RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-T08

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

- 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.

- DM19-0139

Can This Happen to Your Organization?

Law Enforcement Employee Performed Unauthorized Queries in Database; Provided Sensitive Information to Domestic and International Acquaintances

Disgruntled Former Employee Compromised Supervisor Credentials to Read Email, View Employee Reviews, Steal IP, and Post Data to Social Media Site(s)

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?

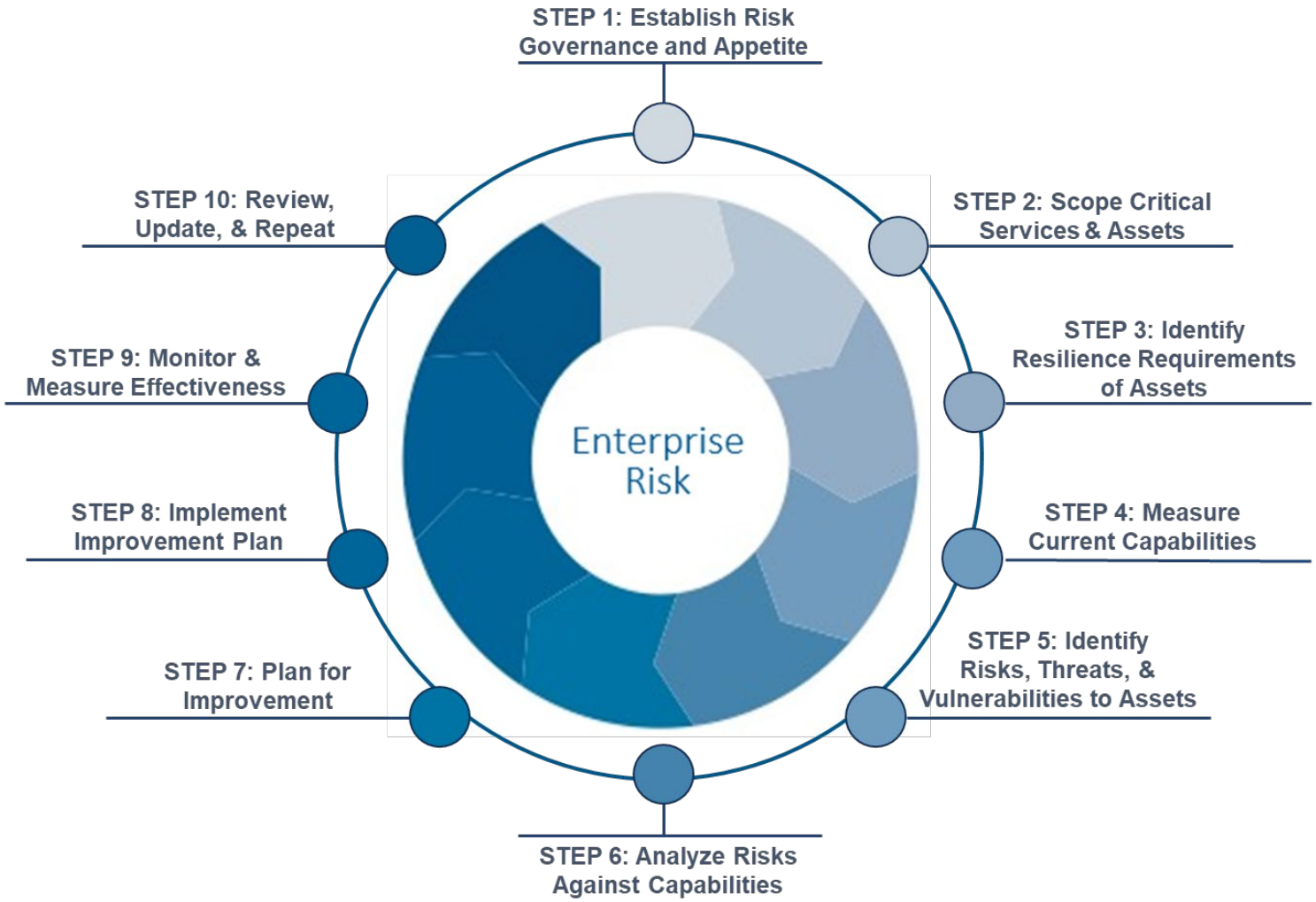
- Risk environment will not contract – number of risks and **complexity will increase**
- Organizations must get better at "**surviving**" uncertainty
- **Knowledge and awareness of risk issues** must be pervasive throughout the organization
- Traditional tools, techniques, and methods may not work and 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

- **F**acilitated – Getting Organizational Input
- **O**perational – Real Time Applicability
- **R**isk – Establishing a Process to Assess
- **T**ailored – Flexible for All Organizations
- **E**nterprise – Application at All Levels

