Getting Ahead of Supply Chain Insider Risks

Randy Trzeciak, Director National Insider Threat Center

Brett Tucker, Technical Manager, Cyber Risk

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.

DM21-0244

The Software Engineering Institute

- A United States Department of Defense Federally Funded Research and Development Center (FFRDC)
- Vision: leading and advancing software engineering and cybersecurity to solve the nation's toughest problems
- Mission: to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

What Is CERT?

Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

Can This Happen to Your Organization?

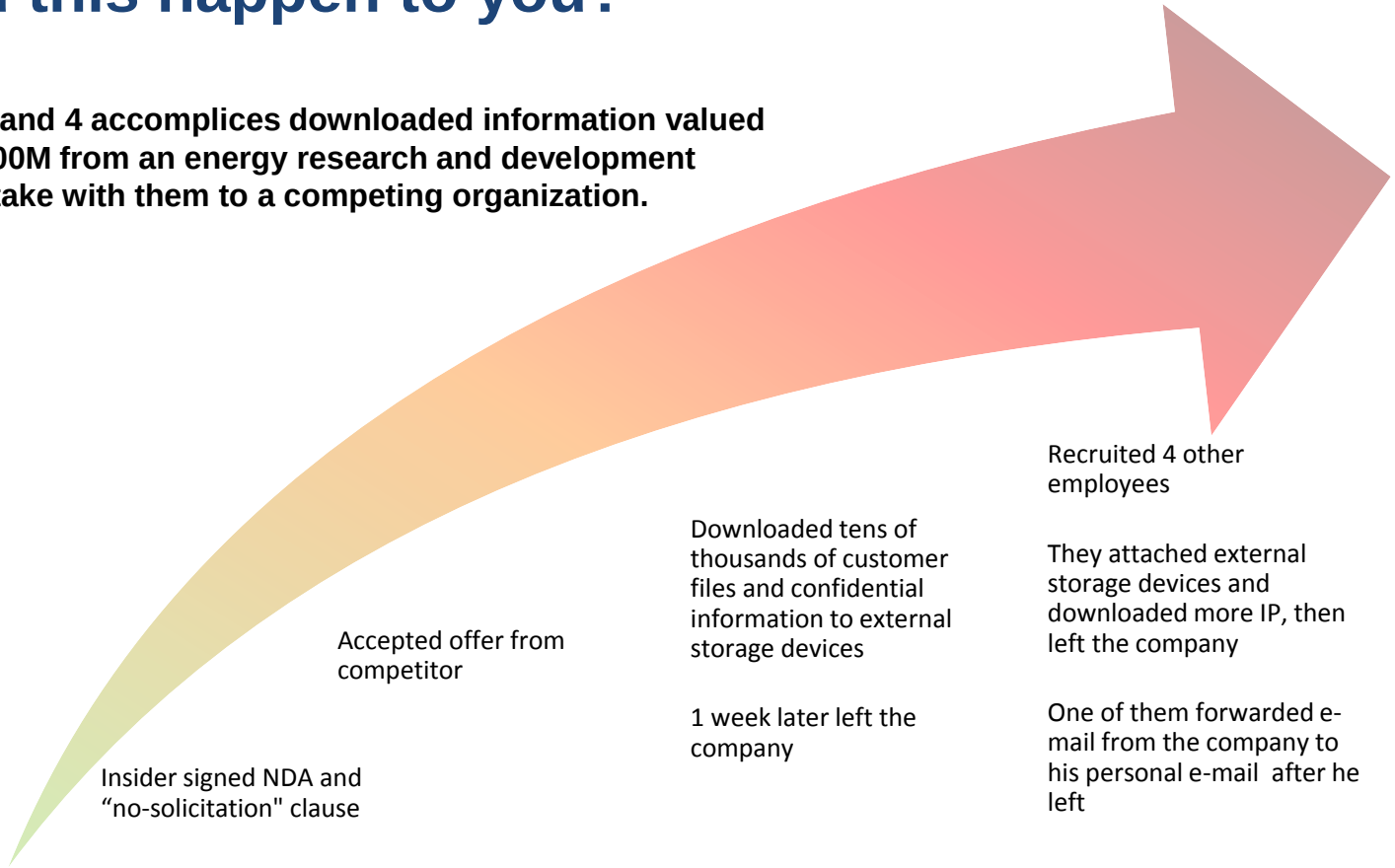
Law Enforcement Employee Performed Unauthorized Queries in Database; Provided Sensitive Information to Domestic and International Acquaintances

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

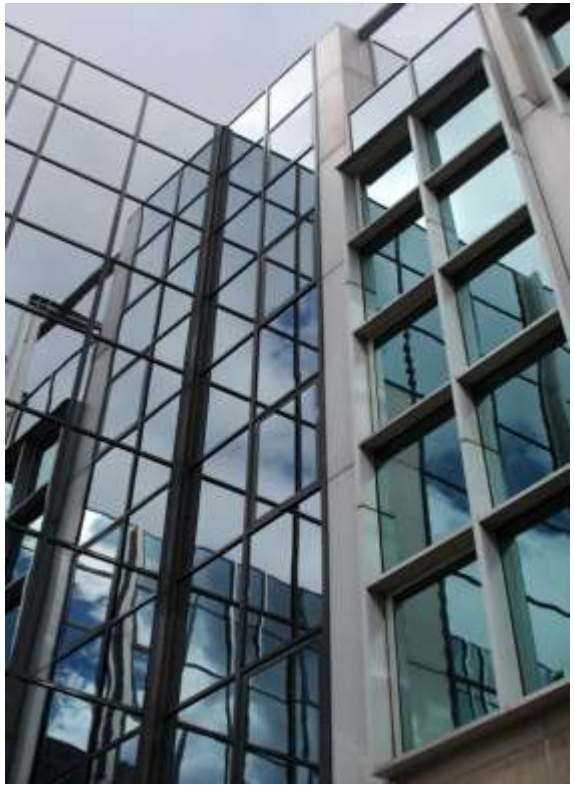
VP of Technology Company Transferred >$19M from Organization to Personal Accounts; Created False Reimbursement Documents for Health Insurance Plan

Could this happen to you?

A director and 4 accomplices downloaded information valued at over $100M from an energy research and development facility to take with them to a competing organization.



The CERT National Insider Threat Center



- The CERT National Insider Threat Center (NITC) focuses on providing insider threat expertise across sectors.
- Began working in this area in 2001 with the U.S. Secret Service
- Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats
- Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

Assessing Insider Threat within the Supply Chain

Attendees will walk away with a greater appreciation for risk:

- Identify common risks related to their supply chain.
- Discuss the various steps of building a risk program to address supplier related risks using OCTAVE FORTE.
- Discuss aspects of insider threat as it relates to partner organizations.

