Building an Effective Insider Risk Program

Randy Trzeciak

Deputy Director; CERT Division

Risk and Resilience Directorate

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.

DM22-0239

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

The CERT Insider Threat Center

Center of insider threat expertise

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

Insider Risk Management Principles

Untangling Insider Taxonomy

Insider: An *insider* of an organization is an employee, contractor, or other business partner who *has or had* authorized access to the organization's critical assets.

Insider Threat: *Insider threat* for an organization is the potential for an insider to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Insider Incident: Harm realized by an organization; either by a malicious or non-malicious insider.

Insider Risk: *Insider risk* is the potential for loss associated with the realization of an insider threat.

Insider risk is unique in organizational security in that the potential threat agents play fundamental roles in accomplishing the organization's mission.

True Story: IT Sabotage

911 services disrupted for 4 major cities

Disgruntled former employee arrested and convicted for this deliberate act of sabotage

True Story: Theft of IP

Research scientist downloads 38,000 documents containing his company's trade secrets before going to work for a competitor

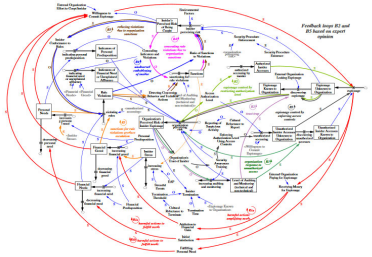
Information was valued at $400 Million

True Story: Fraud

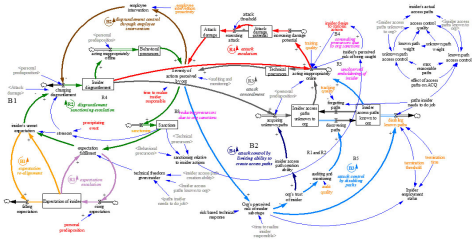
An undercover agent who claims to be on the “No Fly list” buys a fake drivers license from a ring of DMV employees

Insider Incident Types (not exhaustive)

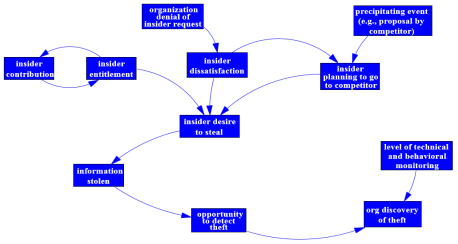
National Security Espionage



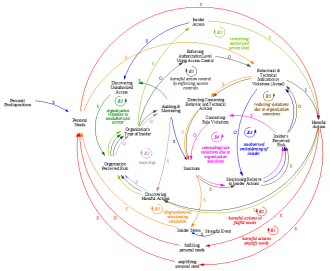
IT System Sabotage



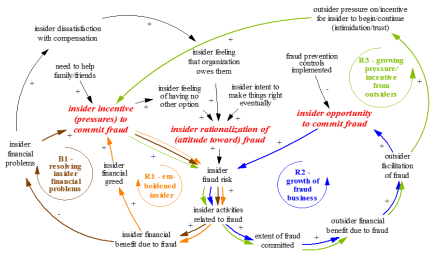
Theft of IP – Entitled Independent



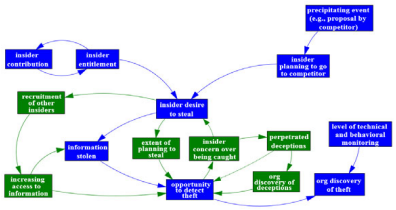
Espionage / Sabotage



Fraud



Theft of IP – Ambitious Leader



The Insider Threat

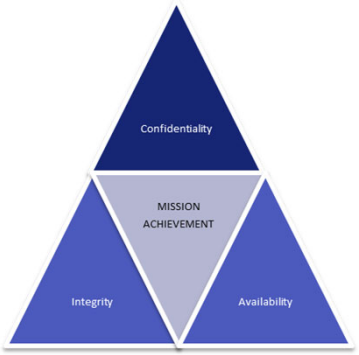
There are no insider threats that can be characterized as “one type”

Remember that the organization’s critical assets include:

