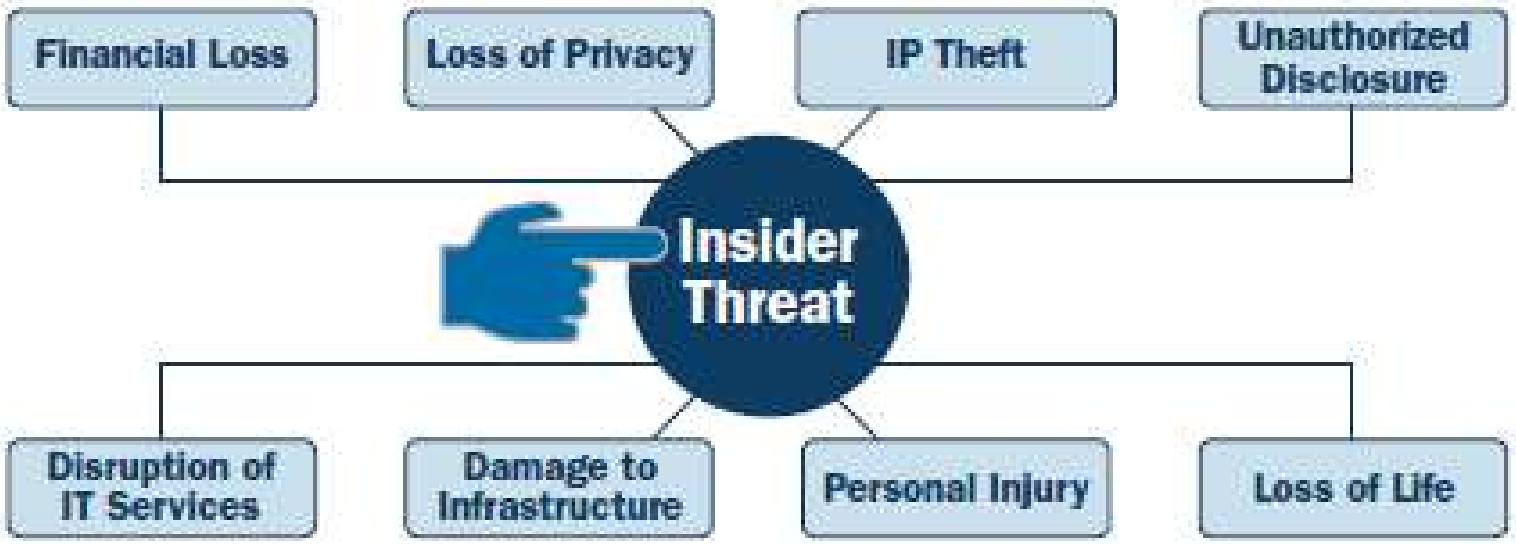
MITIGATING INSIDER THREATS

Cyber and Infrastructure Security Agency

Insider Threat

The **potential** for an insider **to use** their **authorized access** or **special understanding** of an organization **to harm** that organization.



Insider

An **insider** could be an employee, member, contractor, vendor, janitor, repairman, investor, client, family member, associate, or security.

- **A person given a badge or access device**
- **A person given computer or network access**
- **A person who develops products and services**
- **A person with knowledge of the organization's fundamentals, business strategies, and goals**
- **A person with privileged access to protected information**

You work with, talk to, pass by, and see insiders every day.

Threat Types and Expressions

Unintentional and Intentional

Violence

- Terrorism and Workplace/Organizational

Espionage

- Economic, Government, and Criminal

Sabotage

- Physical and Virtual

Theft

- Intellectual Property and Financial Crime

Cyber

- Unintentional and Intentional

Identifying the Threat

No standard profile – impacted by:

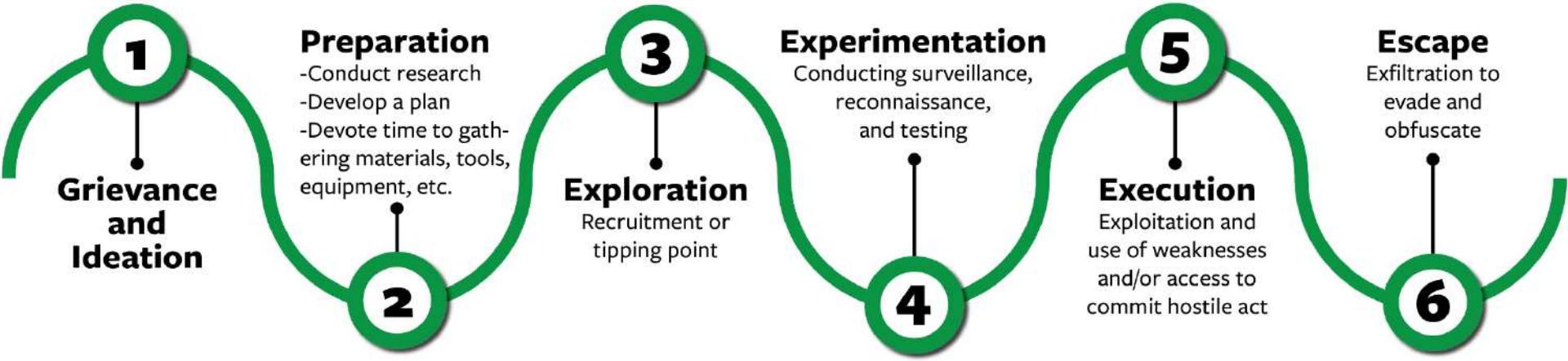
Personal Predispositions - Contextual Stressors - Patterns of Suspicious Behaviors and Actions

