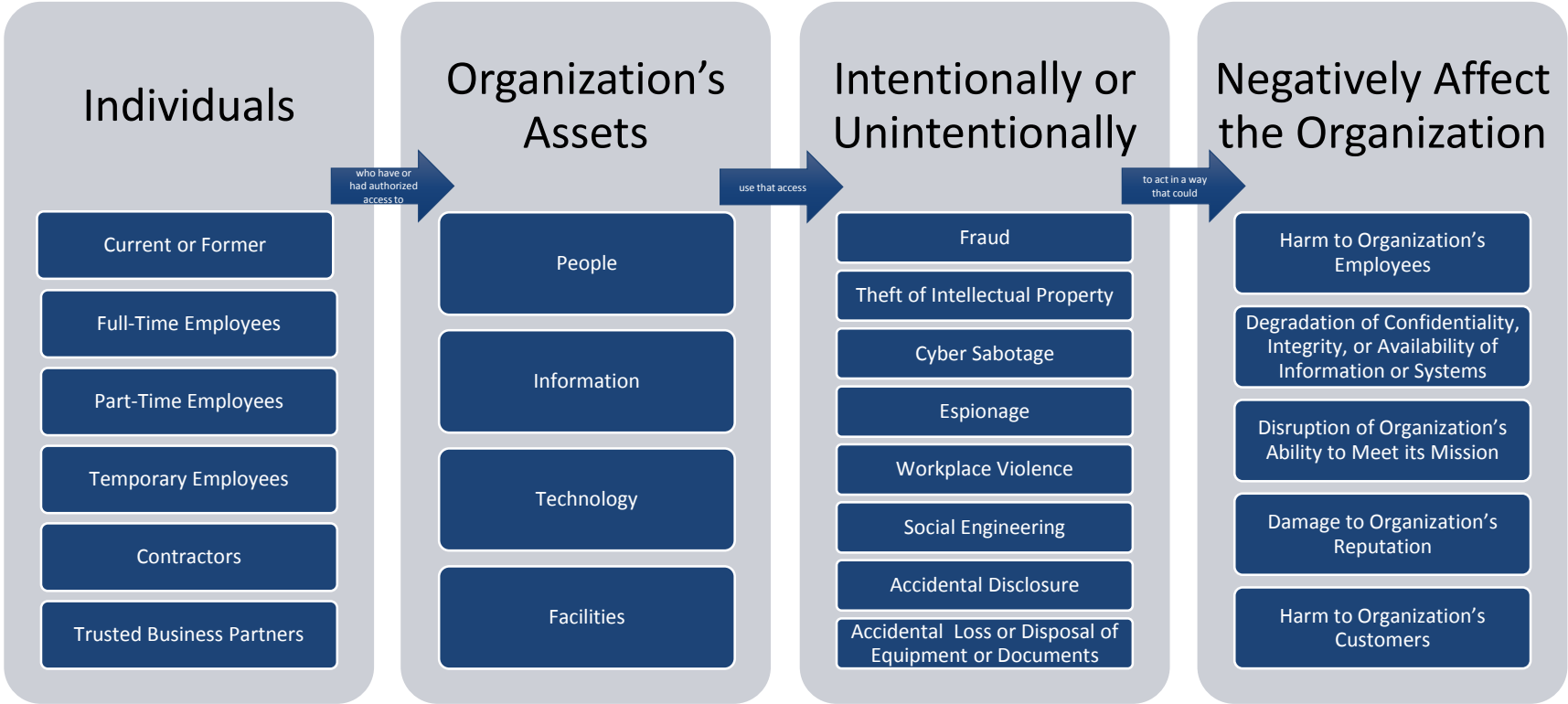
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-1182