Bottom Line: Insider Threat is a critical risk that can be found in your supply chain and must be addressed

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

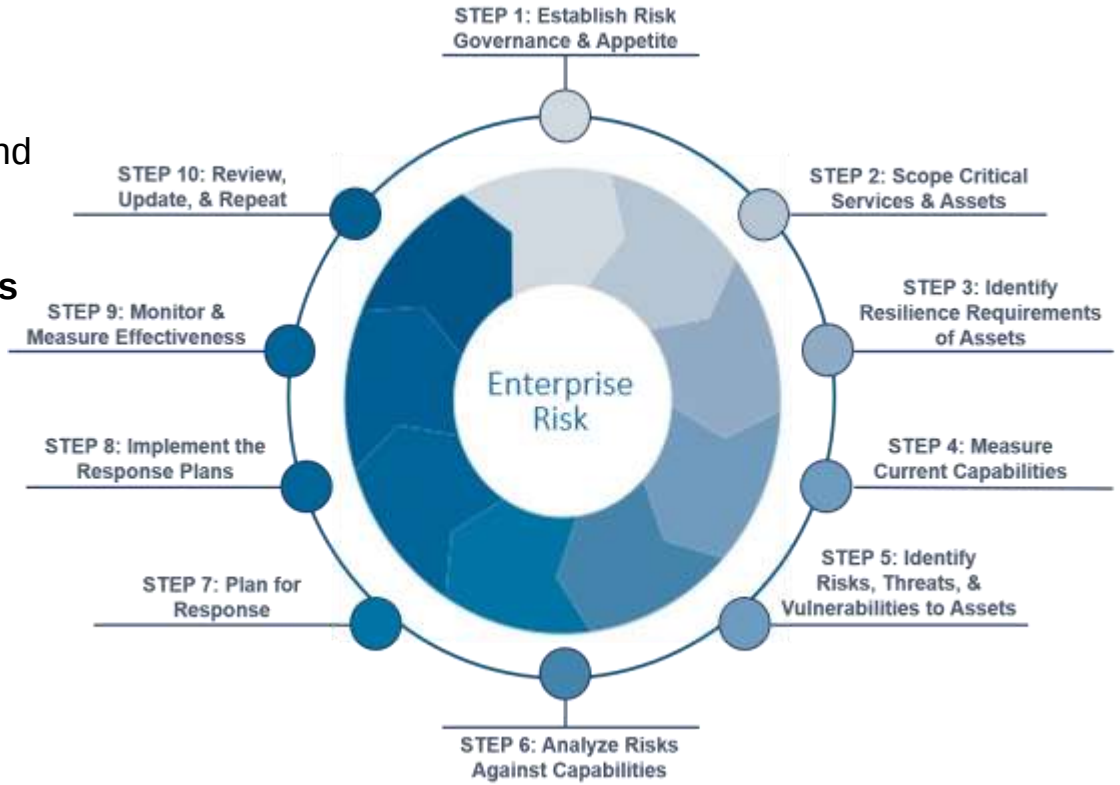
Accounts for Several Standards to Incorporate

FOR **T**he **E**nterprise

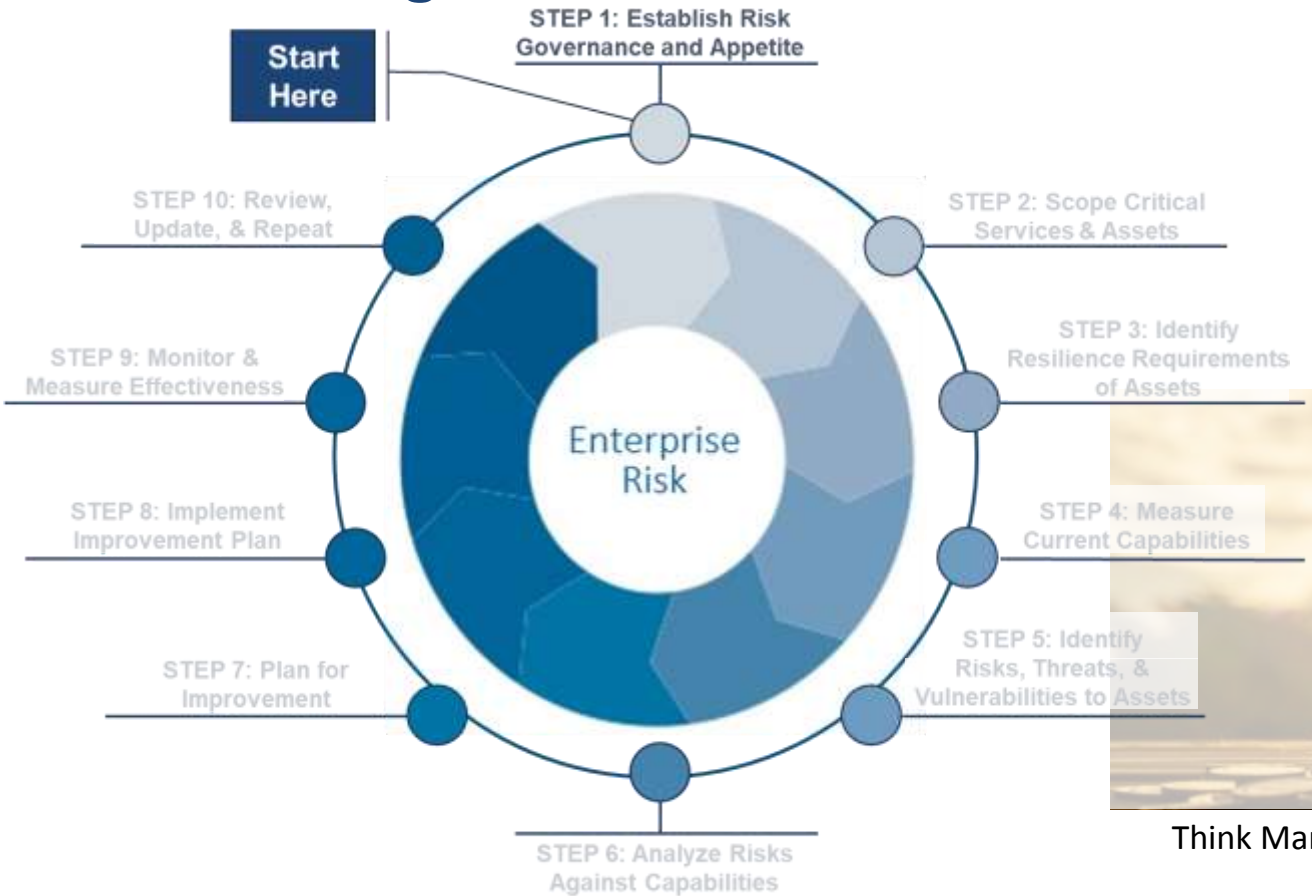
Leverages many standard principles and best practices

Insider risk shares the **same principles of all other risks** and should be managed in the same manner.

This process will enable the enterprise **to identify the interdependence of insider threats from supply chain vectors**.