- **People**
- **Information**
- **Technology**
- **Facilities**

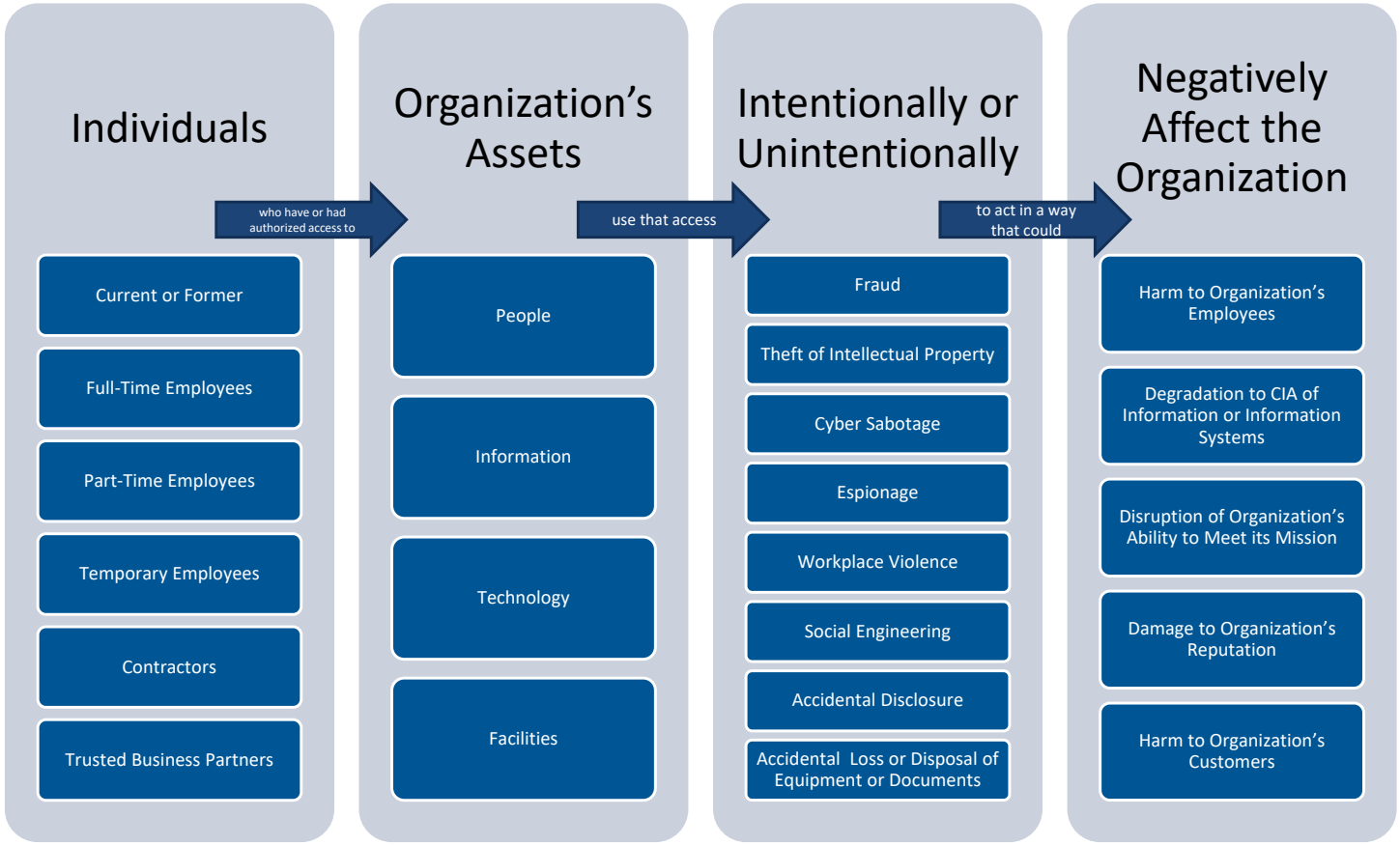
Insider threat can be based on the motive(s) of the insider