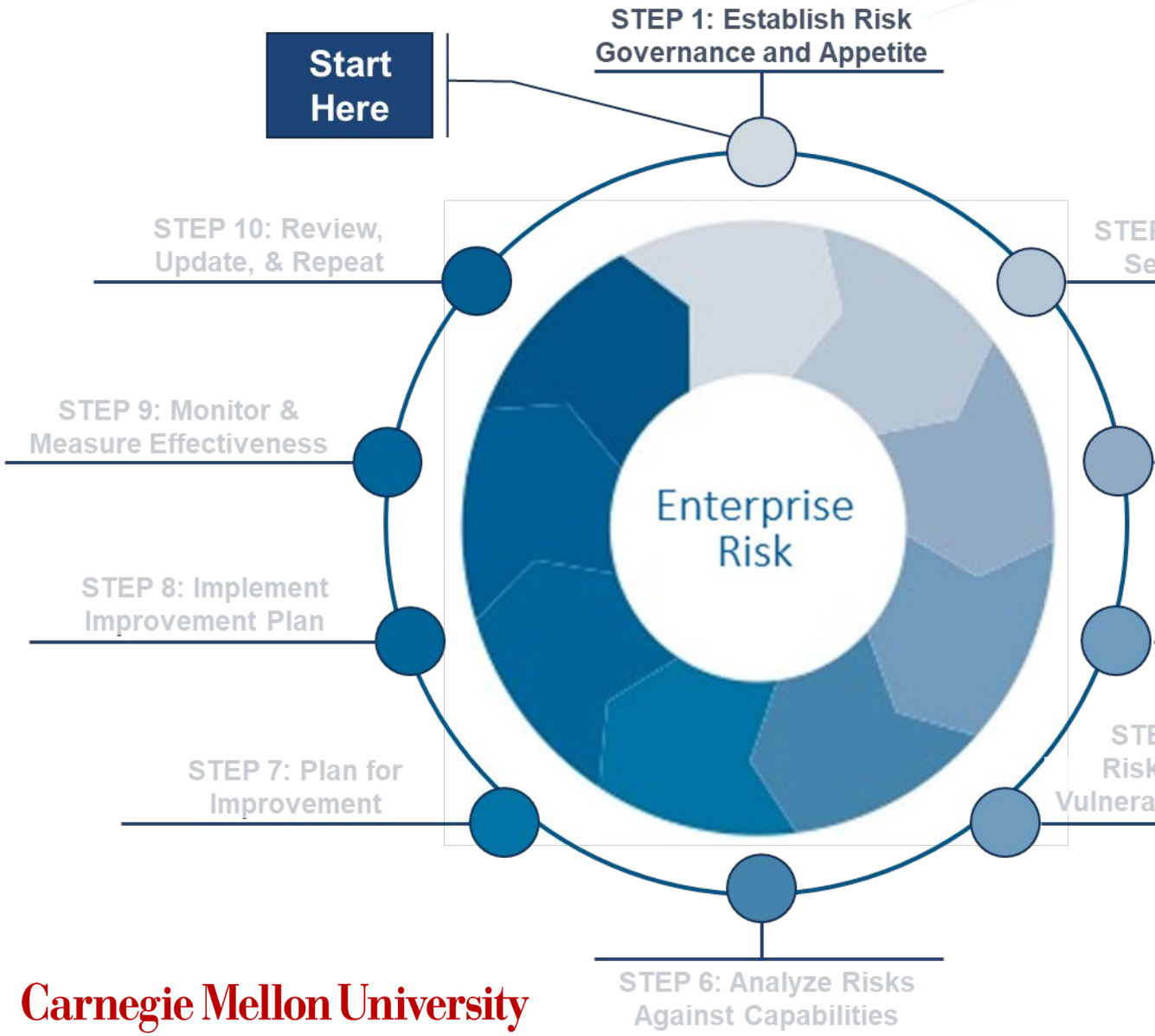


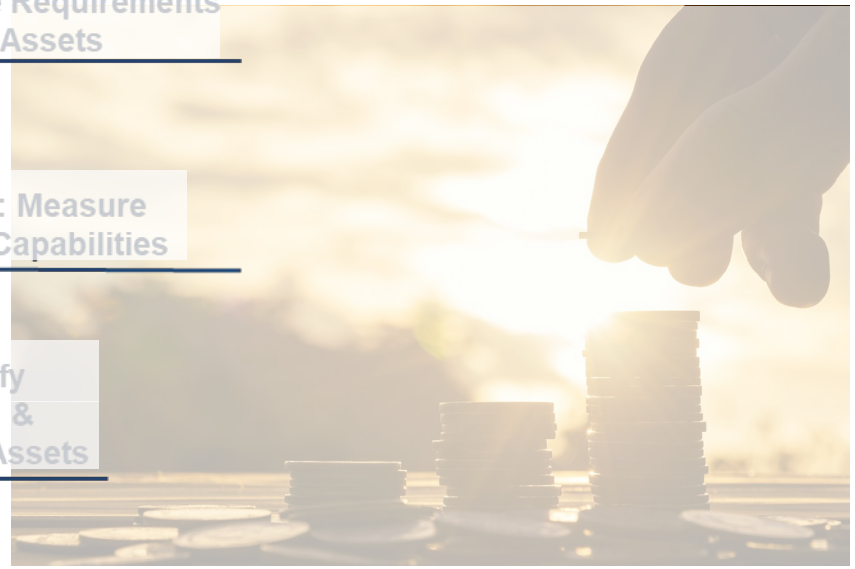
Use Case for an Organization…

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…





Think Marathon, NOT Sprint