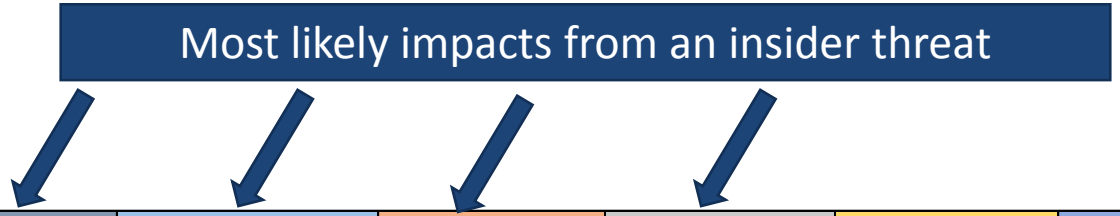
Where to begin…



Think Marathon, NOT Sprint

Most Critical Item to Get Started from Step 1…

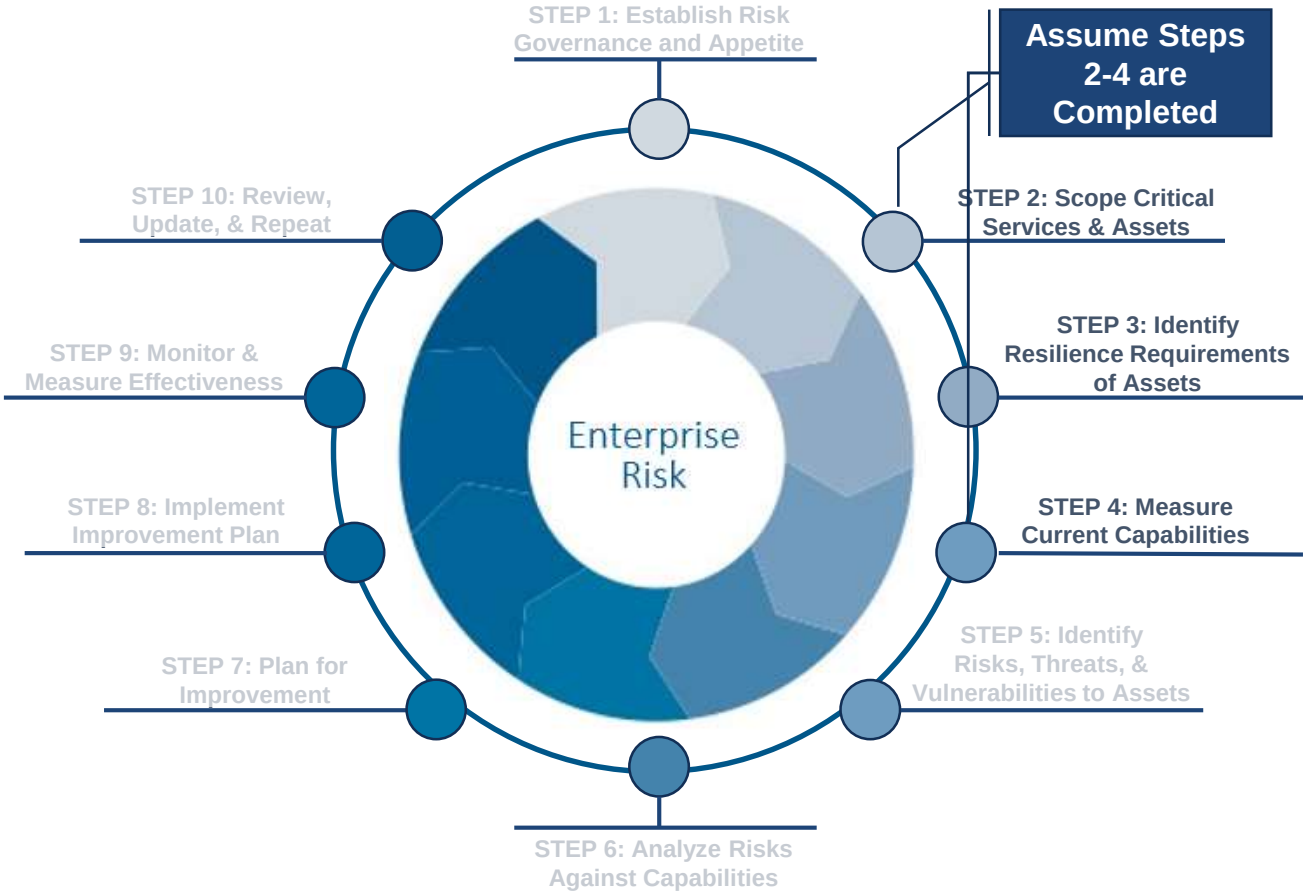
Risk Appetite that is Quantitative and Functional



	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…



High Value Asset:

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

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

CRITICAL STEP in identifying supply chain dependencies

Identifying Assets Supplied from External Sources

Assets identified through **value stream mapping**:

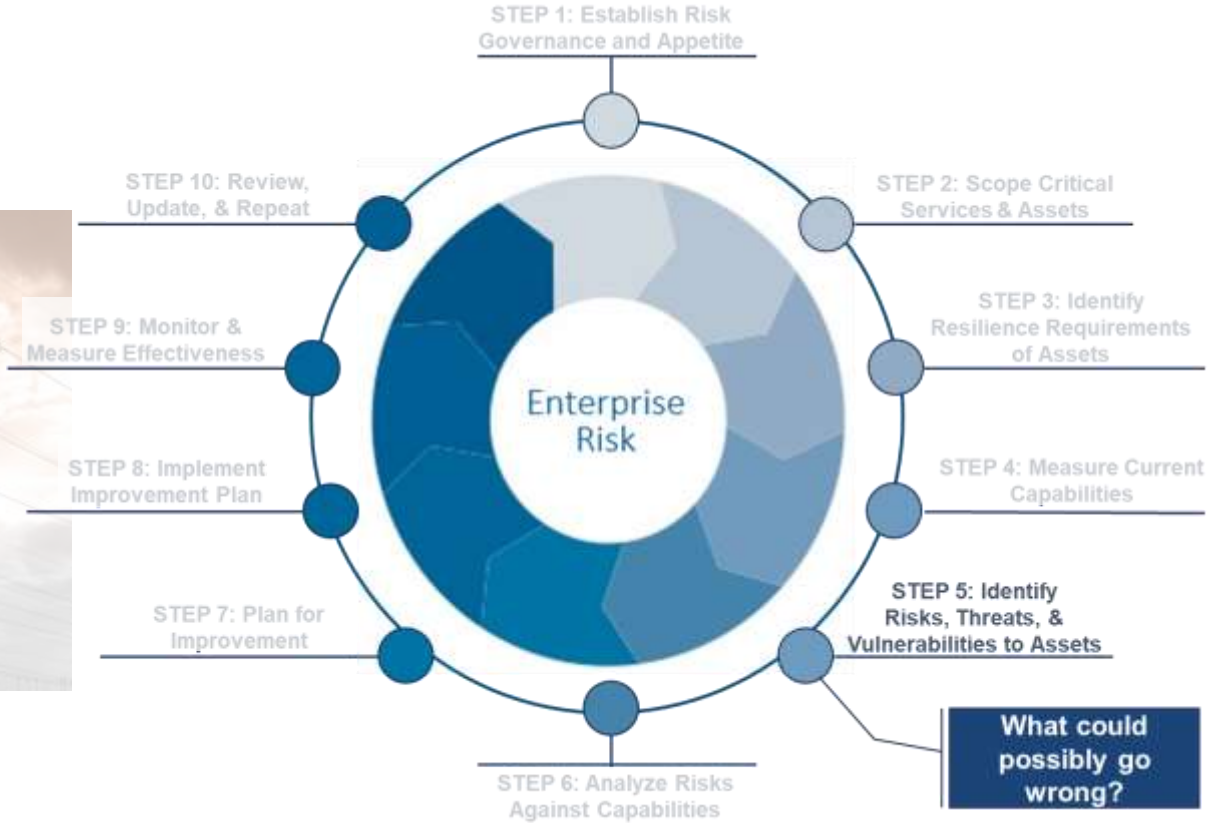
Assets may be classified as:

- People
- Information
- Technology
- Facilities

Assets provided by **external parties may contain vulnerabilities** that are no different than internal sources.