Impacts to **Confidentiality, Integrity, and Availability** are possible

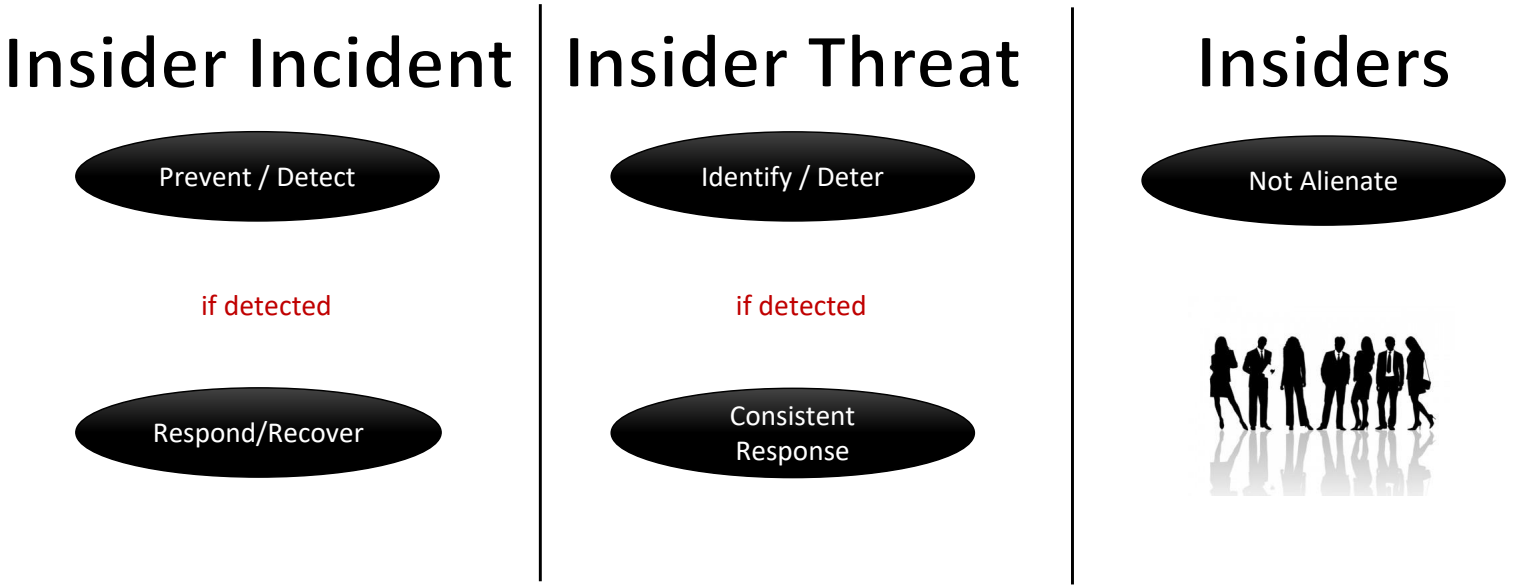


Cyber Attack = Cyber Impact
Physical Attack = Physical Impact
Cyber Attack = Physical Impact
Physical Attack = Cyber Impact

What / Who is an Insider Threat?