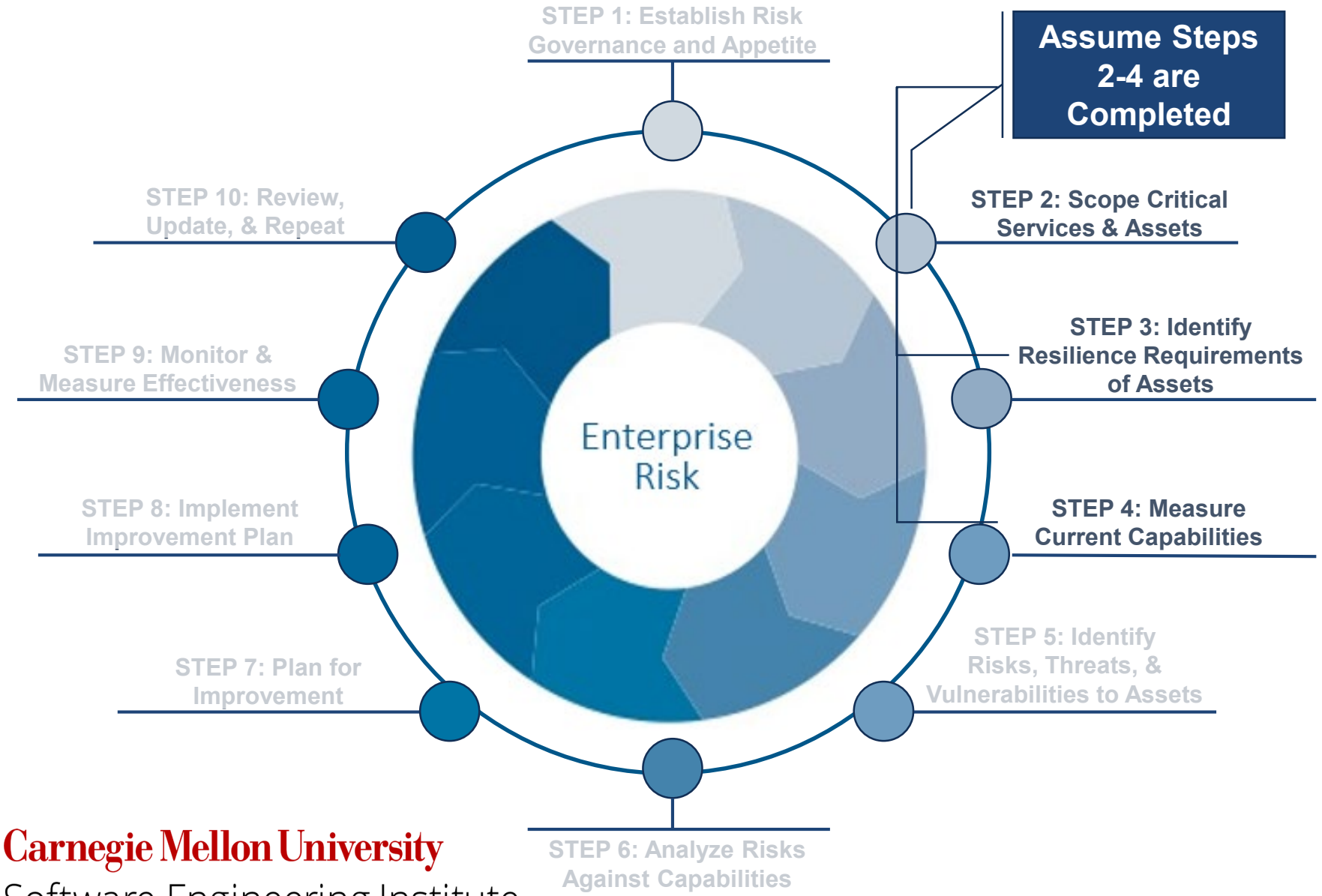
Most Critical Item to Get Started from Step 1…

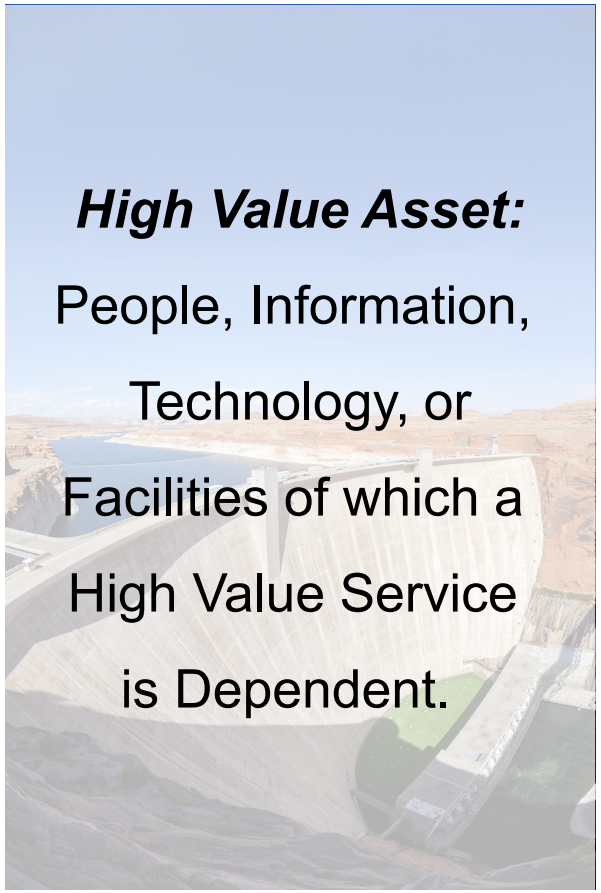
Risk Appetite that is Quantitative and Functional

