NITTF Tech Talk – Trends in Insider Risk Quantification, Part 2

Dan Costa

Angela Horneman

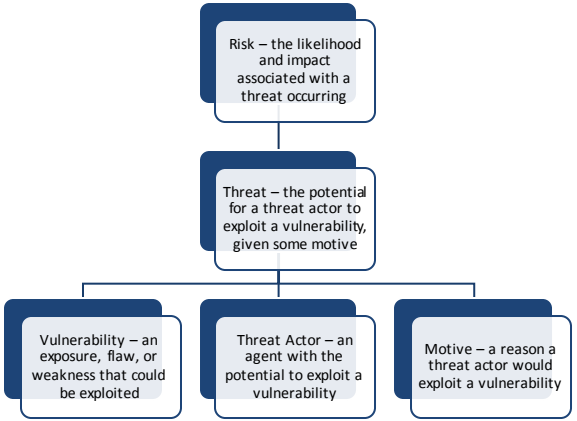
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM21-0063

From Our Last Tech Talk



- From “Mitigating Insider Threats” to “Managing Insider Risk”
- Quantifying risk involves being able to quantify the impact and likelihood associated with a threat occurring

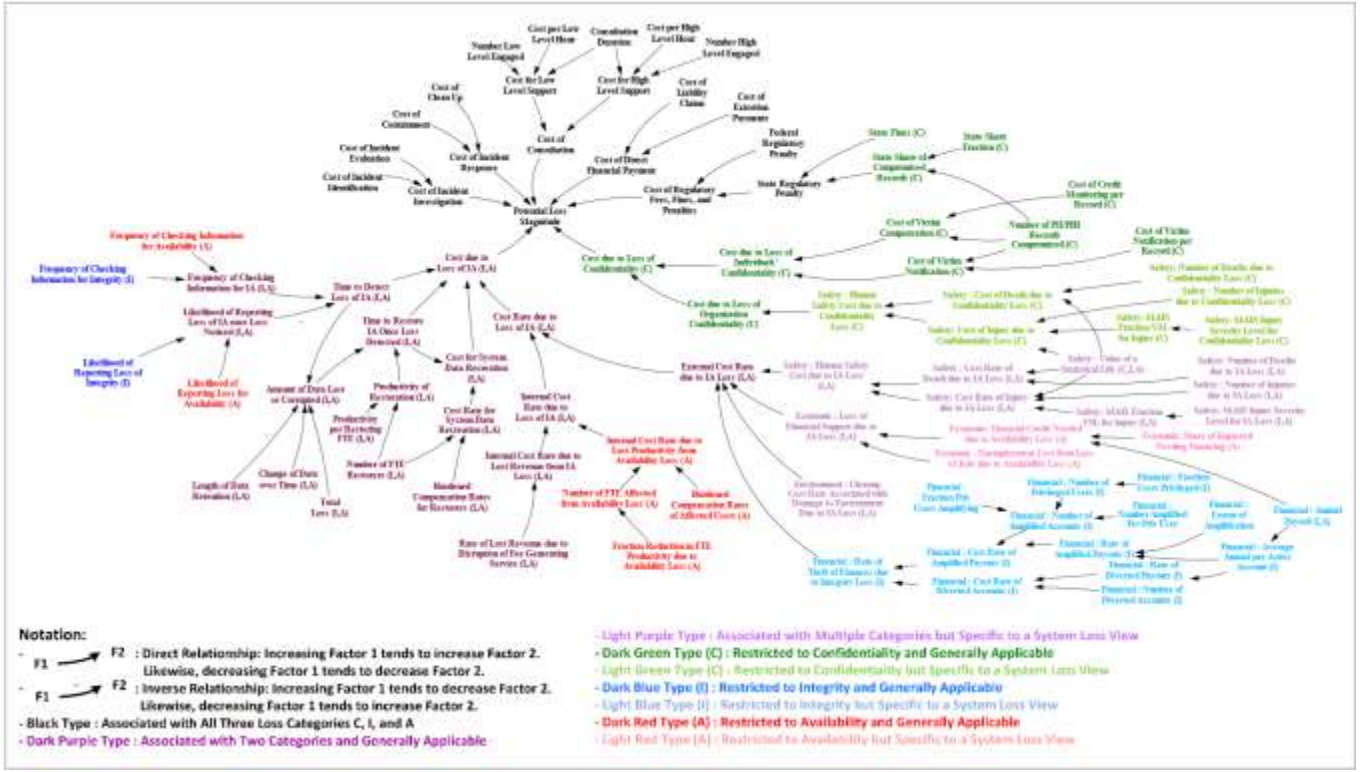
Quantifying Threat Likelihood

What can you use to measure the probability that a specific threat scenario occurs based on a series of conditions?