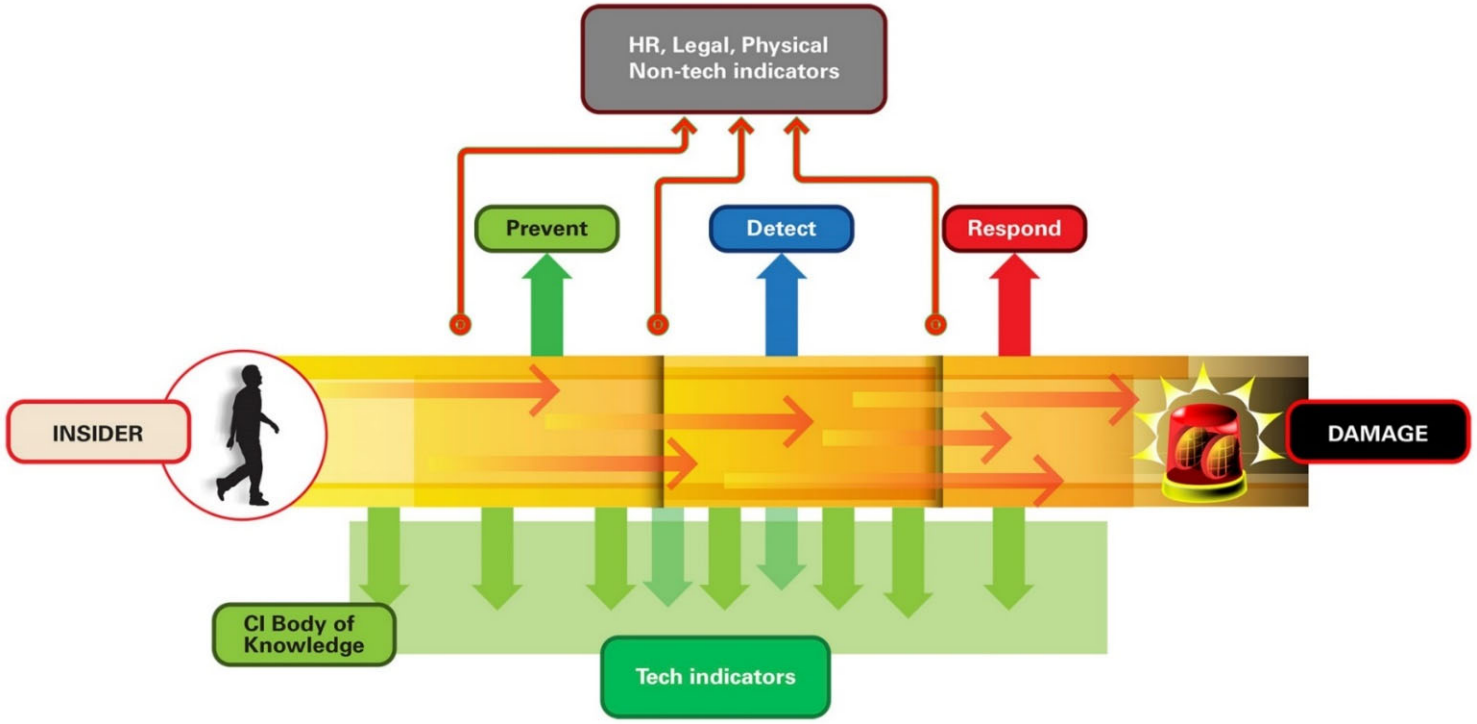
Insider Threat Mitigation



Insider Threat Program

Building an Insider Threat Program

The Goal for an Insider Risk (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

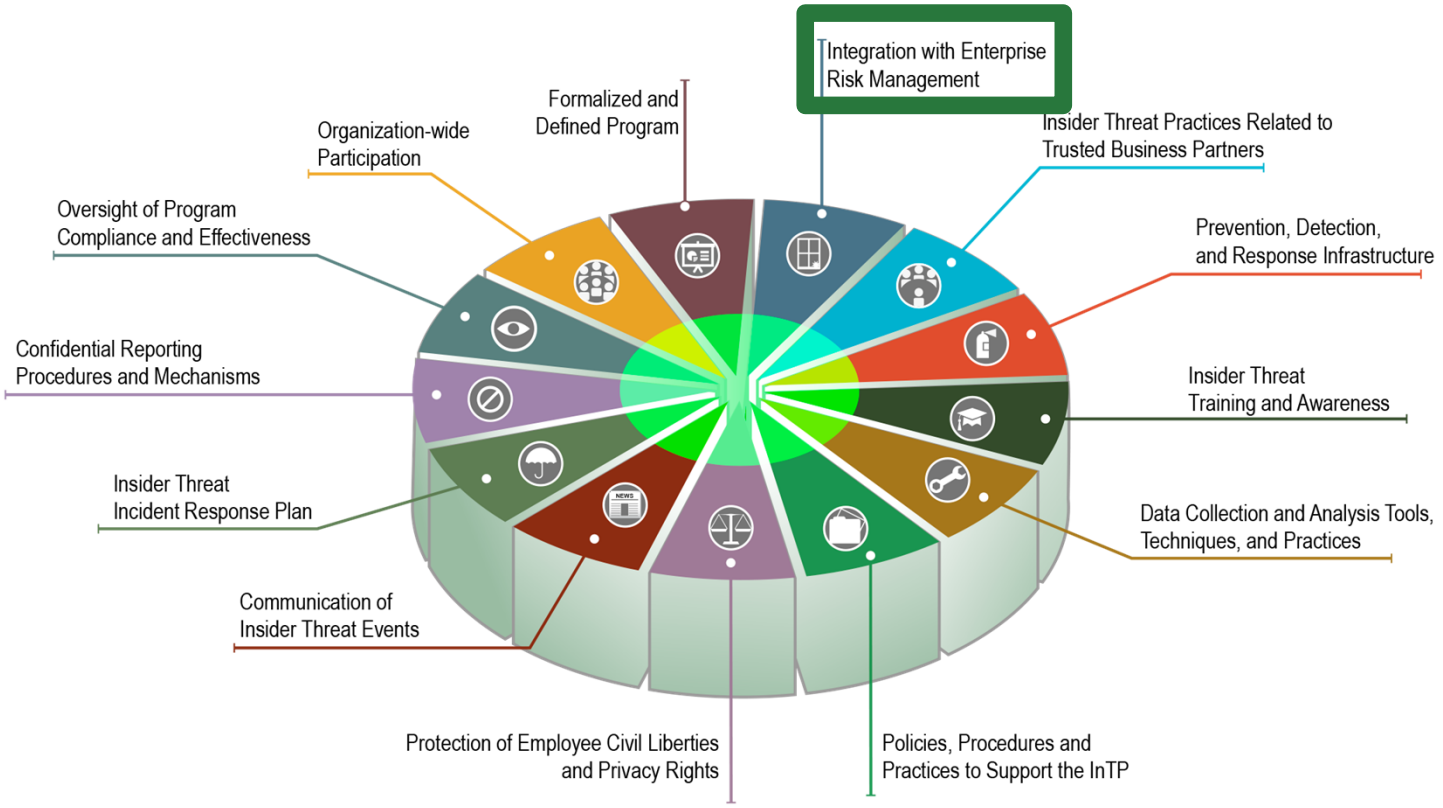
What is an Insider Risk (Threat) Program?

