NITTF Tech Talk – Trends in Insider Risk Quantification

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.

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.

DM20-0808

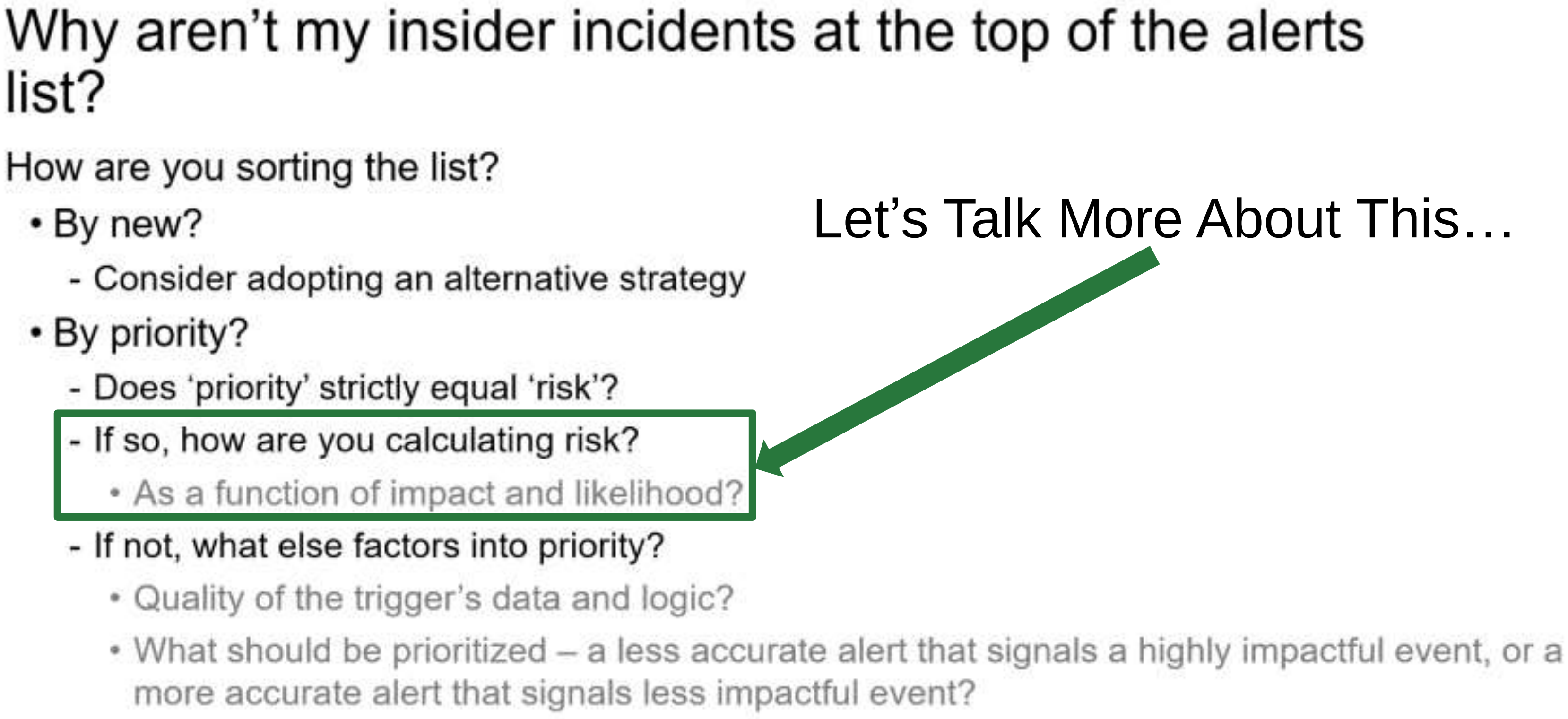
Agenda

Quantifying Insider Risk

Text Analytics for Insider Risk Managment

Quantifying Insider Risk

You May Recall From Our Last Tech Talk



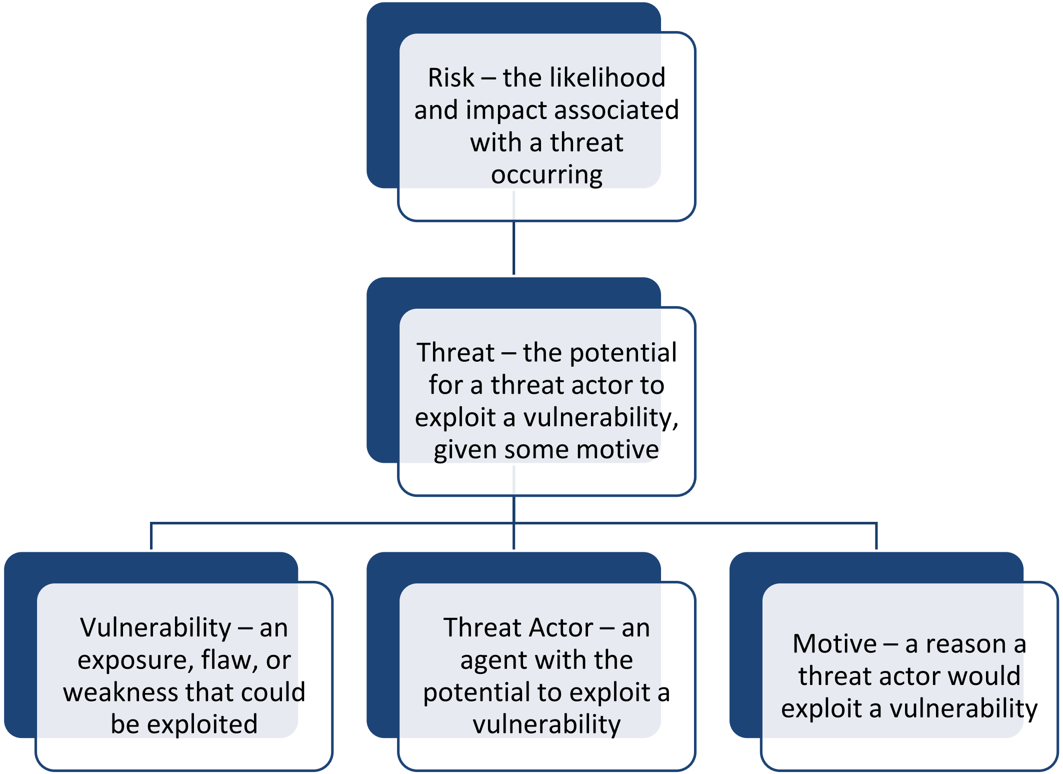
Why aren’t my insider incidents at the top of the alerts list?

How are you sorting the list?

- By new?
  - Consider adopting an alternative strategy
- By priority?
  - Does ‘priority’ strictly equal ‘risk’?
  - If so, how are you calculating risk?
    - As a function of impact and likelihood?
  - If not, what else factors into priority?
    - Quality of the trigger’s data and logic?
    - What should be prioritized – a less accurate alert that signals a highly impactful event, or a more accurate alert that signals less impactful event?

Let’s Talk More About This…

Risk Terminology



Risk – the likelihood and impact associated with a threat occurring

Threat – the potential for a threat actor to exploit a vulnerability, given some motive

