



# 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

Copyright 2021 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.

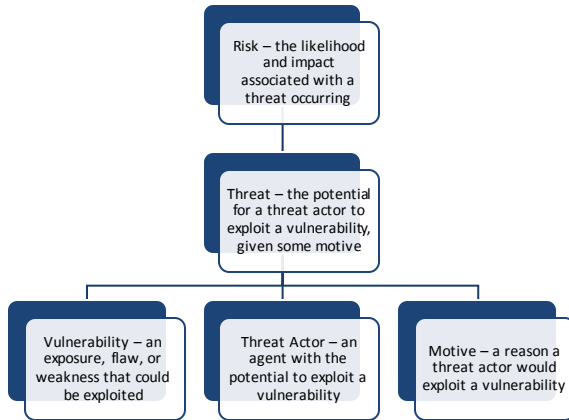
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

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

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



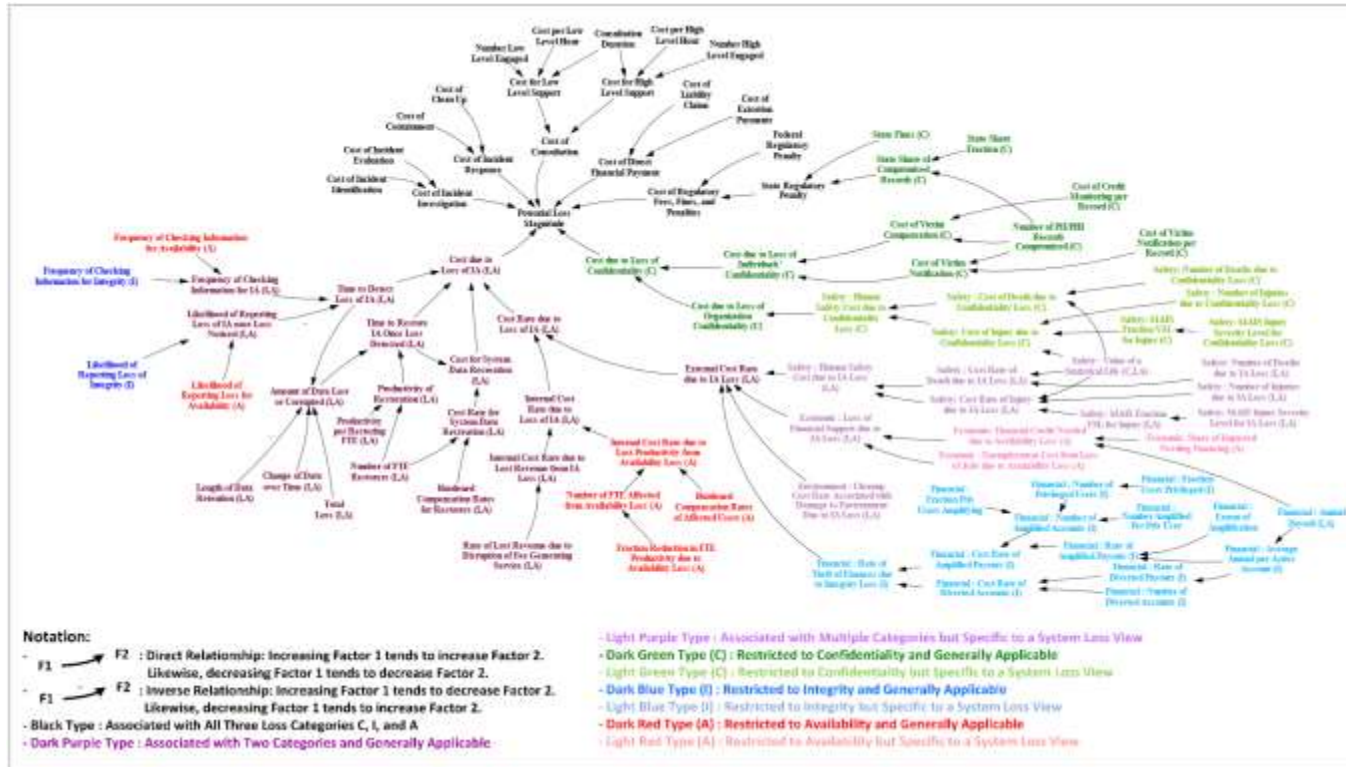
# Quantifying Threat Likelihood

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/librar/vass-et-view.cfm?assetid=650828>

