Finding the Right Answers—Facilitating Insider Threat Analysis Using OCTAVE FORTE

Brett Tucker
Technical Manager, Cyber Risk
Software Engineering Institute/CERT
batucker@cert.org

Randy Trzeciak
Director, National Insider Threat Center
Software Engineering Institute/CERT
rft@cert.org
• Copyright 2019 Carnegie Mellon University. All Rights Reserved.

• 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.

• 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.

• OCTAVE® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

• DM19-0139
<table>
<thead>
<tr>
<th>Law Enforcement Employee</th>
<th>Disgruntled Former Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performed Unauthorized Queries in Database; Provided Sensitive Information to Domestic and International Acquaintances</td>
<td>Compromised Supervisor Credentials to Read Email, View Employee Reviews, Steal IP, and Post Data to Social Media Site(s)</td>
</tr>
</tbody>
</table>

- VP of Technology Company Transferred
- >$19M from Organization to Personal Accounts; Created False Reimbursement Documents for Health Insurance Plan
Assessing Insider Threat with OCTAVE FORTE

All attendees will walk away with a greater appreciation for risk:

Educate + Learn = Apply

- We will apply OCTAVE FORTE process to an Insider Threat Risk
- You will actively participate with your own organizational challenges
- You will gain practical ideas to manage risk and be educated on insider threat

Bottom Line: Insider Threat is a critical risk that can be included in most enterprise risk portfolios
In a World of Great Uncertainty
What is Certain?

- Risk environment will not contract – number of risks and complexity will increase

- Organizations must get better at “surviving” uncertainty

- **Knowledge and awareness of risk issues** must be pervasive throughout the organization

- Traditional tools, techniques, and methods may not work and will need to evolve

- Organizations must be **agile** enough to adapt
OCTAVE’s Evolution => FORTE
Accounts for Several Standards to Incorporate

- Leverages many standard principles and best practices
- Facilitated – Getting Organizational Input
- Operational – Real Time Applicability
- Risk – Establishing a Process to Assess
- Tailored – Flexible for All Organizations
- Enterprise – Application at All Levels
Use Case for an Organization...

No Two Organizations are the Same

- Suppose you belong to a private, mid-sized company that consults for various industry sectors with sensitive information.
Where to begin...

STEP 1: Establish Risk Governance and Appetite
STEP 2: Scope Critical Services & Assets
STEP 3: Identify Resilience Requirements of Assets
STEP 4: Measure Current Capabilities
STEP 5: Identify Risks, Threats, & Vulnerabilities to Assets
STEP 6: Analyze Risks Against Capabilities
STEP 7: Plan for Improvement
STEP 8: Implement Improvement Plan
STEP 9: Monitor & Measure Effectiveness
STEP 10: Review, Update, & Repeat

Think Marathon, NOT Sprint
### Most Critical Item to Get Started from Step 1…

**Risk Appetite that is Quantitative and Functional**

<table>
<thead>
<tr>
<th>Escalate to Executive Attention</th>
<th>Escalate to Management Attention</th>
<th>Provide Front Line Attention</th>
<th>Revenue (Operating Profit)</th>
<th>Safety</th>
<th>Operations</th>
<th>Reputation</th>
<th>Compliance</th>
<th>Human Capital</th>
<th>Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any more than a 10% deviation from planned operating profit for a quarter</td>
<td>Any more than a 5% deviation from planned operating profit for a quarter</td>
<td>Any deviations from planned operating profit for a quarter</td>
<td>Loss of life or permanent disability</td>
<td>Loss of life or permanent disability</td>
<td>Loss of life or permanent disability</td>
<td>Loss of life or permanent disability</td>
<td>Debarment from a particular market segment linked to regulatory violation(s)</td>
<td>Any more than 5% high performer attrition from any business unit in a quarter</td>
<td>Liquidated damages that exceed contract value</td>
</tr>
<tr>
<td>Time away or other reportable incident</td>
<td>No more than one day of lost operation</td>
<td>No more than one shift of lost operation</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Any warnings linked to regulatory violation(s)</td>
<td>Any developing trend in high performer attrition</td>
<td>Liquidated damages that erode the margin as sold</td>
</tr>
<tr>
<td>Bumps, strains, bruises</td>
<td>No more than one shift of lost operation</td>
<td>No more than one shift of lost operation</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Customer complaints or negative social media buzz</td>
<td>Any warnings linked to regulatory violation(s)</td>
<td>Any developing trend in high performer attrition</td>
<td>Liquidated damages that erode the margin as sold</td>
</tr>
</tbody>
</table>