	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

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

Compressing Effort for Time…





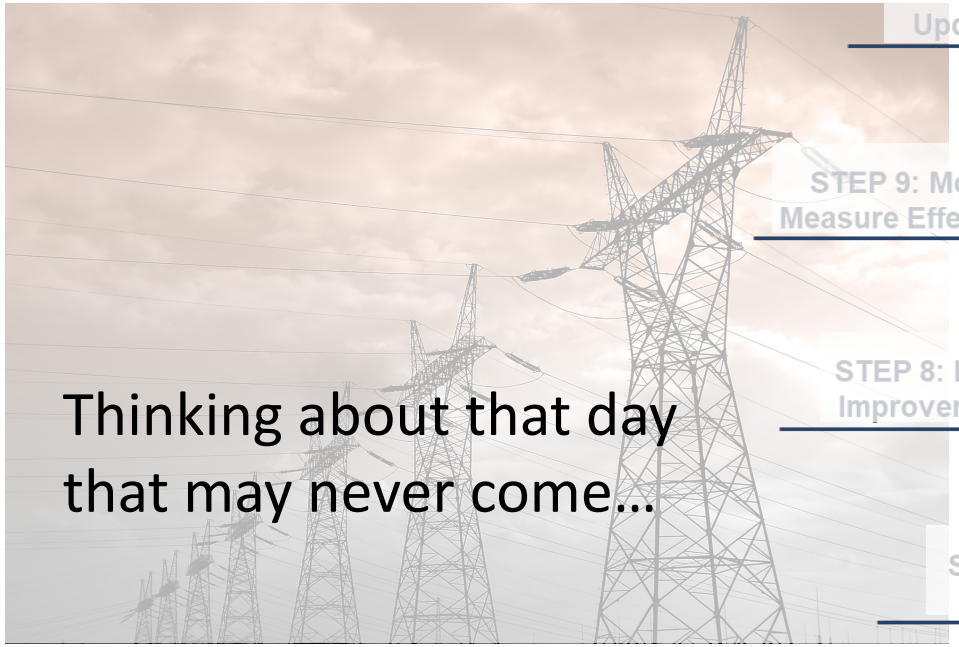
Summary of Results from Steps 2-4

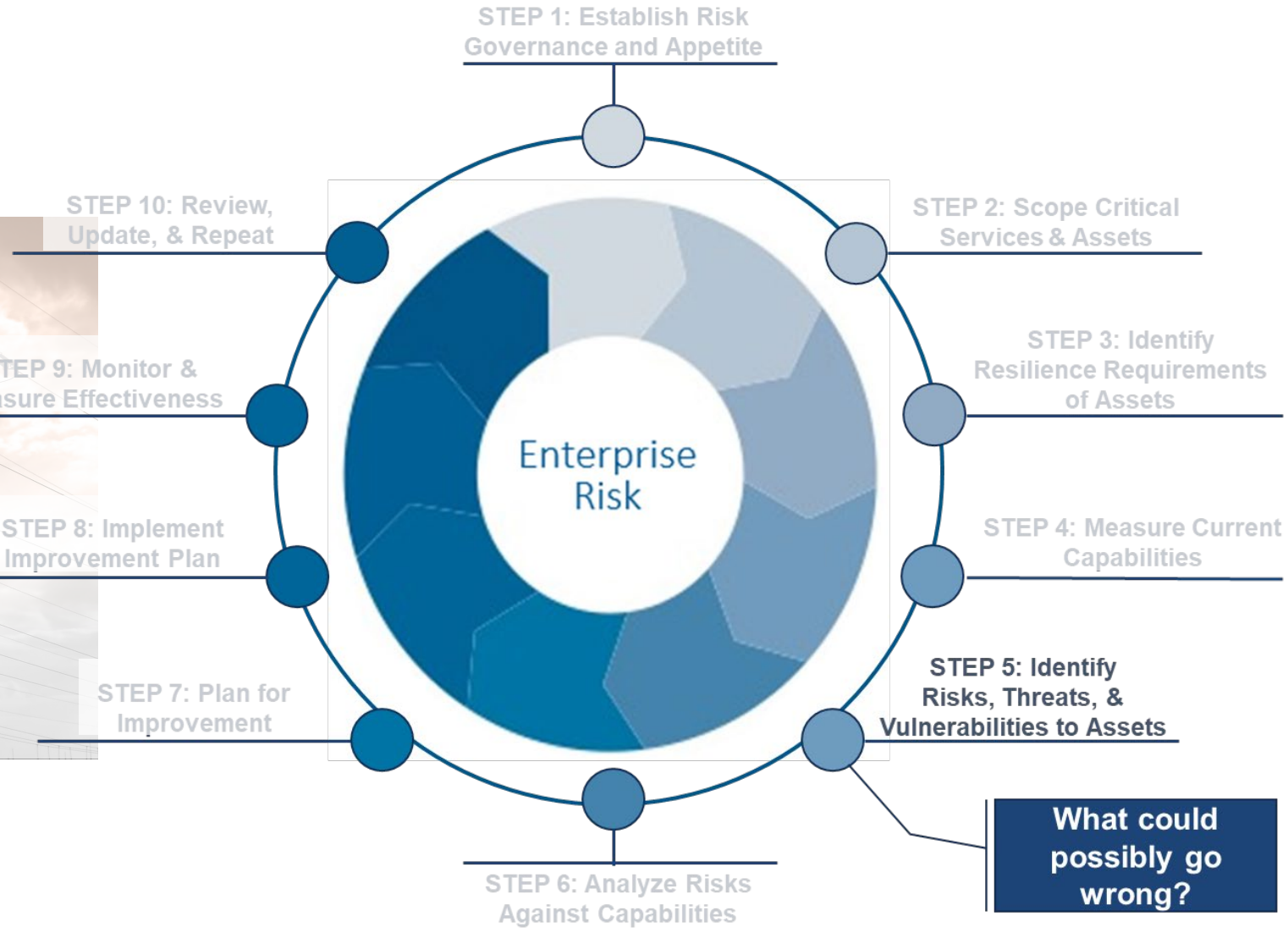
Asset Management and Requirements

- 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