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

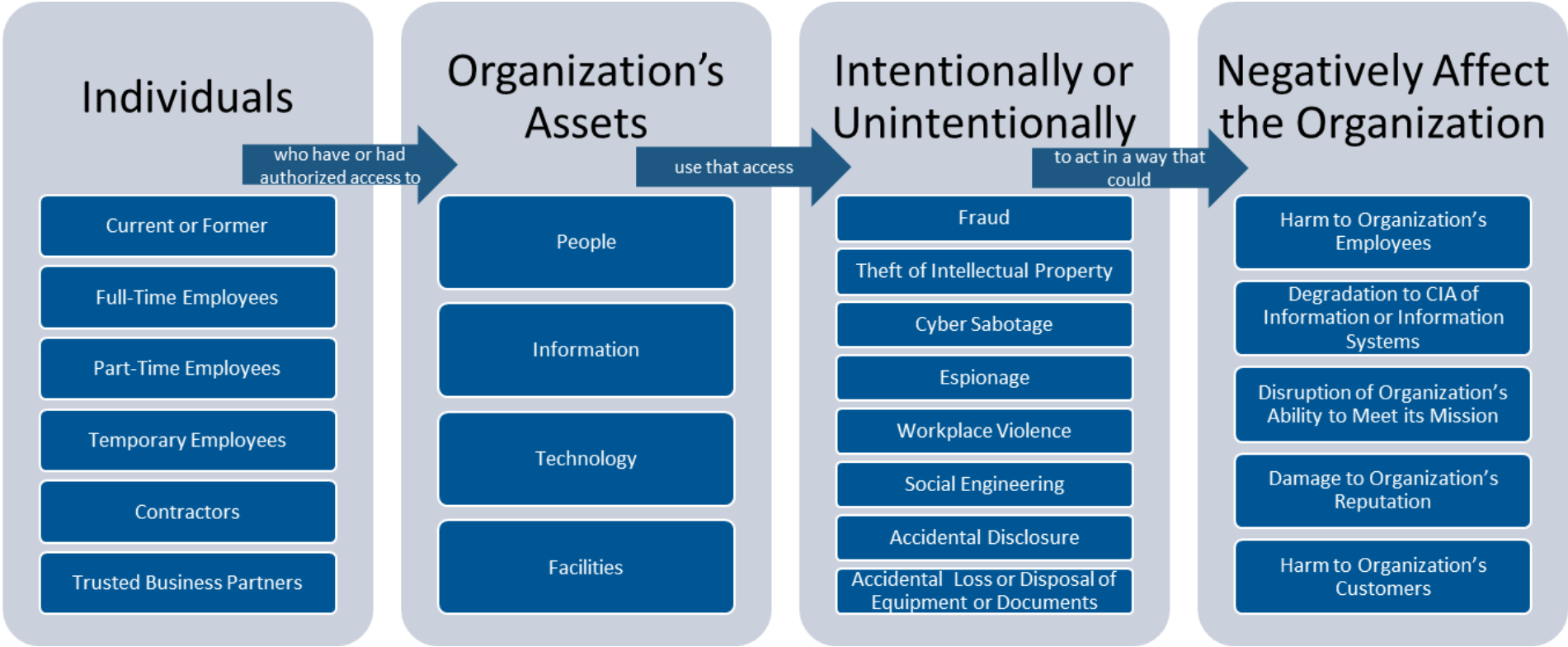
Insider Threat Program

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.

Organizations may provide the same access to external providers, especially contracted team members who may not share the same vetting yet require the same access.

Insider Threat to Critical Assets



The Insider Threat

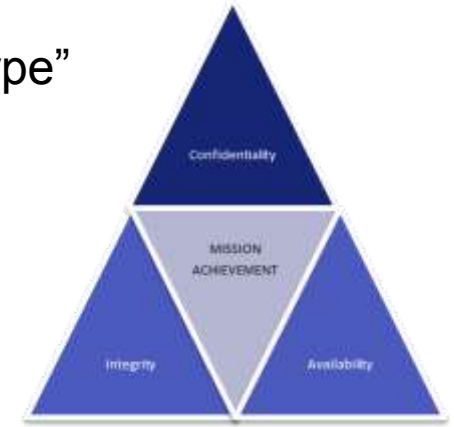
There are no insider threats that can be characterized as “one type”

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



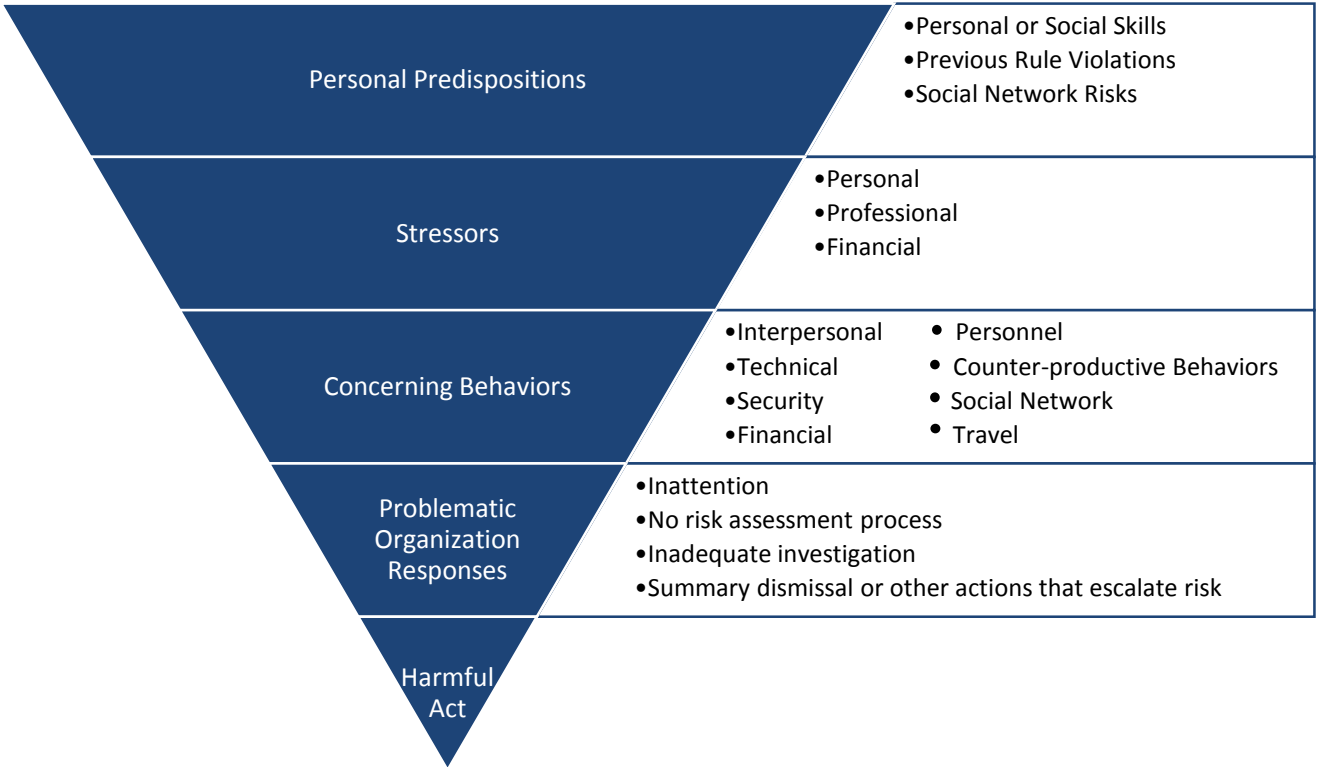
Cyber Attack = Cyber Impact

Physical Attack = Physical Impact

Cyber Attack = Physical Impact

Physical Attack = Cyber Impact

The Critical Path to Insider Risk



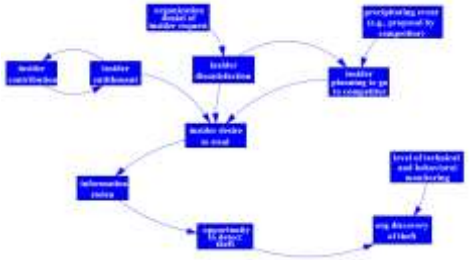
Adapted from Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)