### Appetite May Also be Characterized by Likelihood, Adaptability, and Others

- **Revenue (Operating Profit)**
  - Escalate to Executive Attention: Any more than a 10% deviation from planned operating profit for a quarter
  - Escalate to Management Attention: Any more than a 5% deviation from planned operating profit for a quarter
  - Provide Front Line Attention: Any deviations from planned operating profit for a quarter

- **Safety**
  - Escalate to Executive Attention: Loss of life or permanent disability
  - Escalate to Management Attention: Loss of life or permanent disability
  - Provide Front Line Attention: Loss of life or permanent disability

- **Operations**
  - Escalate to Executive Attention: No more than three days of lost operations
  - Escalate to Management Attention: No more than one day of lost operation
  - Provide Front Line Attention: No more than one shift of lost operation

- **Reputation**
  - Escalate to Executive Attention: Loss of market segment with multiple customers
  - Escalate to Management Attention: Loss of customer
  - Provide Front Line Attention: Customer complaints or negative social media buzz

- **Compliance**
  - Escalate to Executive Attention: Debarment from a particular market segment linked to regulatory violation(s)
  - Escalate to Management Attention: Any fines or other penalties linked to regulatory violation(s)
  - Provide Front Line Attention: Any warnings linked to regulatory violation(s)

- **Human Capital**
  - Escalate to Executive Attention: Any more than 5% high performer attrition from any business unit in a quarter
  - Escalate to Management Attention: Any more than 3% high performer attrition from any business unit in a quarter
  - Provide Front Line Attention: Any developing trend in high performer attrition

- **Projects**
  - Escalate to Executive Attention: Liquidated damages that exceed contract value
  - Escalate to Management Attention: Liquidated damages that erode the margin as sold
  - Provide Front Line Attention: Minor disputes with limited contractual impact

---

**Carnegie Mellon University**
Software Engineering Institute
Compressing Effort for Time...

High Value Asset: People, Information, Technology, or Facilities of which a High Value Service is Dependent.

STEP 1: Establish Risk Governance and Appetite
STEP 2: Scope Critical Services & Assets
STEP 3: Identify Resilience Requirements of Assets
STEP 4: Measure Current Capabilities
STEP 5: Identify Risks, Threats, & Vulnerabilities to Assets
STEP 6: Analyze Risks Against Capabilities
STEP 7: Plan for Improvement
STEP 8: Implement Improvement Plan
STEP 9: Monitor & Measure Effectiveness
STEP 10: Review, Update, & Repeat

Assume Steps 2-4 are Completed

Carnegie Mellon University
Software Engineering Institute

RSA Conference 2019
Summary of Results from Steps 2-4
Asset Management and Requirements

- People, information, technology, facilities, and external providers are documented
- Their contributions to business objectives are understood
- Ownership determination is critical
Linking Asset Disruptions to Strategic Objectives

Crossroads of Strategy, Risk, and Operations

STEP 1: Establish Risk Governance and Appetite
STEP 2: Scope Critical Services & Assets
STEP 3: Identify Resilience Requirements of Assets
STEP 4: Measure Current Capabilities
STEP 5: Identify Risks, Threats, & Vulnerabilities to Assets
STEP 6: Analyze Risks Against Capabilities
STEP 7: Plan for Improvement
STEP 8: Implement Improvement Plan
STEP 9: Monitor & Measure Effectiveness
STEP 10: Review, Update, & Repeat

Thinking about that day that may never come...

What could possibly go wrong?

Carnegie Mellon University
Software Engineering Institute
Information Security Risk Management

Risk = Probability (Threat exploits Vulnerability causing Unwanted Outcome)

Threat = External, Internal, Human, Non-Human, Malicious, Non-Malicious
Insider Threat Mitigation

**Insider Incident**
- Prevent / Detect
- if detected
- Respond / Recover

**Insider Threat**
- Identify / Deter
- if detected
- Consistent Response

**Insiders**
- Not Alienate

Carnegie Mellon University
Software Engineering Institute

RSA Conference 2019
CERT’s Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
Insider Threat to Critical Assets

Individuals
- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

Organization’s Assets
- People
- Information
- Technology
- Facilities

Intentionally or Unintentionally
- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental Loss or Disposal of Equipment or Documents

Negatively Affect the Organization
- Harm to Organization’s Employees
- Degradation to CIA of Information or Information Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers
The Insider Threat

There are no insider threats that can be characterized as “one type”

Remember that the organization’s critical assets include:

• People
• Information
• Technology
• Facilities

Insider threat can be based on the motive(s) of the insider

Impacts to Confidentiality, Integrity, and Availability are possible

Cyber Attack = Cyber Impact
Physical Attack = Physical Impact
Cyber Attack = Physical Impact
Physical Attack = Cyber Impact
Examples of Insider Incidents

National Security Espionage

IT System Sabotage

Theft of IP – Entitled Independent

Espionage / Sabotage

Fraud

Theft of IP – Ambitious Leader

Carnegie Mellon University
Software Engineering Institute
Insider Threat Observables

The CERT National Insider Threat Center has amassed a repository of over 2500 Insider incidents (over 18 years).