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

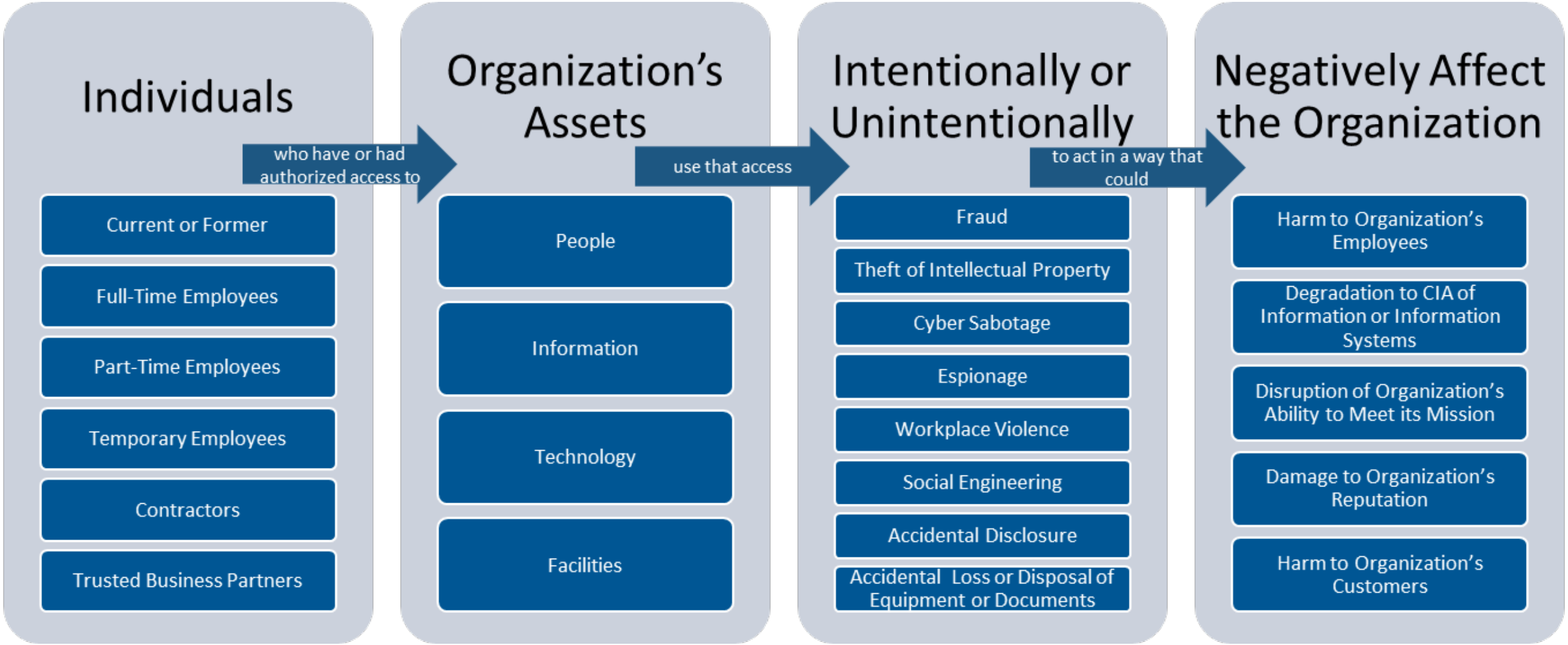
Not Alienate

Insider Threat Program

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



The Insider Threat

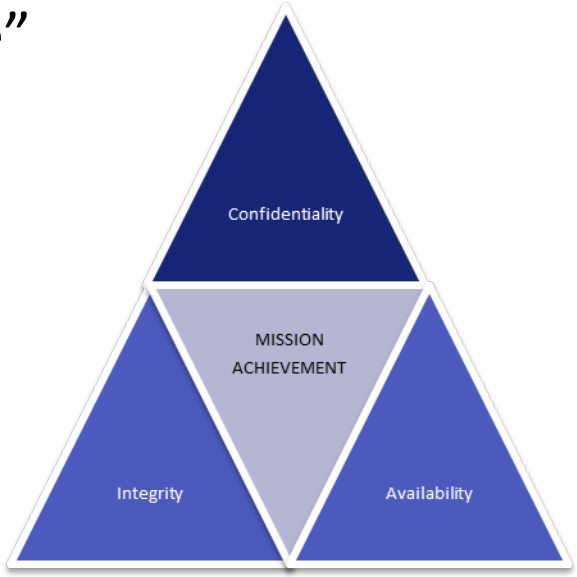
There are no insider threats that can be characterized as “one type”