Examples of Insider Incidents

National Security Espionage

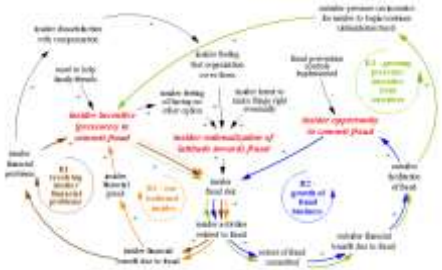
IT System Sabotage

Theft of IP – Entitled Independent

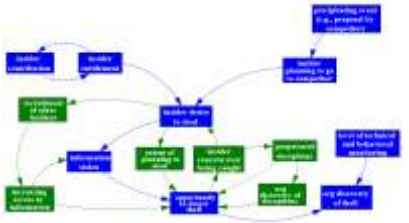


Espionage / Sabotage

Fraud



Theft of IP – Ambitious Leader

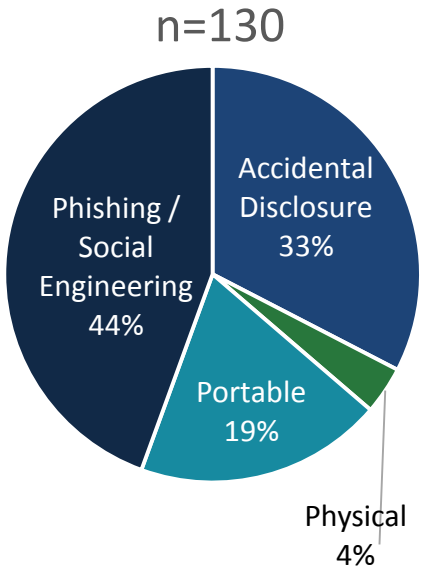


Insider Threat Observables

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)

Unintentional Insider Threats



Accidental Disclosure (e.g., via the internet)

- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

Malicious Code (e.g., hacking, malware/spyware)

- an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

Improper/accidental disposal of physical records

- lost, discarded, or stolen non-electronic records, such as paper documents

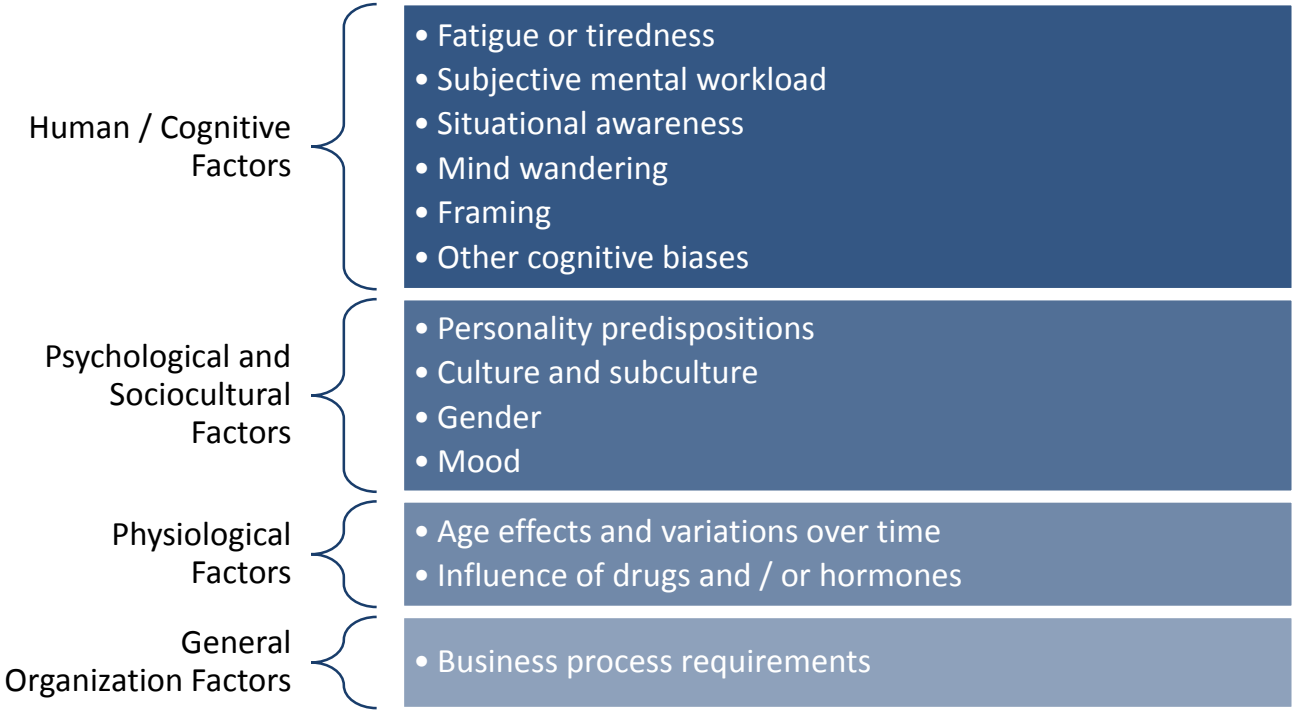
Portable equipment no longer in possession

- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

Source: Unintentional Insider Threats: A Foundational Study, Available Online at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