The CERT *Common Sense Guide to Mitigating Insider Threats 7th Edition* defines an insider threat program (InTP) as an enterprise-wide program with

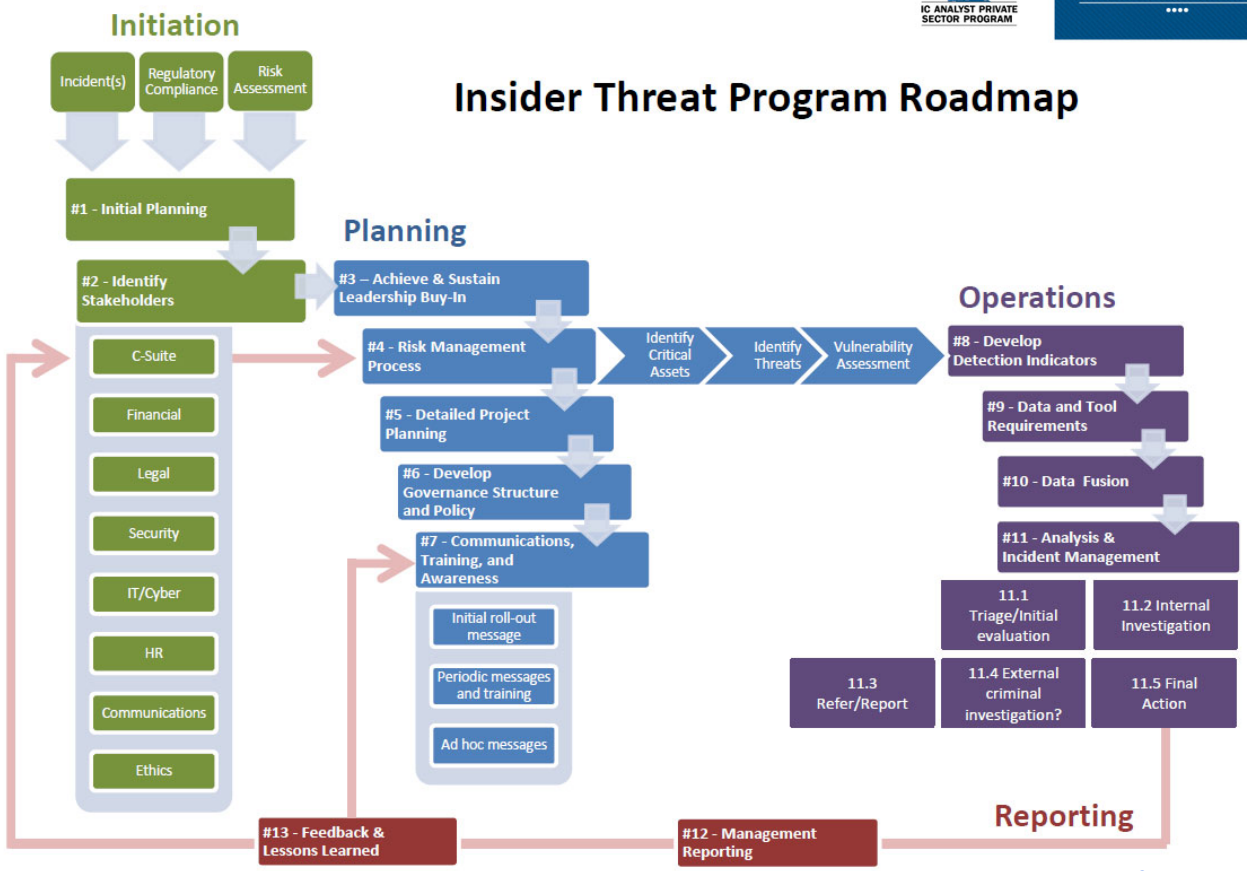
- an established vision
- defined roles and responsibilities for those involved
- specialized awareness and training for all involved
- criteria and thresholds for
  - data collection and analysis
  - declaring insider threat activity and risks
  - conducting inquiries
  - referring to investigators
  - requesting prosecution
- supporting policies, procedures, and practices
- a process to ensure privacy and confidentiality
- management's support