- Assessments / Red-team / Purple-team / Table-top exercises
- Threat models
- Simulations
- Incident and operational data

← Today's Focus

Loss Magnitude Estimation in Support of Business Impact Analysis



https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=650828

Threat Modeling

Threat Modeling Method	Features
STRIDE	+ Helps identify relevant mitigating techniques + Is the most mature + Is easy to use but is time consuming
PASTA	+ Helps identify relevant mitigating techniques + Directly contributes to risk management + Encourages collaboration among stakeholders + Contains built-in prioritization of threat mitigation + Is laborious but has rich documentation
LINDDUN	+ Helps identify relevant mitigation techniques + Contains built-in prioritization of threat mitigation + Can be labor intensive and time consuming
CVSS	+ Contains built-in prioritization of threat mitigation + Has consistent results when repeated + Has automated components + Has score calculations that are not transparent
Attack Trees	+ Helps identify relevant mitigation techniques + Has consistent results when repeated + Is easy to use if you already have a thorough understanding of the system
Persona non Grata	+ Helps identify relevant mitigation techniques + Directly contributes to risk management + Has consistent results when repeated + Tends to detect only some subsets of threats
Security Cards	+ Encourages collaboration among stakeholders + Targets out-of-the-ordinary threats + Leads to many false positives
hTMM	+ Contains built-in prioritization of threat mitigation + Encourages collaboration among stakeholders + Has consistent results when repeated
Quantitative TMM	+ Contains built-in prioritization of threat mitigation + Has automated components + Has consistent results when repeated
Trike	+ Helps identify relevant mitigation techniques + Directly contributes to risk management + Contains built-in prioritization of threat mitigation + Encourages collaboration among stakeholders + Has automated components + Has vague, insufficient documentation
VAST Modeling	+ Helps identify relevant mitigation techniques + Directly contributes to risk management + Contains built-in prioritization of threat mitigation + Encourages collaboration among stakeholders + Has consistent results when repeated + Has automated components + Is explicitly designed to be scalable + Has little publicly available documentation
OCTAVE	+ Helps identify relevant mitigation techniques + Directly contributes to risk management + Contains built-in prioritization of threat mitigation + Encourages collaboration among stakeholders + Has consistent results when repeated + Is explicitly designed to be scalable + Is time consuming and has vague documentation

https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Simulation

Analyze the effects of potential insider activity in the broader organizational context

To do this, you can use techniques such as:

- Agent-based modeling
- System dynamics modeling
- Bayesian belief networks

https://insights.sei.cmu.edu/sei_blog/2016/09/modeling-and-simulation-in-insider-threat.html

Test your technical controls in a test environment, and not in production

To do this, you'll need:

- Virtual Environments, e.g., https://github.com/cmu-sei/crucible
- User Simulation, e.g., https://github.com/cmu-sei/GHOSTS

Data – From Where and For What?

- Baseline data – 'assumed good'
- Incident data – both yours and others
  - Collect your own, here's a schema: https://insights.sei.cmu.edu/insider-threat/2011/08/the-cert-insider-threat-database.html
- Base rates of occurrence – how often do certain conditions occur in non-incidents?
  - See *Normalizing Normal: Analyzing Potential Risk Indicators of Insider Threat in the U.S. Department of Defense and Intelligence Communities* (May 2019) – Available from max.gov via the PAC PMO SSC Research Index
- Synthetic data – simulated threat activity inserted into a baseline of assumed-good activity
  - See the CERT Insider Threat Test Data Set: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099

The Insider Threat Community's Data Challenges

Not Enough

Too Much

Square Pegs, Round Holes

Apples to Oranges

Where to Next?

- Better models, more context
- Better information sharing, and information sharing tools
  - Focus on *metadata*
- More telemetry around the analysis process
- Research → Operations → Research

Q&A / Open Discussion

Presenter Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

Angela Horneman

Cybersecurity Engineer, CERT National Insider Threat Center

ahorneman@sei.cmu.edu