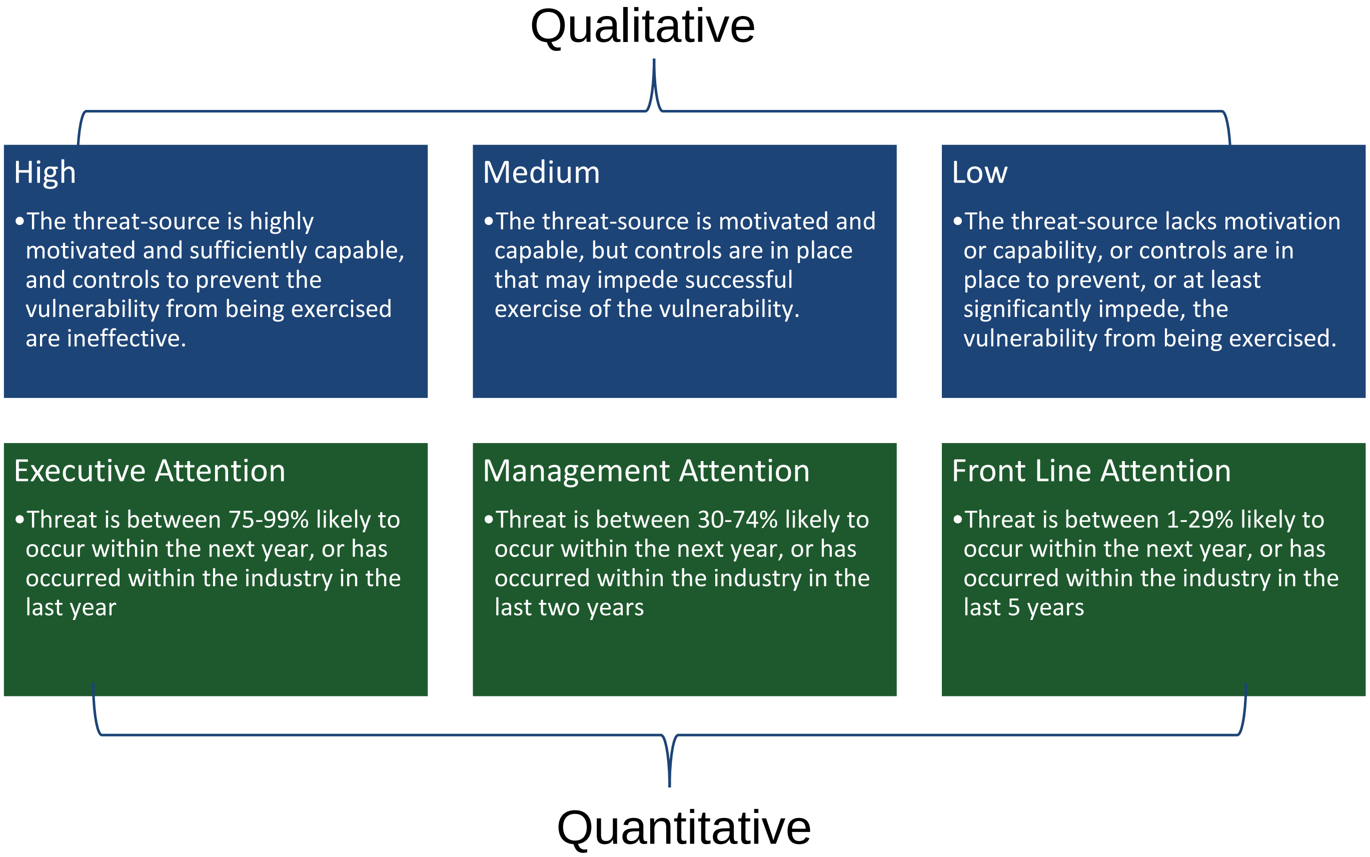
Vulnerability – an exposure, flaw, or weakness that could be exploited

Threat Actor – an agent with the potential to exploit a vulnerability

Motive – a reason a threat actor would exploit a vulnerability

Definitions adapted from the CERT® Resilience Management Model

Specifying Likelihood



Qualitative

High

- The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

Medium

- The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Low

- The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Executive Attention

- Threat is between 75-99% likely to occur within the next year, or has occurred within the industry in the last year

Management Attention

- Threat is between 30-74% likely to occur within the next year, or has occurred within the industry in the last two years

Front Line Attention

- Threat is between 1-29% likely to occur within the next year, or has occurred within the industry in the last 5 years

Quantitative

The Likelihood of What?

Probability that a user is a threat → We can, and must, do better

Probability that a specific threat scenario occurs based on a series of conditions (indicators) → Better, but how?

- Incident data – yours, and others
- Threat models
- Red-team / blue team
- Table-top exercises
- Simulation