Contributing Factors to Human Error

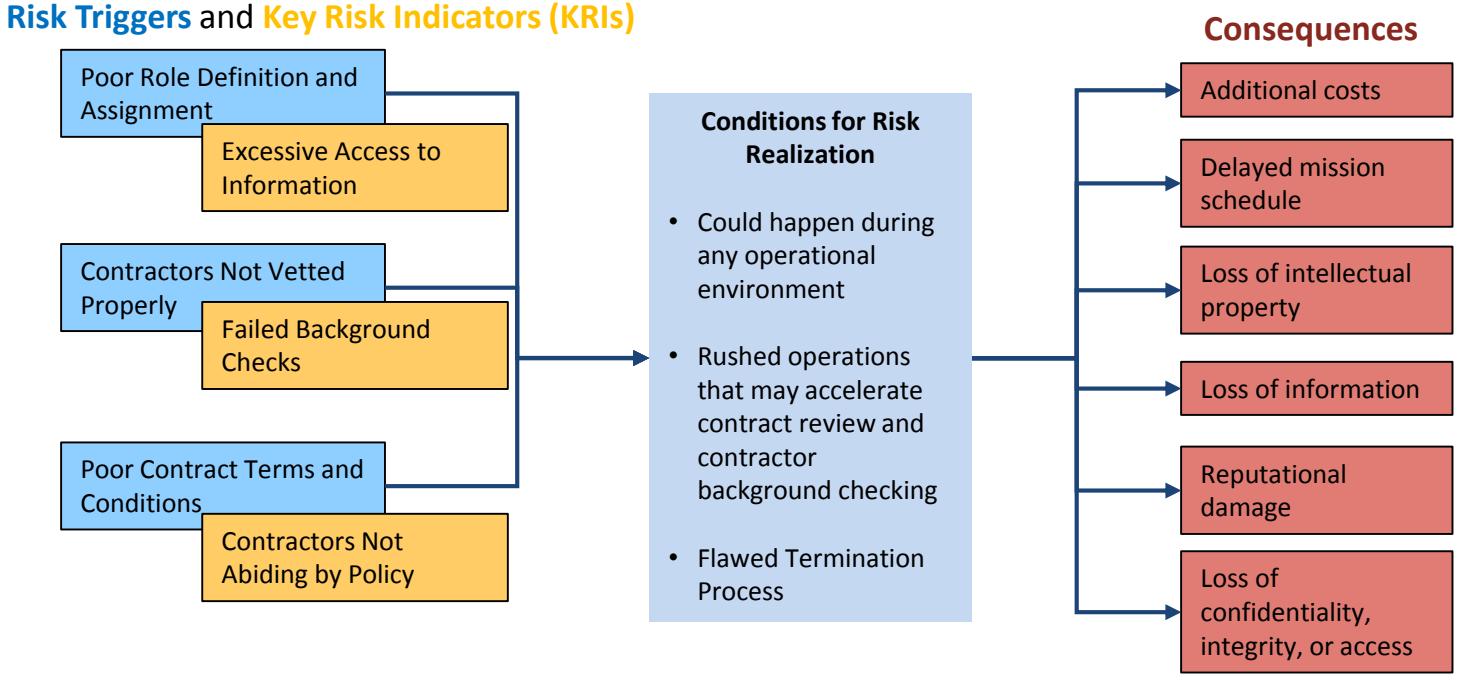
Contributing Factors in Risk Perception



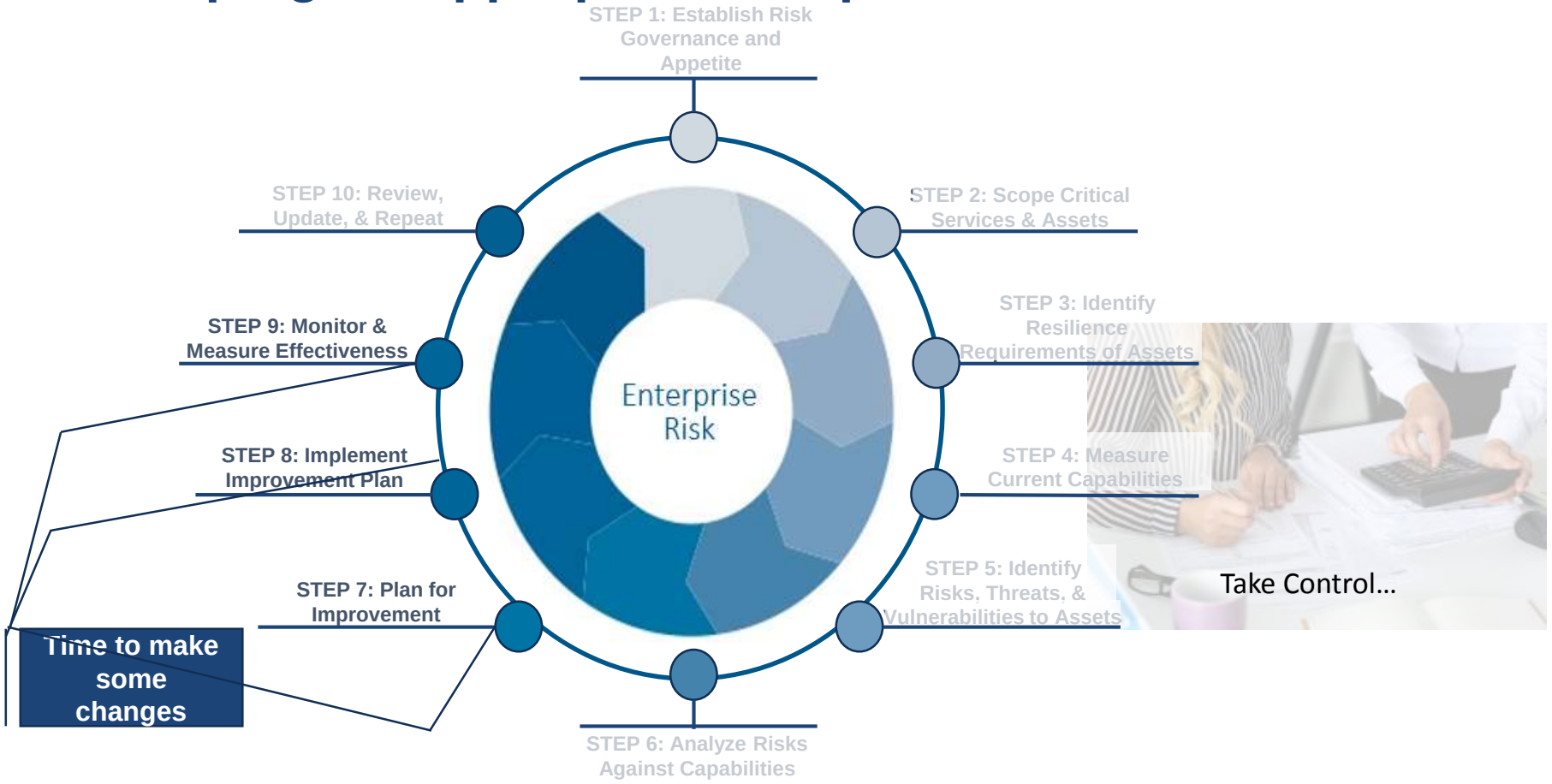
Qualifying the Insider Threat

Operations: Insider Threat in the Supply Chain

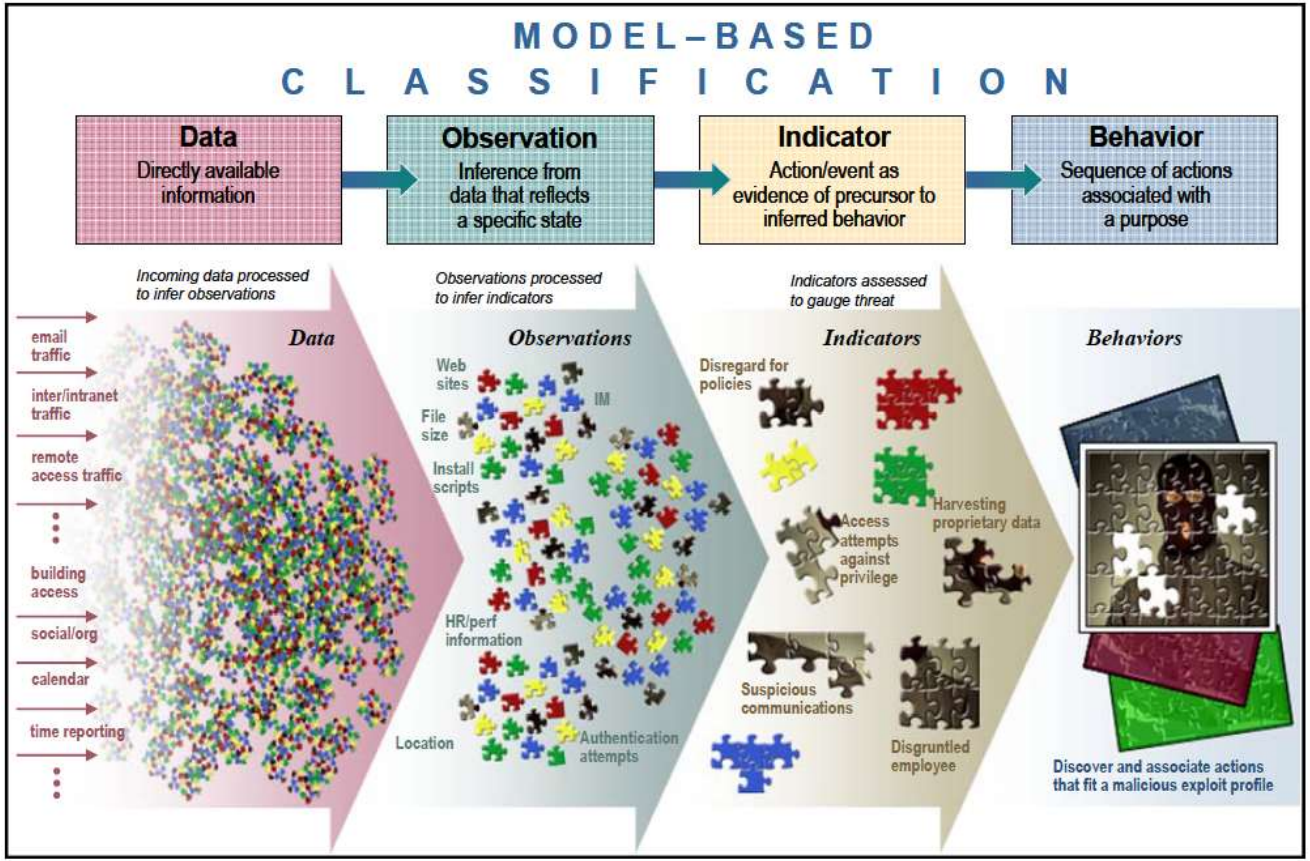
Scope Statement: If the organization fails to properly review external providers, then mission and lives could be jeopardized by risk exposure from that provider.