https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

CERT InTP Key Components – It Starts With Risk Management

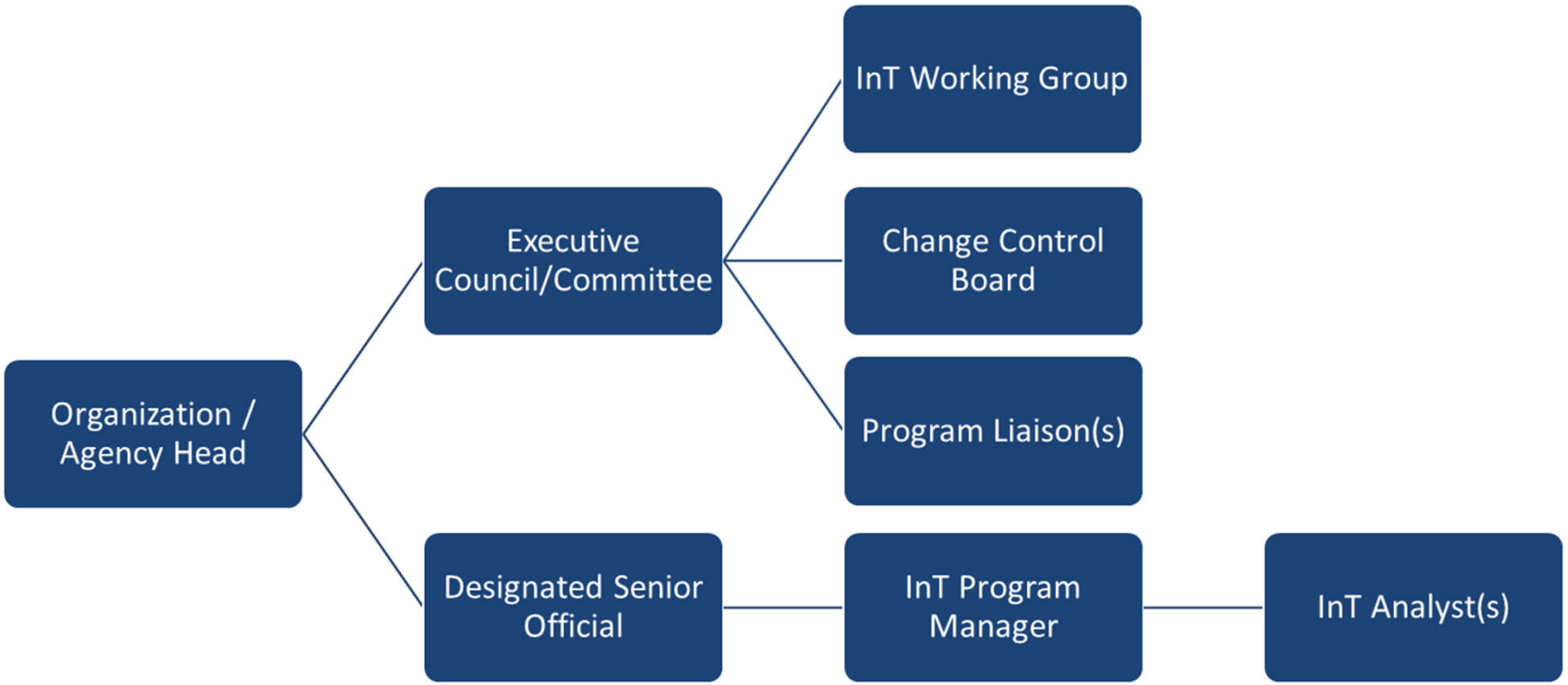


Building an Insider Threat Program

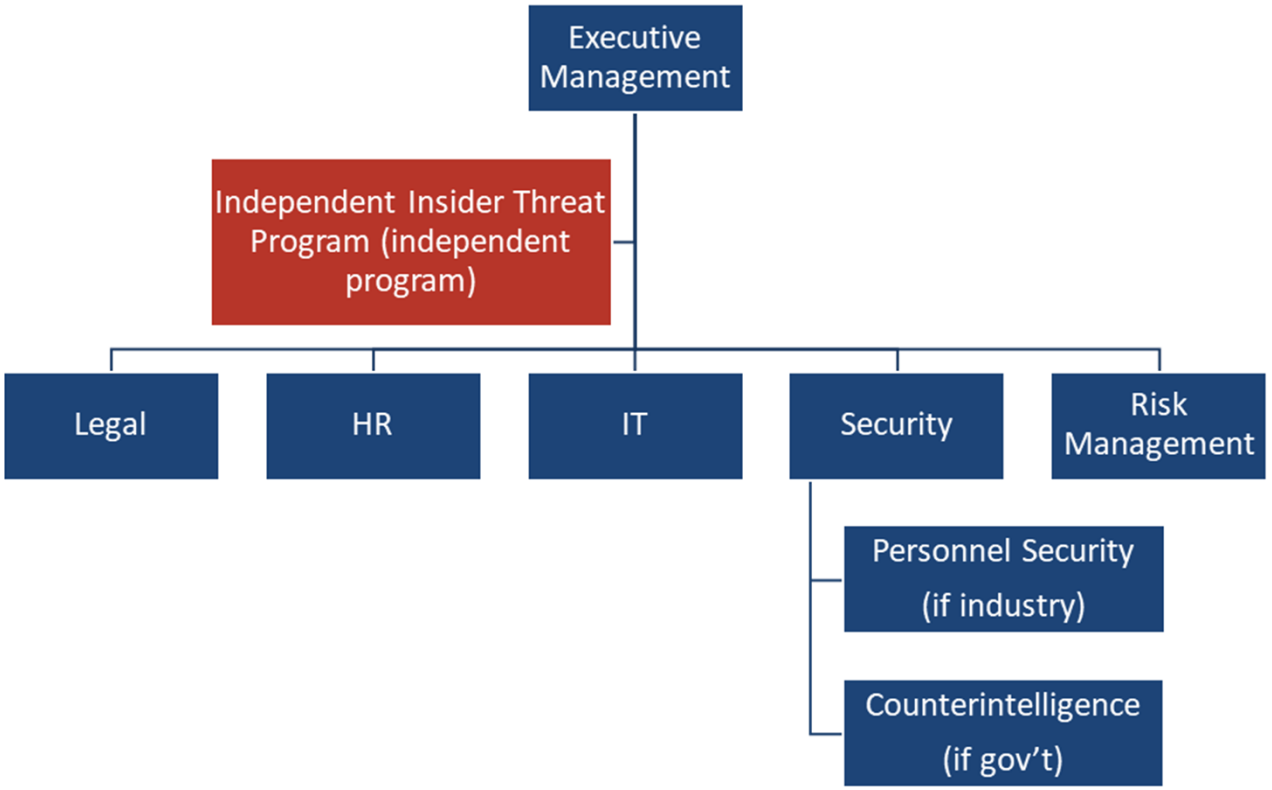


Source: https://www.insaonline.org/insider-threat-roadmap/

Notional InTP Organizational Structure



Potential Reporting Structure



Common Documents to Build an InTP

There are a core set of documents that most organizations need in order to formalize the InTP:

- Insider Threat Policy (*you will*)
- Insider Threat Charter (*you will what*)
- Concept of Operations (CONOPS) (*you will how*)
- Implementation Plan (*how you will get there*)
- Incident Response Plan (*what to do when something happens there*)
- Communications Plan (*who/how to tell what happened there*)