Specifying Impact

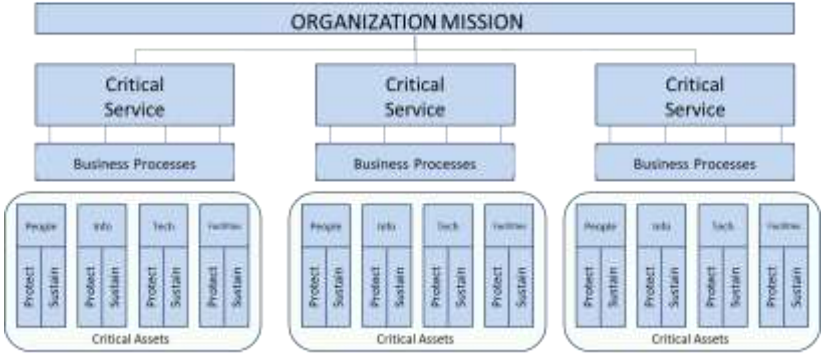
Qualitative

	Revenue (Operating Profit)	Safety	Operations	Reputation	Compliance	Human Capital	Projects
Escalate to Executive Attention	Any more than a 10% deviation from planned operating profit for a quarter	Loss of life or permanent disability	No more than three days of lost operations	Loss of market segment with multiple customers	Debarrment from a particular market segment linked to regulatory violation(s)	Any more than 5% high performer attrition from any business unit in a quarter	Liquidated damages that exceed contract value
Escalate to Management Attention	Any more than a 5% deviation from planned operating profit for a quarter	Time away or other reportable incident	No more than one day of lost operation	Loss of customer	Any fines or other penalties linked to regulatory violation(s)	Any more than 3% high performer attrition from any business unity in a quarter	Liquidated damages that erode the margin as sold
Provide Front Line Attention	Any deviations from planned operating profit for a quarter	Bumps, strains, bruises	No more than one shift of lost operation	Customer complaints or negative social media buzz	Any warnings linked to regulatory violation(s)	Any developing trend in high performer attrition	Minor disputes with limited contractual impact

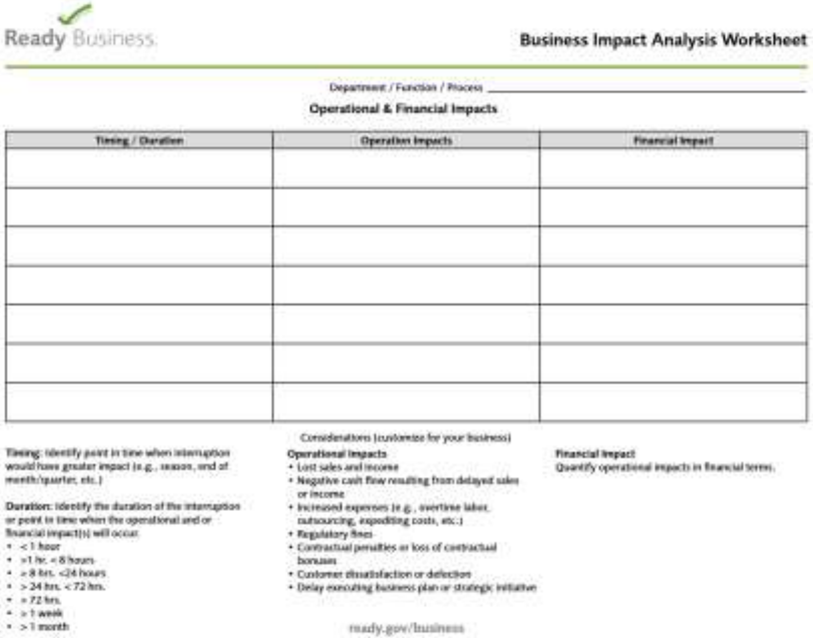
https://www.rsaconference.com/industry-topics/presentation/finding-the-right-answersfacilitating-insider-threat-analysis-using-octave

Quantitative

Business Impact Analysis



“Threats to assets”



Ready Business

Business Impact Analysis Worksheet

Department / Function / Process ____________________

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur:

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact
Quantify operational impacts in financial terms.

ready.gov/business

Questions for Those Giving Us Risk Scores

How are the algorithms trained?

- If they come pre-trained, how is that data representative of my population?
- Can I fine-tune the models with my data?

How can the models be audited?

- Are the outputs *explained* or *justified*?

How do you suggest to measure performance?

What types of intelligence can this tool provide?

- How configurable is the tool to non-standard tasks?

What KSAs are required to use/interpret the output from this tool?

- Do we need behavioral science PhDs/expertise? Data Science?

Spotlight On: Text Analytics for Insider Risk Management

Why Decision-Support Systems?