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

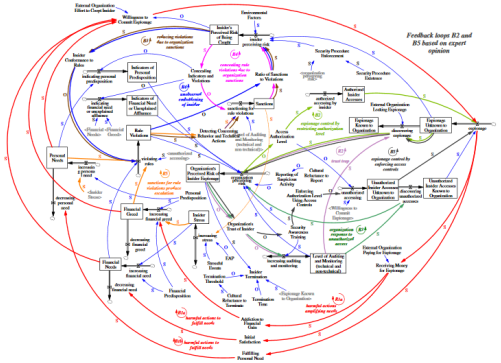
Physical Attack = Physical Impact

Cyber Attack = Physical Impact

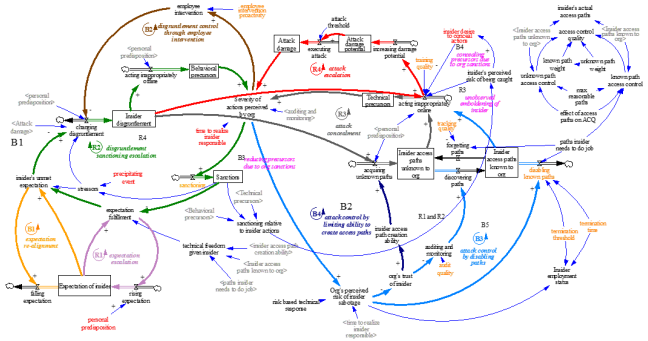
Physical Attack = Cyber Impact

Examples of Insider Incidents

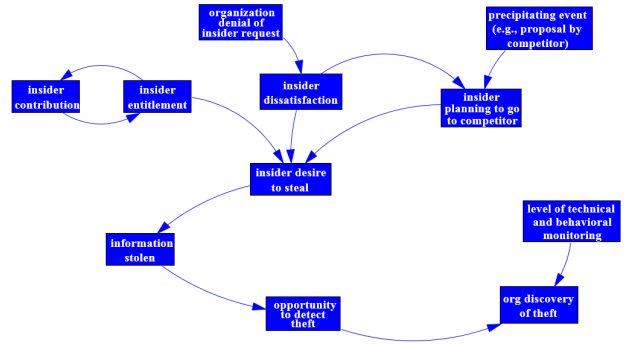
National Security Espionage



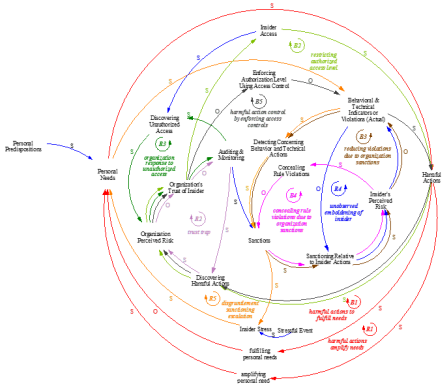
IT System Sabotage



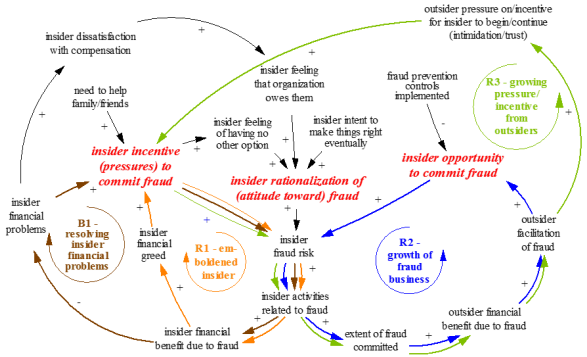
Theft of IP – Entitled Independent



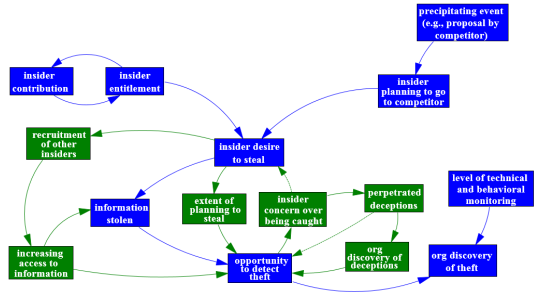
Espionage / Sabotage



Fraud



Theft of IP – Ambitious Leader



Insider Threat Observables

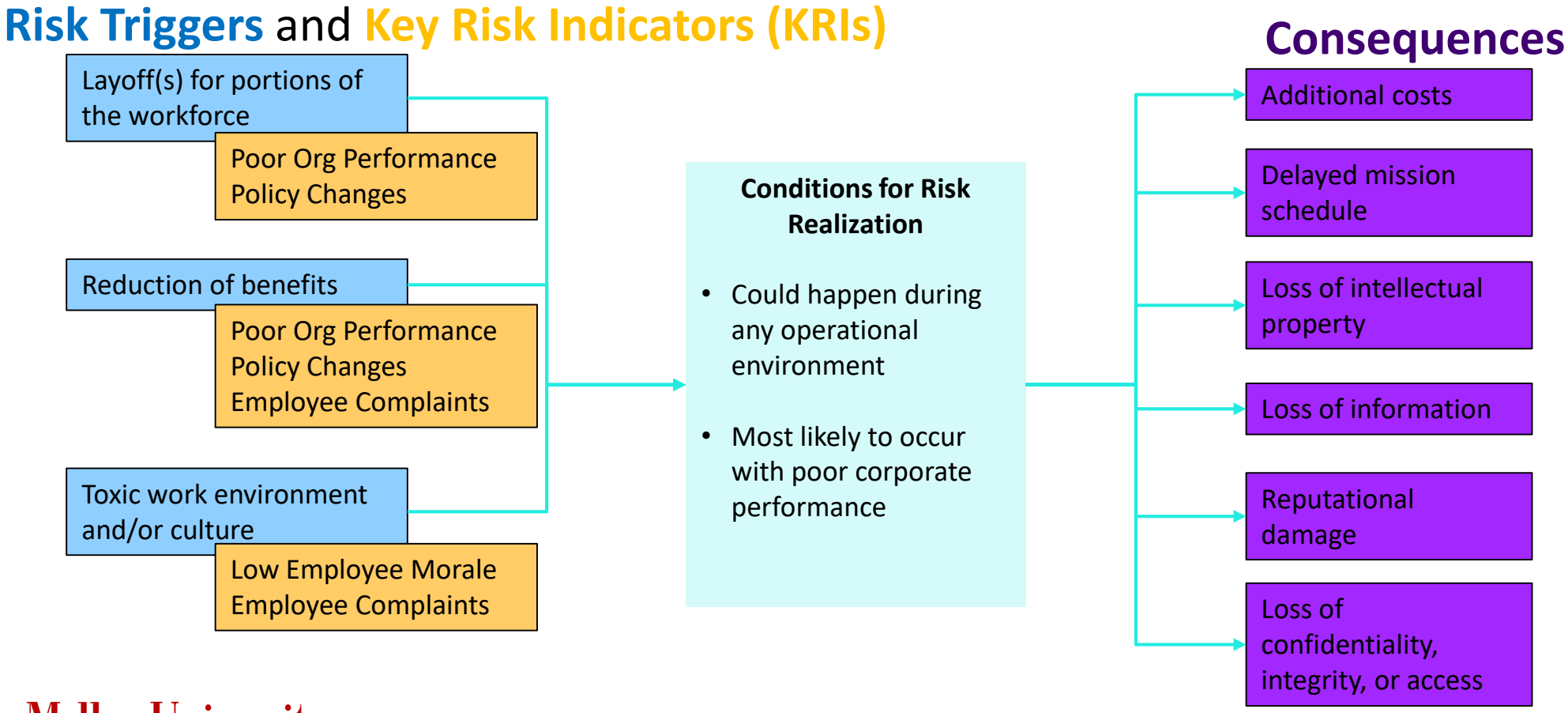
The CERT National Insider Threat Center has amassed a repository of over 2500 Insider incidents (over 18 years).