# Threat Modeling

Threat Modeling Method	Features
STRIDE	<ul style="list-style-type: none"> <li>Helps identify relevant mitigating techniques</li> <li>Is the most mature</li> <li>Is easy to use but is time consuming</li> </ul>
PASTA	<ul style="list-style-type: none"> <li>Helps identify relevant mitigating techniques</li> <li>Directly contributes to risk management</li> <li>Encourages collaboration among stakeholders</li> <li>Contains built-in prioritization of threat mitigation</li> <li>Is laborious but has rich documentation</li> </ul>
LINDDUN	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Contains built-in prioritization of threat mitigation</li> <li>Can be labor intensive and time consuming</li> </ul>
CVSS	<ul style="list-style-type: none"> <li>Contains built-in prioritization of threat mitigation</li> <li>Has consistent results when repeated</li> <li>Has automated components</li> <li>Has score calculations that are not transparent</li> </ul>
Attack Trees	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Has consistent results when repeated</li> <li>Is easy to use if you already have a thorough understanding of the system</li> </ul>
Persona non Grata	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Directly contributes to risk management</li> <li>Has consistent results when repeated</li> <li>Tends to detect only some subsets of threats</li> </ul>
Security Cards	<ul style="list-style-type: none"> <li>Encourages collaboration among stakeholders</li> <li>Targets out-of-the-ordinary threats</li> <li>Leads to many false positives</li> </ul>
hTMM	<ul style="list-style-type: none"> <li>Contains built-in prioritization of threat mitigation</li> <li>Encourages collaboration among stakeholders</li> <li>Has consistent results when repeated</li> </ul>
Quantitative TMM	<ul style="list-style-type: none"> <li>Contains built-in prioritization of threat mitigation</li> <li>Has automated components</li> <li>Has consistent results when repeated</li> </ul>
Trike	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Directly contributes to risk management</li> <li>Contains built-in prioritization of threat mitigation</li> <li>Encourages collaboration among stakeholders</li> <li>Has automated components</li> <li>Has vague, insufficient documentation</li> </ul>
VAST Modeling	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Directly contributes to risk management</li> <li>Contains built-in prioritization of threat mitigation</li> <li>Encourages collaboration among stakeholders</li> <li>Has consistent results when repeated</li> <li>Has automated components</li> <li>Is explicitly designed to be scalable</li> <li>Has little publicly available documentation</li> </ul>
OCTAVE	<ul style="list-style-type: none"> <li>Helps identify relevant mitigation techniques</li> <li>Directly contributes to risk management</li> <li>Contains built-in prioritization of threat mitigation</li> <li>Encourages collaboration among stakeholders</li> <li>Has consistent results when repeated</li> <li>Is explicitly designed to be scalable</li> <li>Is time consuming and has vague documentation</li> </ul>

[https://insights.sei.cmu.edu/sei\\_blog/2018/12/threat-modeling-12-available-methods.html](https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html)

As a mechanical engineer, Marvin developed a new design for an implantable cardioverter-defibrillator (ICD) that he planned to patent. However, the MedsRUs Company beat him to the punch and filed a patent for a similar design. MedsRUs is now getting rich and Marvin is feeling cheated and angry at his lost opportunity.

Recently divorced, and without the funds to support the lifestyle he dreamed of, he has become increasingly bitter about his perceived loss.

**Marvin's Misuse Cases that Threaten Correct Operation of the ICD**

1. Sniff on the data transmitted along the serial cable between the ICDs' reprogramming equipment and communication device in order to retrieve the patient's name, ID, and basic medical history that is all stored in the ICD.
2. Transmit commands to replace the patient's personal information in the ICD.
3. Transmit commands to shut off the device's ability to respond to cardiac events.
4. Transmit commands to switch to test mode so that a carefully timed current triggers an arrhythmic test event that could stop the heart entirely.

**Goals:**

- To undermine the reputation of MedsRUs by disrupting the ICD behavior of random ICD users on the street.
- To accomplish the attack without detection.
- To cause discomfort to ICD users without killing them.

**Skills:**

- Strong code/hacking skills
- Mechanical engineering/device building skills

**Marvin**  
Mechanical Engineer  
Bitter and revengeful

# 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](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](mailto:dlcosta@sei.cmu.edu)

Angela Horneman

Cybersecurity Engineer, CERT National Insider Threat Center

[ahorneman@sei.cmu.edu](mailto:ahorneman@sei.cmu.edu)