Process Speed

Process Standardization

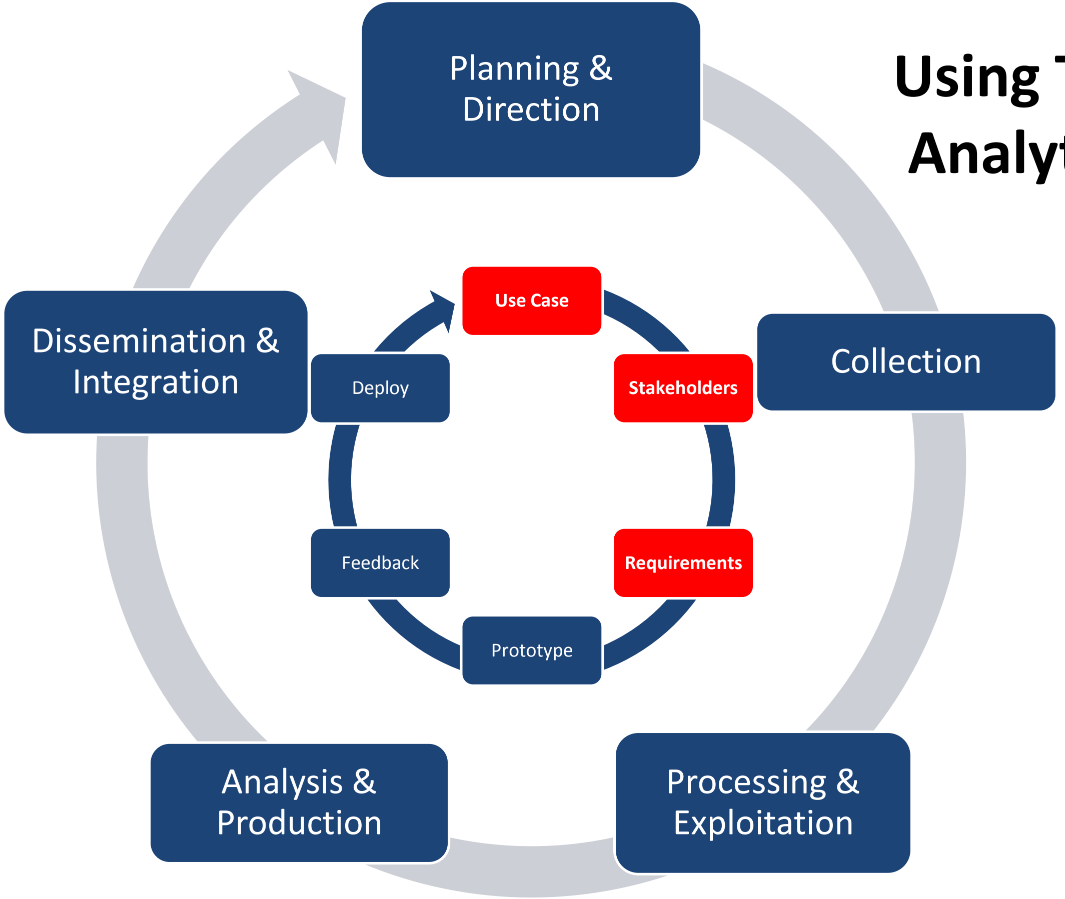
Pattern Recognition

Text Analytics

What is Text Analytics?

It is ***Intelligence***

- Context
- Meaning
- Perception
- Semantics
- Emotion
- Sentiment
- Relationships