Potential Insider Threat Risk Indicators (not a complete list)

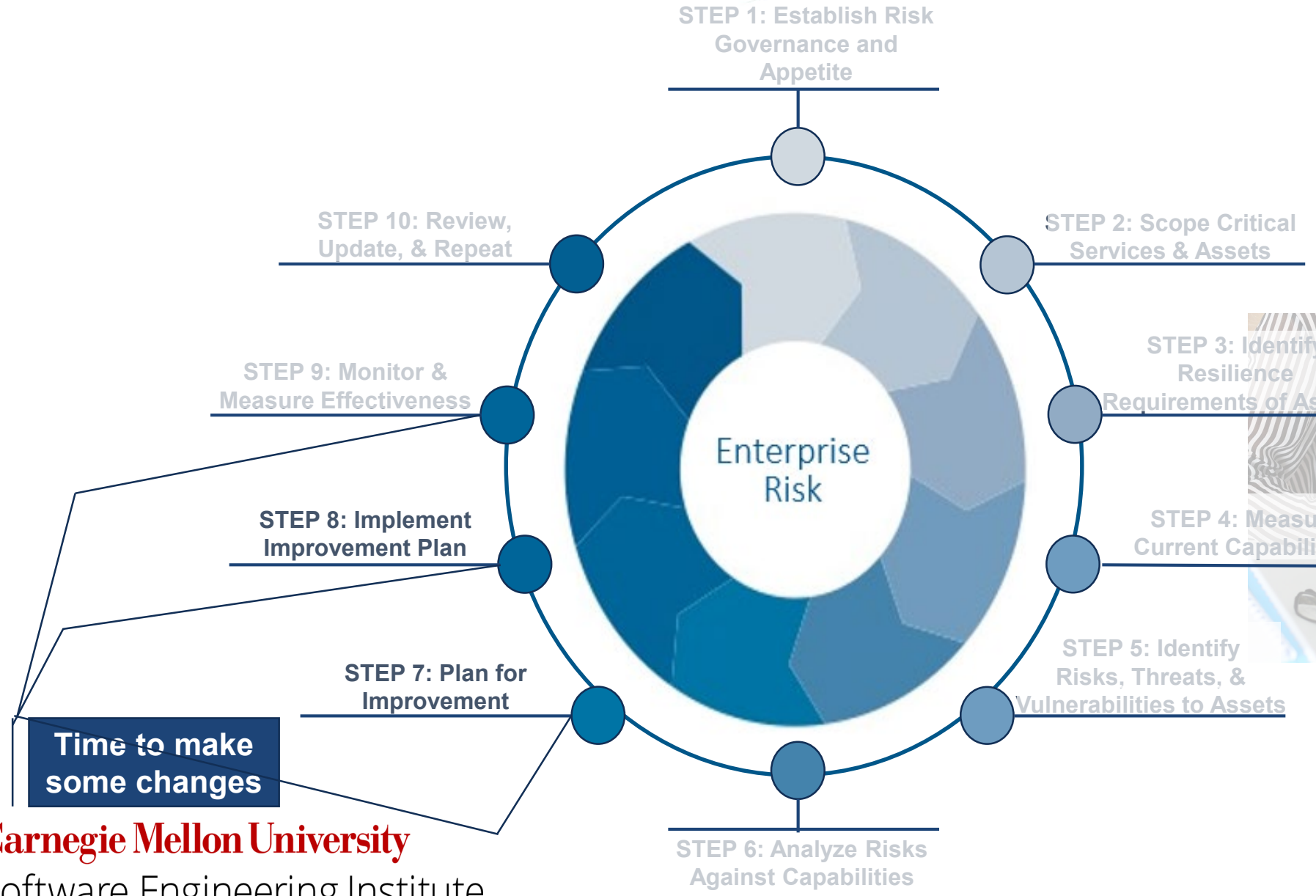
Qualifying the Insider Threat

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.



Developing an Appropriate Response



Time to make some changes

Insider Threat Tools Vary in Features and Functions

Auditing Host-based Activity	Auditing Network-based Activity	Preventing Data from Leaving Authorized Locations
Preserving Forensic Artifacts	Data Visualization	Rule-Based Alerting
Identity Management / Access Management	Data Correlation / Entity Resolution	Anomaly Detection
Machine Learning	Text Analysis	Risk Scoring
Case / Incident Management	Data Masking / Anonymization	... And More ...

