RSA 2022

The Components of an Effective Insider Risk Program

Randall (Randy) Trzeciak

Carnegie Mellon University
Software Engineering Institute

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.

DM22-0495

Carnegie Mellon University (CMU)

Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
  - #1 in computer engineering, AI, cybersecurity, and software engineering
  - #2 in overall computer science
  - #3 in data analytics/science

CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

CERT Division: Birthplace of Cybersecurity

Trusted
Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued
Collaborating with military, industry, and academia globally to innovate solutions

Relevant
Achieving technology and talent results for our mission partners

Why Insider Risk Management?

Ensures insider risks are managed consistently with other types of risk

Allows the insider threat program to leverage existing resources

- Avoids duplication of effort
- Ensures the insider threat program is working with the best available information

Enables precise definition of InTP scope and quantifiable goals

Critical Asset Identification

Ask yourself:

- What products or services do we provide?
- What do we do in order to provide these services or products?
- What assets do we use when performing these things?
- What are the security requirements of these assets?
- What is the value of these 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

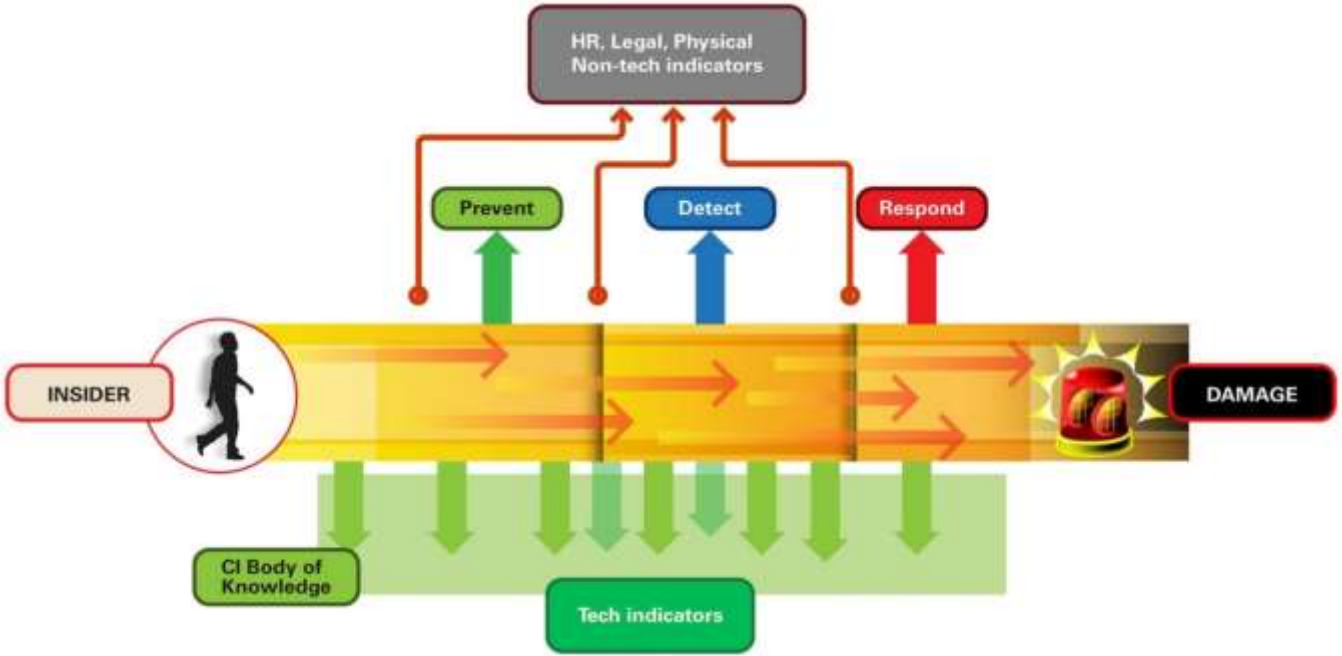
Cyber Attack = Cyber Impact

Physical Attack = Physical Impact

Cyber Attack = Physical Impact

Physical Attack = Cyber Impact

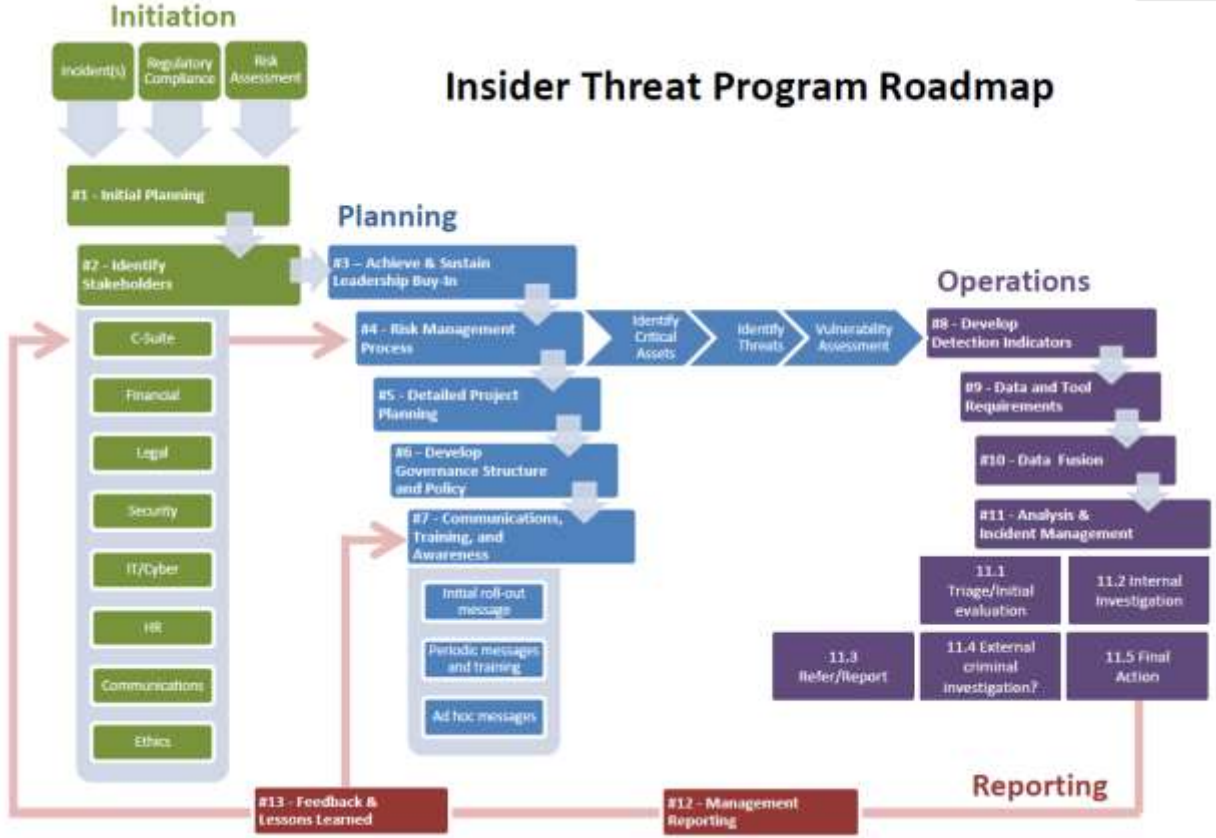
The Goal for an Insider Threat Program…



Is to reduce insider risks to critical assets to acceptable levels

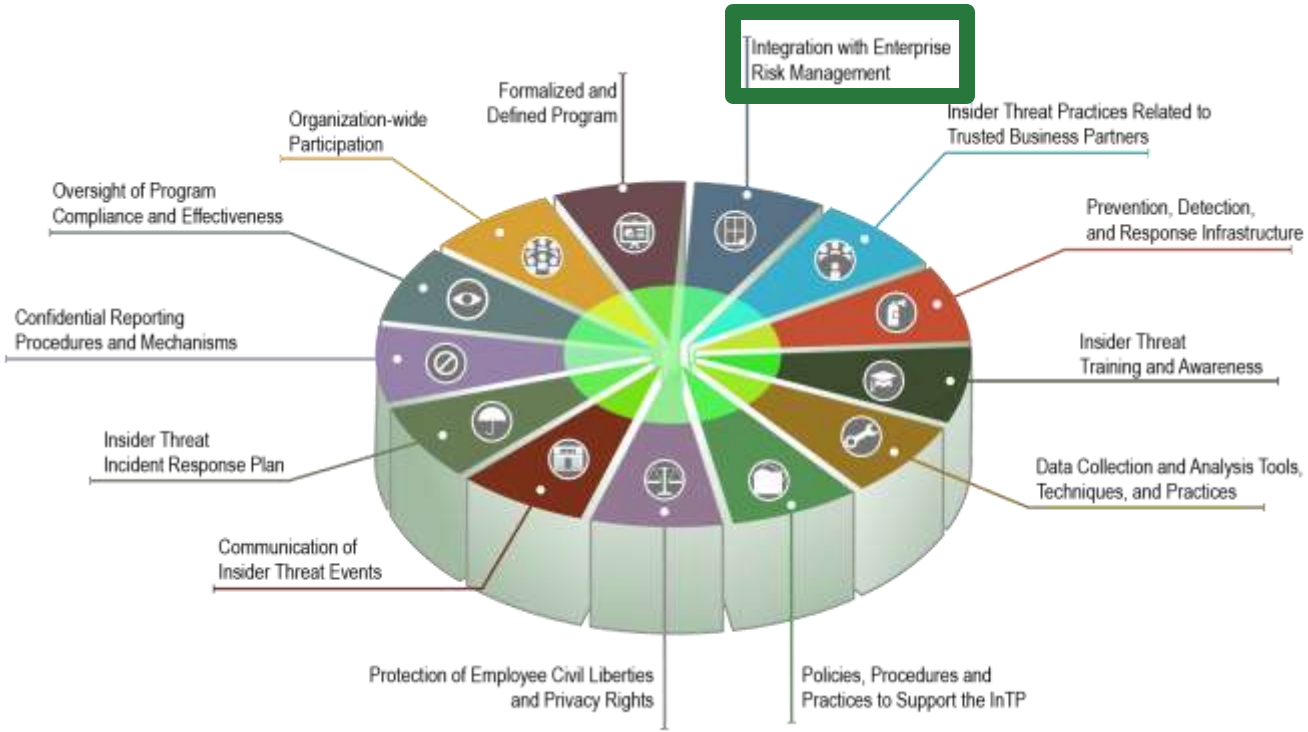
https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html

Building an Insider Threat Program



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

CERT InTP Key Components – It Starts With Risk Management



Recommended Best Practices for Insider Threat Mitigation

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 or search "cert common sense guide insider threat"

Engage with Us

Download software and tools

Participate in education offerings

Attend an event

Search the digital library

Read the SEI Year in Review

Explore our research and capabilities

Collaborate with the SEI on a new project

Contact Us

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479

info@sei.cmu.edu
www.sei.cmu.edu