Potential Insider Threat Risk Indicators (not a complete list)
Qualifying the Insider Threat

Operations: Insider Driven Disruption

Scope Statement: If the organization suffers a major interruption in operations or impairment from an internal actor, then mission and lives could be jeopardized. Opportunistically, if all malign insider action is avoided, then resources could be saved, reputation could elevate, and mission success could improve.

Risk Triggers and Key Risk Indicators (KRIs)

- Layoff(s) for portions of the workforce
- Poor Org Performance
- Policy Changes
- Reduction of benefits
- Toxic work environment and/or culture
- Low Employee Morale
- Employee Complaints

Conditions for Risk Realization
- Could happen during any operational environment
- Most likely to occur with poor corporate performance

Consequences
- Additional costs
- Delayed mission schedule
- Loss of intellectual property
- Loss of information
- Reputational damage
- Loss of confidentiality, integrity, or access
Developing an Appropriate Response

STEP 1: Establish Risk Governance and Appetite

STEP 2: Scope Critical Services & Assets

STEP 3: Identify Resilience Requirements of Assets

STEP 4: Measure Current Capabilities

STEP 5: Identify Risks, Threats, & Vulnerabilities to Assets

STEP 6: Analyze Risks Against Capabilities

STEP 7: Plan for Improvement

STEP 8: Implement Improvement Plan

STEP 9: Monitor & Measure Effectiveness

STEP 10: Review, Update, & Repeat

Time to make some changes

Take Control
Insider Threat Tools Vary in Features and Functions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing Host-based Activity</td>
<td>Preventing Data from Leaving Authorized Locations</td>
</tr>
<tr>
<td>Auditing Network-based Activity</td>
<td>Rule-Based Alerting</td>
</tr>
<tr>
<td>Preserving Forensic Artifacts</td>
<td>Data Visualization</td>
</tr>
<tr>
<td>Identity Management / Access Management</td>
<td>Data Correlation / Entity Resolution</td>
</tr>
<tr>
<td>Machine Learning</td>
<td>Anomaly Detection</td>
</tr>
<tr>
<td>Case / Incident Management</td>
<td>Risk Scoring</td>
</tr>
<tr>
<td></td>
<td>Data Masking / Anonymization</td>
</tr>
<tr>
<td></td>
<td>... And More ...</td>
</tr>
</tbody>
</table>
Insider Threat Tools Vary in Features and Functions

- Prevent: Stop something from happening
  - Example: Block a sensitive document from being moved to removable media

- Detect: Figure out that something is happening (or about to happen)
  - Example: Alert security staff of (suspicious?) file activity

- Deter: Discourage something from happening
  - Example: Present a dialog that requires a user to acknowledge the organization’s removable media policy

- Respond: Address something that happened
  - Example: Restore missing data from backups

Carnegie Mellon University
Software Engineering Institute

#RSAC
RSACConference2019
Mitigation Plans to Consider

1. Identify insider threats to critical Assets
2. Establish an insider threat control baseline
3. Fill critical gaps in control baseline
4. Measure effectiveness of insider threat controls
5. Refine and refresh insider threat controls

PROCESS + TOOLS = RESILIENCE

Carnegie Mellon University
Software Engineering Institute
Apply What You Have Learned Today

• **Next week you should:**
  – Determine the what risk processes are used in your organization
  – Identify ownership and state of insider threat management

• **In the first three months following this presentation you should:**
  – Understand how risks are managed and who is managing the program
  – Apply existing risk management process to insider threat as a use case

• **Within six months you should:**
  – Devise response plans to mitigate insider threat and build a business case for necessary resources
  – Begin implementation of plan to seek quick wins
Resources and References

- Introduction to OCTAVE Allegro: [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419)
- Podcast for OCTAVE Allegro: [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34702](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34702)
- OCTAVE Version 1.0: [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473)
- OCTAVE for Smaller Organizations: [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795)
- COSO Direction on Implementing a Cyber Risk Management Framework: [https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf](https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf)
- ISACA – COBIT 5 Risk Framework: [http://www.isaca.org/COBIT/Pages/default.aspx](http://www.isaca.org/COBIT/Pages/default.aspx)
Any Questions?

Brett Tucker
Telephone: 412.268.6682  
Email: batucker@cert.org

Randy Trzeciak
Telephone: 412.268.7040  
Email: rft@cert.org