Developing an Appropriate Response



A Conceptual Model



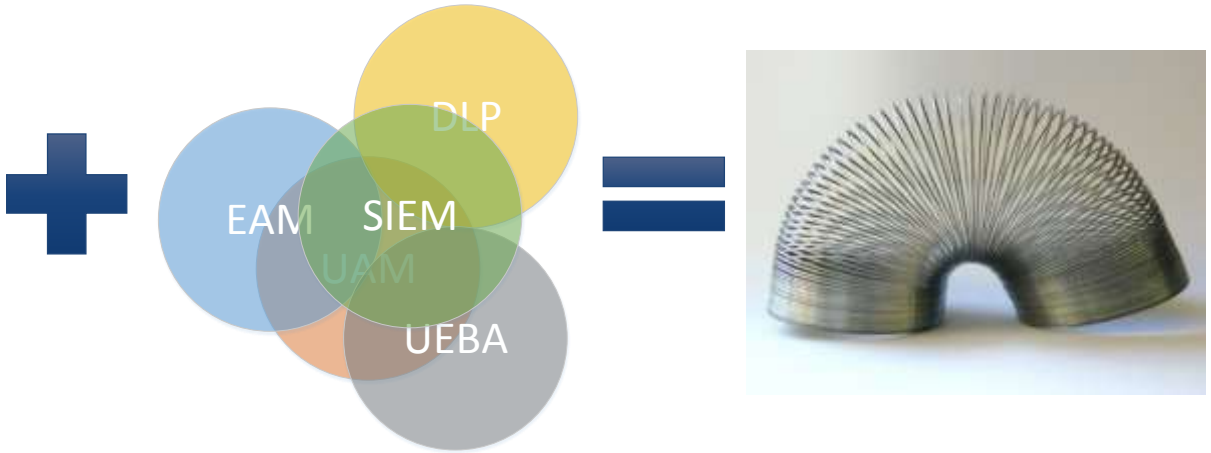
Source: Greitzer, et al., "Predictive Modeling for Insider Threat Mitigation," PNNL-SA-65204, April 2009.

Insider Threat Tools Vary in Features and Functions

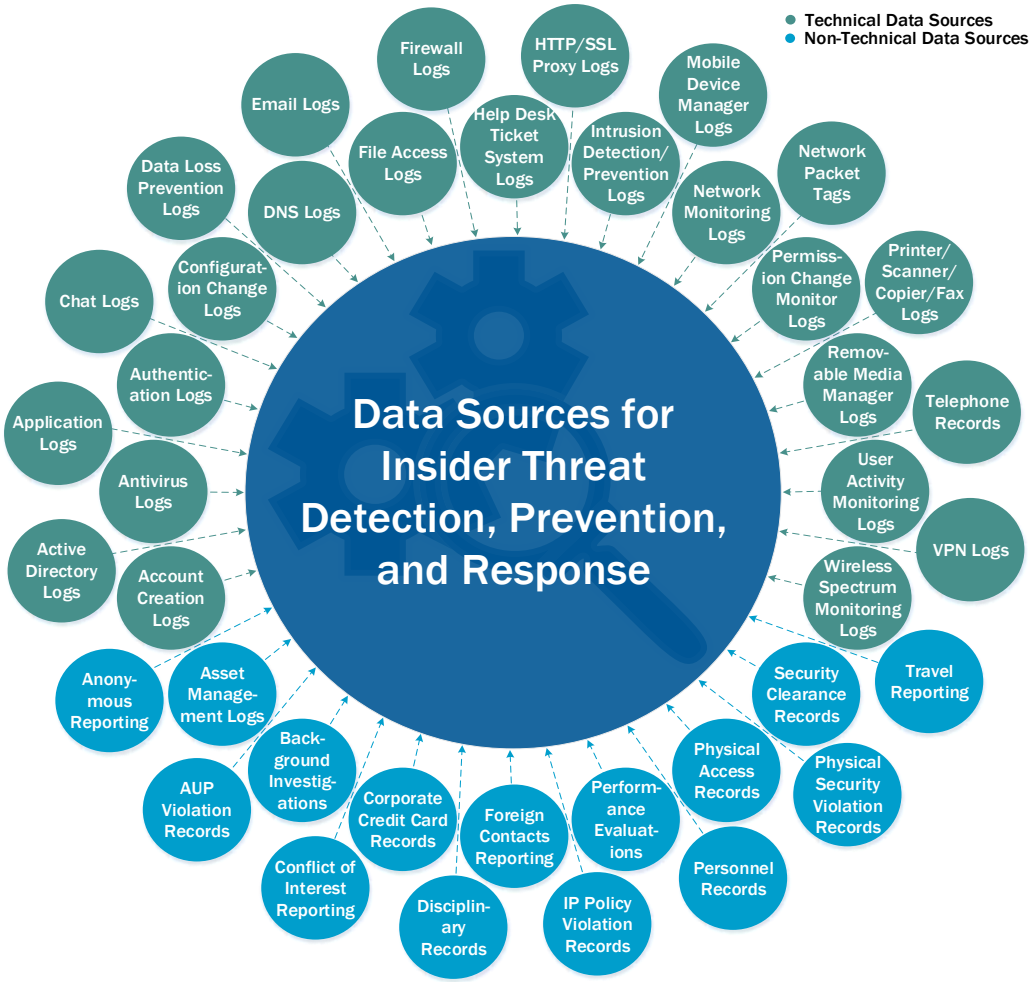
Insider Threat Tools Vary in Features and Functions

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 ...