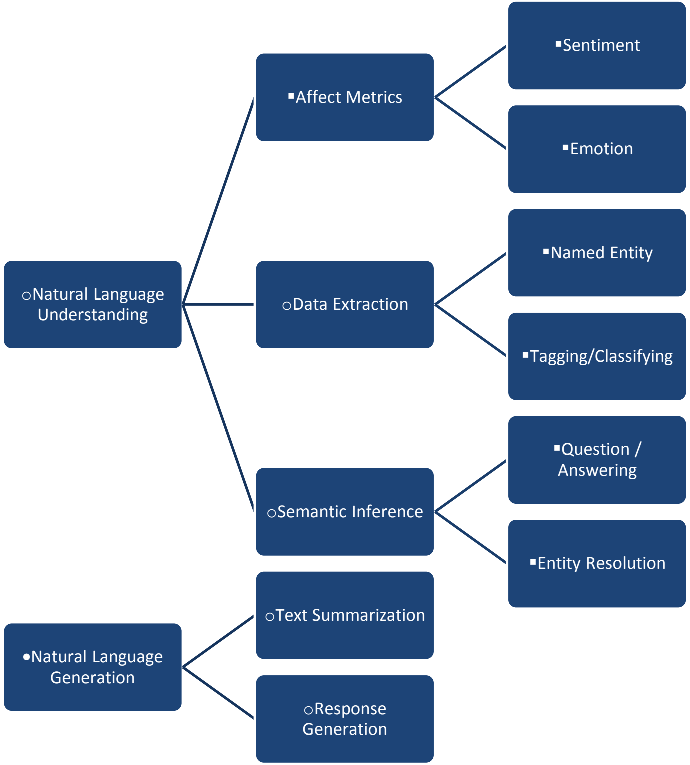


Using Text Analytics

Example Insider Threat Use Cases

- Employee Satisfaction/Disgruntlement
- Workforce Sentiment
- Anomalous Anger Detection
- Hate Speech Detection
- Codeword/Code Reference Detection
- Named Entity Tagging
- Incident Prioritization
- Incident Summarization

General Text Analytics Tasks



Defining a Use Case

Goal Statement

- “Detect anomalous and extreme negative sentiment”

Justification Statement

- “Text analytics has repeatedly shown to be effective at identifying sentiment and emotion” citation: X,Y,Z

Method Statement

- “We will use use a mixed-method approach of using LIWC and pre-trained embeddings”

Stakeholders

Identify business needs/interests of prospective stakeholders

- Talent Management/HR probably wants to increase productivity & job satisfaction
- Security/IT wants to mitigate policy violations
- Physical Security wants to prevent workplace violence

Identify shared goals

- Measure employee/workforce affect
- Detect unauthorized exfiltration of sensitive documents
- Detect threatening language

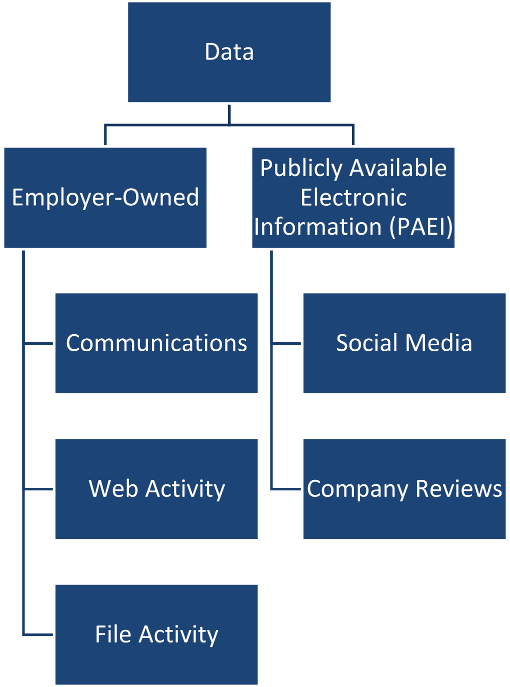
Identify data resources of prospective stakeholders

- Employer-owned communications/PAEI
- File access records

Requirements: Data Sources

Questions to Ask Legal, Privacy/Data Protection, Data Owners

- Data Usage Restrictions
- Data Protection Requirements
- Type of Data Feed
  - Push/Pull
  - Frequency
  - Volume
  - Format



Data

Employer-Owned

Publicly Available Electronic Information (PAEI)

Communications

Web Activity

File Activity

Social Media

Company Reviews

Requirements: Usage & Auditability

What do we want to be able to do with this intelligence? [Usage]

How can we measure the utility of this intelligence? [Effectiveness]

How can we verify the veracity and dependability of this intelligence? [Auditability]

Do’s and Don’ts

Do

- **Engage I/O Psychologists & Other Experts.**
- **Apply appropriate data handling protocols**
- **Apply equal treatment**
- **Audit.**
- **Know what data points cannot be collected/used.**

Don’t

- **Armchair Psychology.** Leave the clinical diagnoses to the APA licensed professionals
- **Monitor without a disclosure/consent agreement in place.**
- **Ignore council, privacy/data protection, ethics boards**
- **Ignore other internal prospective stakeholders.**

More Detailed Use Cases for Insider Threat

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

Questions / Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

Carrie Gardner, CISSP, CIPP

Cybersecurity Engineer, CERT National Insider Threat Center

cgardner@sei.cmu.edu