Insider Threat Tools Vary in Features and Functions

Auditing Host-based Activity	Auditing Network-based Activity	Preventing Data from Leaving Authorized Locations
Preserving Forensic Artifacts	Data Visualization	Rule-Based Alerting
Identity Management / Access Management	Data Correlation / Entity Resolution	Anomaly Detection
Machine Learning	Text Analysis	Risk Scoring
Case / Incident Management	Data Masking / Anonymization	... And More ...

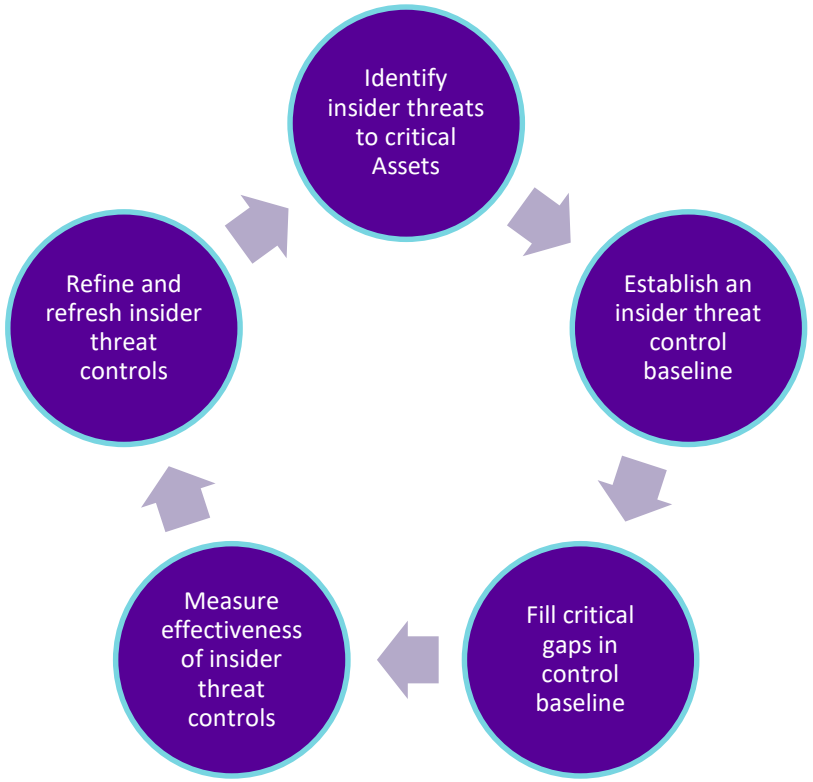
Prevent
- Stop something from happening
- Example: Block a sensitive document from being moved to removable media

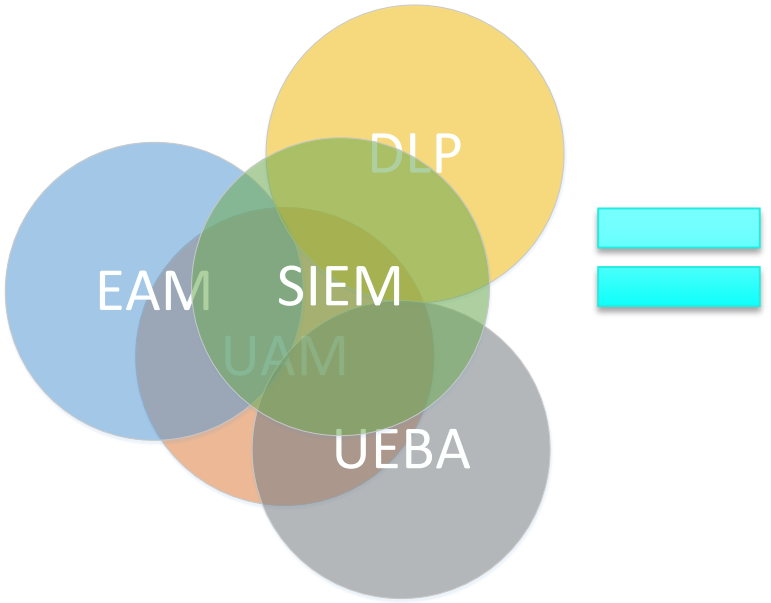
Detect
- Figure out that something is happening (or about to happen)
- Example: Alert security staff of (suspicious?) file activity

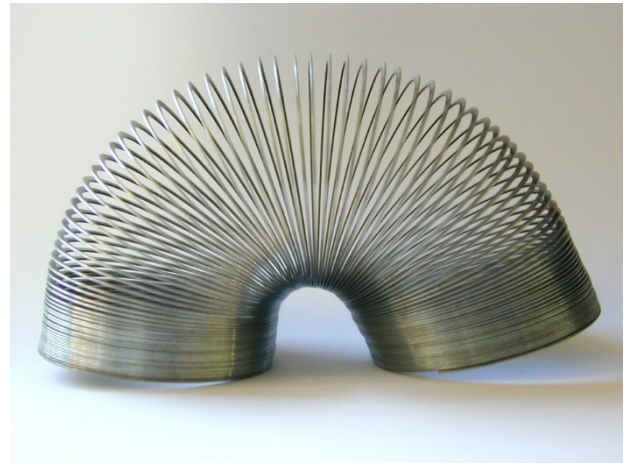
Deter
- Discourage something from happening
- Example: Present a dialog that requires a user to acknowledge the organization's removable media policy

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

Mitigation Plans to Consider







PROCESS + TOOLS = RESILIENCE

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

- CERT National Insider Threat Center: http://www.cert.org/insider-threat/
- Introduction to OCTAVE Allegro: 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
- OCTAVE Version 1.0: 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
- US Federal Government, GAO Report on ERM, December 2016: 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
- NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
- ISACA – COBIT 5 Risk Framework: 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