Mitigation Plans to Consider



PROCESS + TOOLS = RESILIENCE

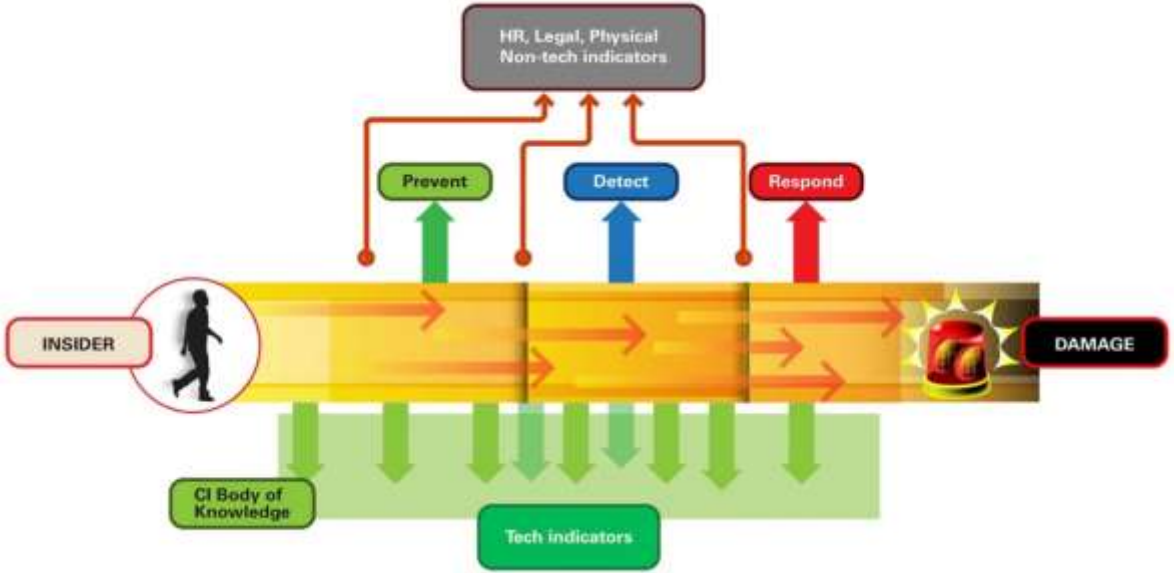


Use-Case Based Data Source Prioritization Example

Use Case	Use Case Priority	Observable	HR System	DLP Logs	Help Desk Tickets	Active Directory Logs	Windows Event Logs
Departing Employee IP Theft	HIGH	Employee Termination	X				
	HIGH	Data Exfiltration		X			
Unauthorized Account Creation	MEDIUM	Account Creation				X	
	MEDIUM	Job Role of Account Creator	X				
	MEDIUM	No Associated Help Desk Ticket			X		
Clearing Security Logs	LOW	Windows Security Logs Cleared					X
…							
Data Source Priority Score			**5**	**3**	**2**	**2**	**1**

Insider Risk Program Building

The Goal for an Insider Risk Program…



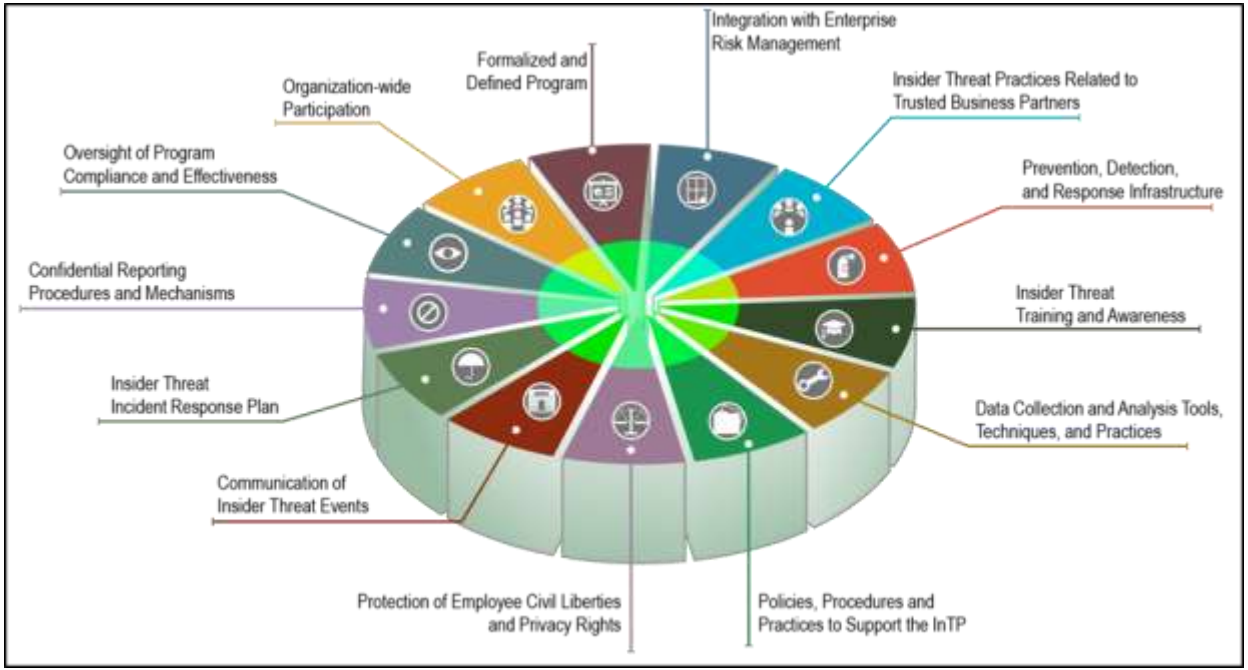
Is to reduce insider risks to critical assets to acceptable levels

https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html

Essential Elements of an Insider Risk Program

Source: https://www.insaonline.org/insider-threat-roadmap/

Key Components of an Insider Threat Program



Best Practices from the CERT Common Sense Guide to Mitigating Insider Threats

1 - Know and protect your critical assets.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
2 - Develop a formalized insider threat program.	13 - Monitor and control remote access from all endpoints, including mobile devices.
3 - Clearly document and consistently enforce policies and controls.	14 - Establish a baseline of normal behavior for both networks and employees
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	15 - Enforce separation of duties and least privilege.
5 - Anticipate and manage negative issues in the work environment.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	17 - Institutionalize system change controls.
7 - Be especially vigilant regarding social media.	18 - Implement secure backup and recovery processes.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	19 - Close the doors to unauthorized data exfiltration.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	20 - Develop a comprehensive employee termination procedure.
10 - Implement strict password and account management policies and practices.	21 - Adopt positive incentives to align the workforce with the organization.
11 - Institute stringent access controls and monitoring policies on privileged users.	

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644

Apply What You Have Learned Today

Next week you should:

- Determine the what asset management processes are used in your organization
- Identify ownership and state of insider threat management
- ***Determine the intersection of insider threat program with contracted workforce***

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
- Seek legal assistance to enhance contractual terms and conditions

Training from the CERT National Insider Threat Center

Our insider threat program manager, vulnerability assessor, and program evaluator certificate programs and insider threat analyst training courses are now available in live-online delivery formats!

For more information, please visit
www.sei.cmu.edu/education-outreach/courses/index.cfm

Additional Training from the CERT

OCTAVE Allegro Training: Provide your work force with a process and tool set for analyzing and managing information risk

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P10B

Introduction to the CERT Resilience Management Model: Learn how to build a more resilient organization

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P66

Measuring What Matters: Learn how to develop metrics for your risk programs

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P117

OCTAVE FORTE – Connecting the Board Room to Cyber Risk: Learn how to build a more effective risk management program

https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P136

Open Source Insider Threat (OSIT) Information Sharing Group

Community of Interest for insider threat program practitioners across industry organizations

Over 520 members from ~225 organizations

Special interest groups

- Data Analytics
- Financial Services
- Energy Sector
- Privacy

Monthly Telecons

- Tool Vendor Demos

Bi-annual In-Person Meetings

- Hosted by various members of the group

To join, contact:

rft@cert.org

Resources and References

- CERT National Insider Threat Center: http://www.cert.org/insider-threat/
- Advancing Risk Management Capability Using the OCTAVE FORTE Process: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf
- 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?

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

Brett Tucker, PMP, CSSBB, CISSP
Telephone: 412.268.6682
Email: batucker@cert.org