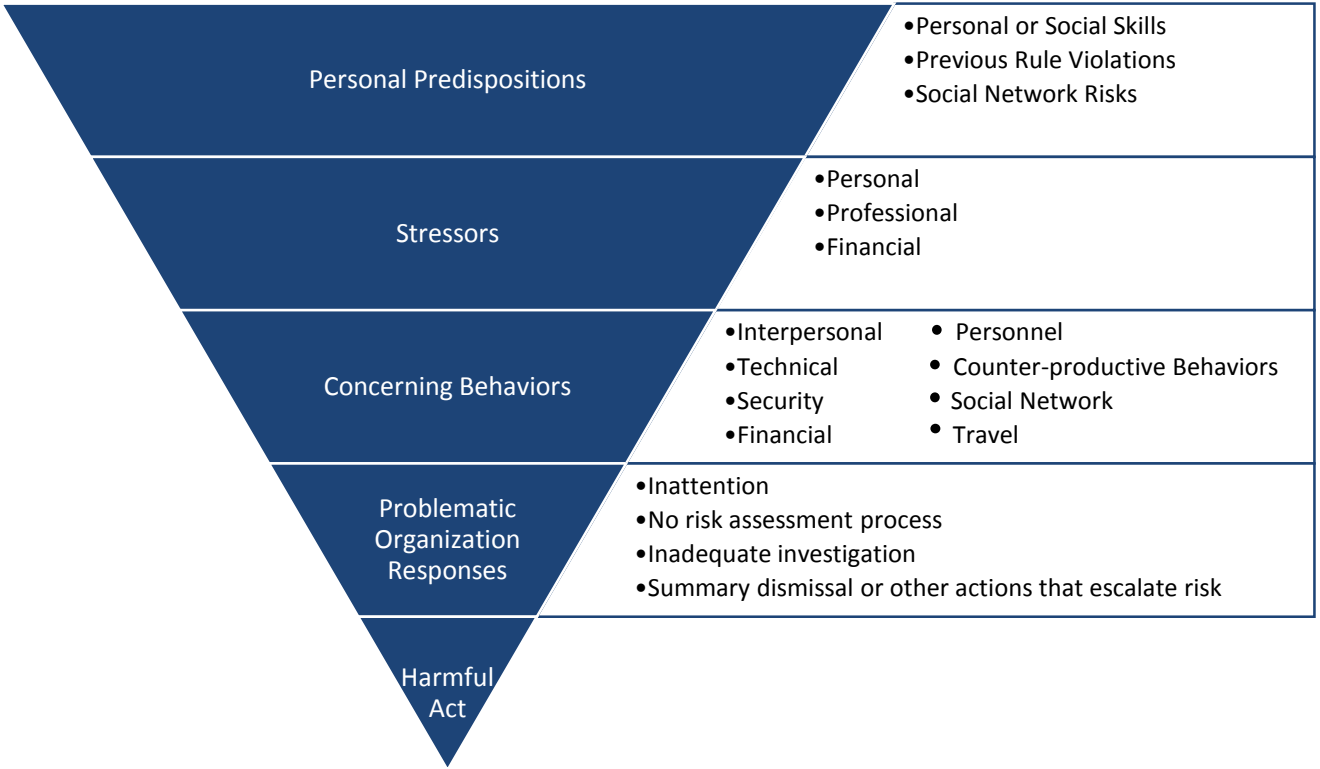
Scope of the Insider Threat



© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

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)

© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Text Analytics Tasks

Recognize Entities

Classify & Tag "Documents"

Detect Sentiment

Detect Concepts

Generate Summaries

© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

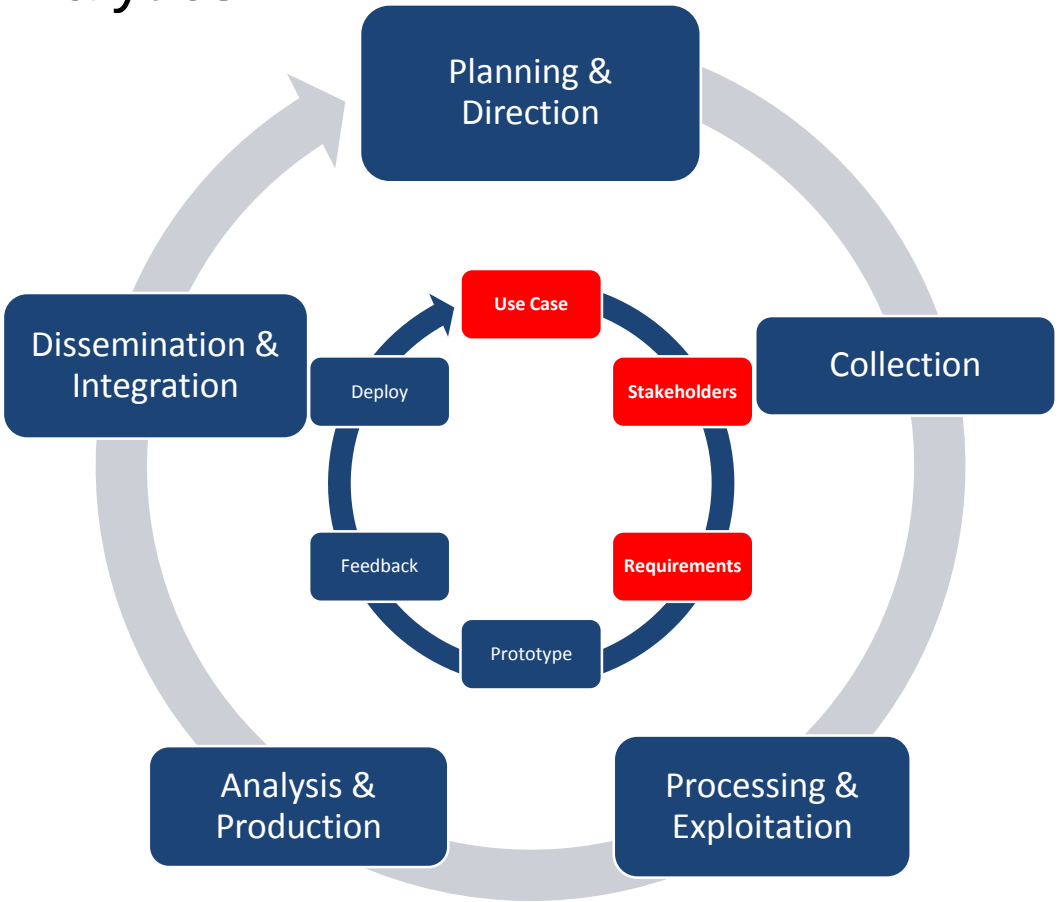
Applying Text Analytics to Insider Threat Use Cases

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

© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Using Text Analytics



© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

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

© 2020 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]