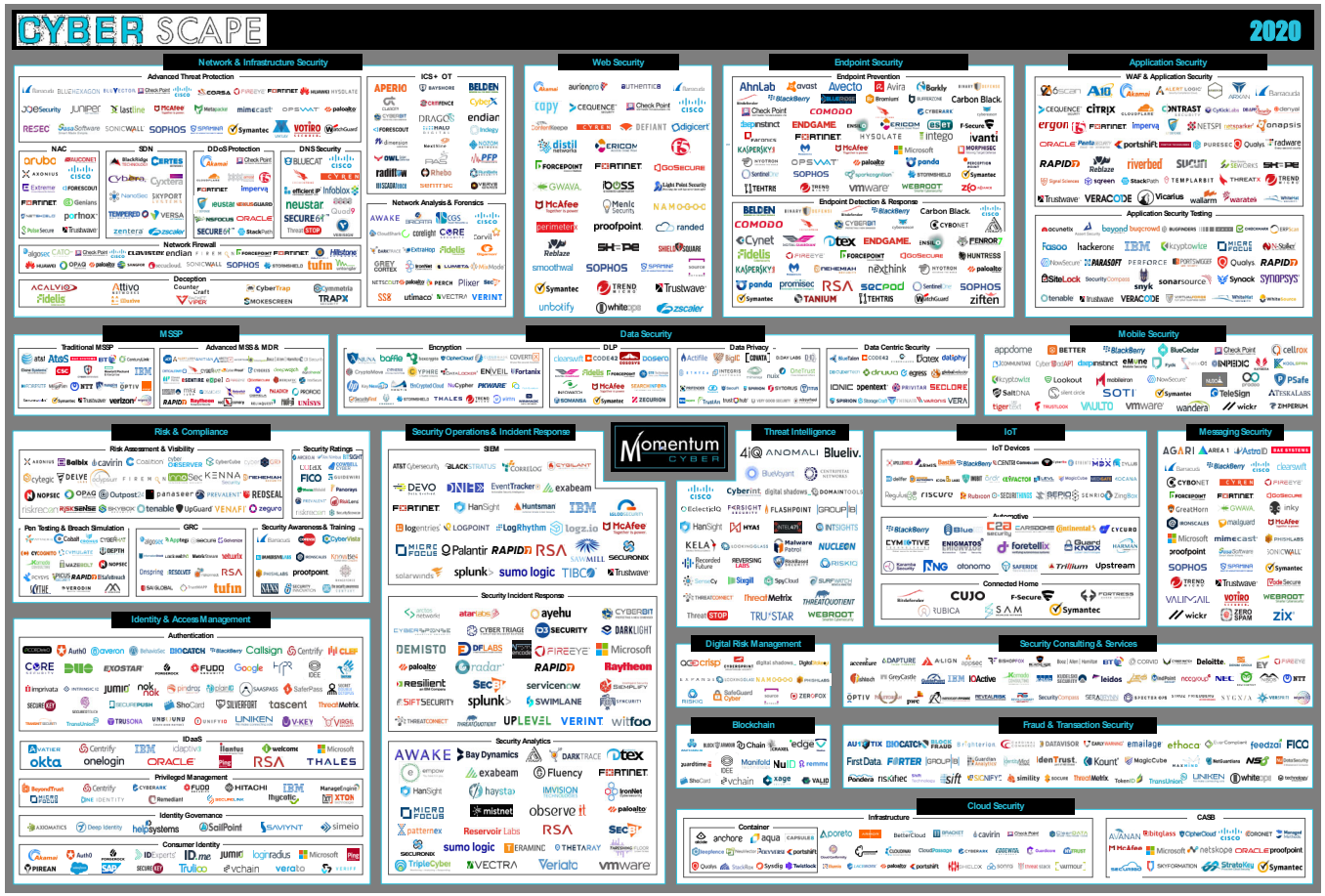
Run Everything Through Legal/Privacy

Before creating these documents:

- Work with legal counsel and privacy officers in the development of the InTP
- Make sure both groups have ongoing involvement with process/procedures involving investigations and dispositions of inquiries.
- Ensure that all InTP actions meet legal mandates and protect the rights and privacy of employees.

Insider Threat Tools

The Tool Landscape Is Vast



Purpose of Tools

Tools provide two main purposes

- Main Insider Threat Hub tools
  - Data Loss Prevention (DLP)
  - Security Incident and Event Management (SIEM)
  - User Activity Monitoring (UAM)
  - User/Entity Behavioral Analytics (UEBA)
- Supporting tools
  - Digital Forensics
  - Analytics
  - Identity Management (IAM/PAM)

Best Practices for the Mitigation of Insider Threats

Recommended Best Practices for Insider Threat Mitigation – 7th Edition

1 - Know and protect your critical assets.	12 - Deploy solutions for monitoring workforce member actions and correlating information from multiple data sources.
2 - Develop a formalized insider risk management program.	13 - Monitor and control remote access from all endpoints, including mobile devices.
3 - Clearly document and consistently enforce administrative controls.	14 - Establish a baseline of normal behavior for both networks and workforce members.
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 trusted external entities 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 – Mitigate unauthorized data exfiltration.
9 - Incorporate insider threat awareness into periodic security training for all workforce members.	20 - Develop a comprehensive workforce member 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.	22 – Learn from past insider threat incidents.

CERT Common Sense Guide to Mitigating Insider Threats , Seventh Edition

For More Information (Insider Risk)

The Common Sense Guide to Mitigating Insider Threats, Seventh Edition

Balancing Organizational Incentives to Counter Insider Threat

Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program

Insider Threats Across Industry Sectors

Insider Threat Program Manager Certificate

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

Analytic Approaches to Detect Insider Threats

Workplace Violence & IT Sabotage: Two Sides of the Same Coin?

SEI – Our Work – Insider Threat

Wrap Up

Open-Source Insider Threat (OSIT) Information Sharing Group

Open-Source Insider Threat (OSIT) Information Sharing Group

Community of Interest for insider threat program practitioners across industry organizations

Over 500 members from ~250 organizations

Special interest groups around sectors (banking/finance) and sub-topics(data analytics)

Monthly Telecons
- Tool Vendor Demos

Bi-annual In-Person Meetings
- Hosted by various members of the group

To join, contact: rft@cert.org

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
USA

Randy Trzeciak
Director, National Insider Threat Center
+1 412 268-7040
rft@cert.org

https://sei.cmu.edu/our-work/insider-threat