Seldom act impulsively

Moving from Idea to Action

Red flags involve changes in baseline behavior

Usually exhibit observable patterns

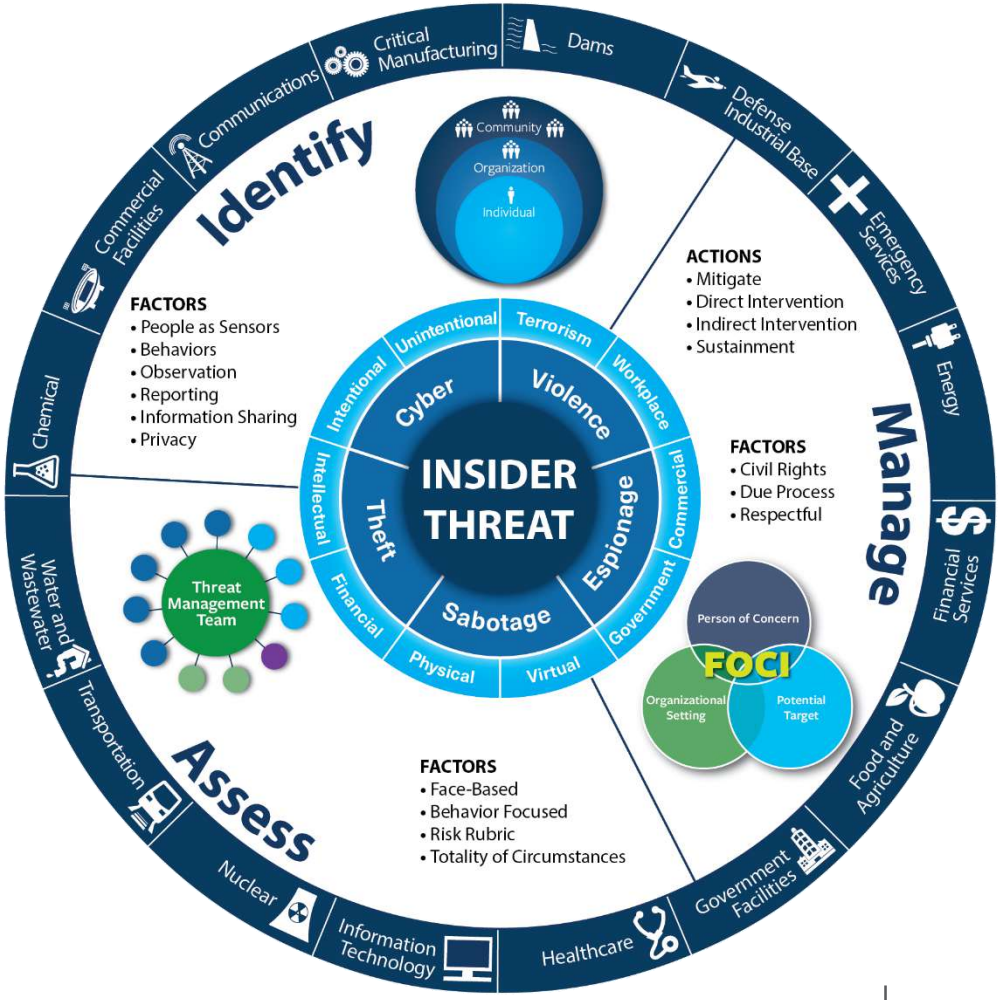


Indicators

Personal	• Predispositions • Personal stressors • Professional stressors
Background	• Patterns of previous behavior
Behavioral	• Observable actions or behaviors • Change from “normal”
Technical	• Require IT systems and tools to detect • Email / Social media use • Network access and behaviors
Environmental	• Impact of organizational actions • Can motivate or trigger a hostile act

Insider Threat Framework

- **Prevention** is the preferred course of action
- Provide tools to **help insiders** before they make a mistake
- Not a "**gotcha**" program – help deter harmful and illegal behavior to the organization, its resources, or its members
- Every organization must **Detect and Identify**, **Assess**, and **Manage** potential insider threats



Insider Threat Reporting

- Create a culture of shared responsibility, connection, and respect
- Develop an anonymous/confidential reporting system
- Take steps to ensure bystander reporting is valued and treated with discretion (in policy and practice)
- Emphasize the purpose of reporting is to help the individual who may be a potential threat
- Act when threats are reported so employees know reports are taken seriously

Managing Insider Threats

Threat Management Team:

Threat Management Strategies:

- Are holistic
- Leverage multiple concurrent intervention strategies
- Short-term or long-term
- Active or passive engagement
- Require continual reassessment, adjustment, and follow-through
- Allow each team member to offer a solution
- May not work as planned
- Must be flexible and sustainable

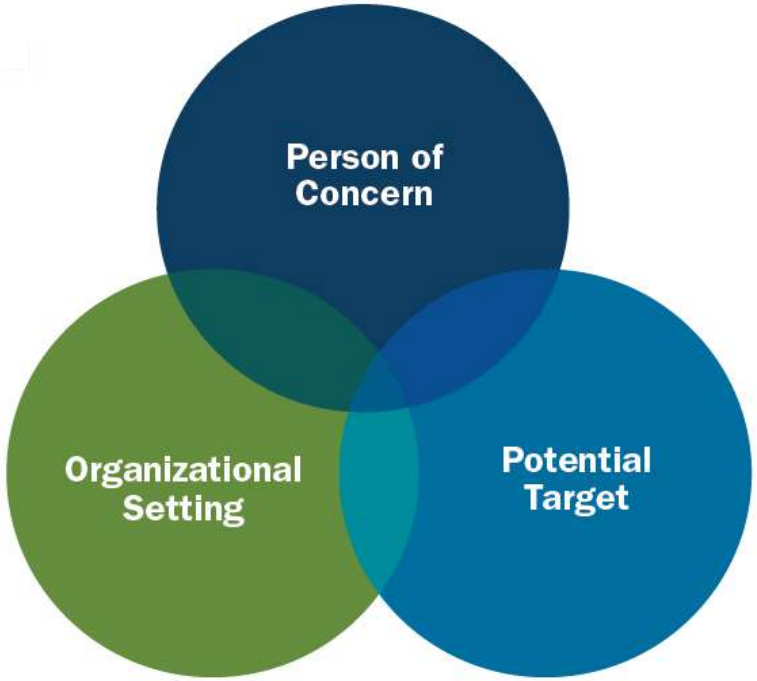
Protecting the organization and its people is the ultimate goal.

Managing Insider Threats

Goal is to help the person of concern, prevent insider threat incidents, and mitigate effects

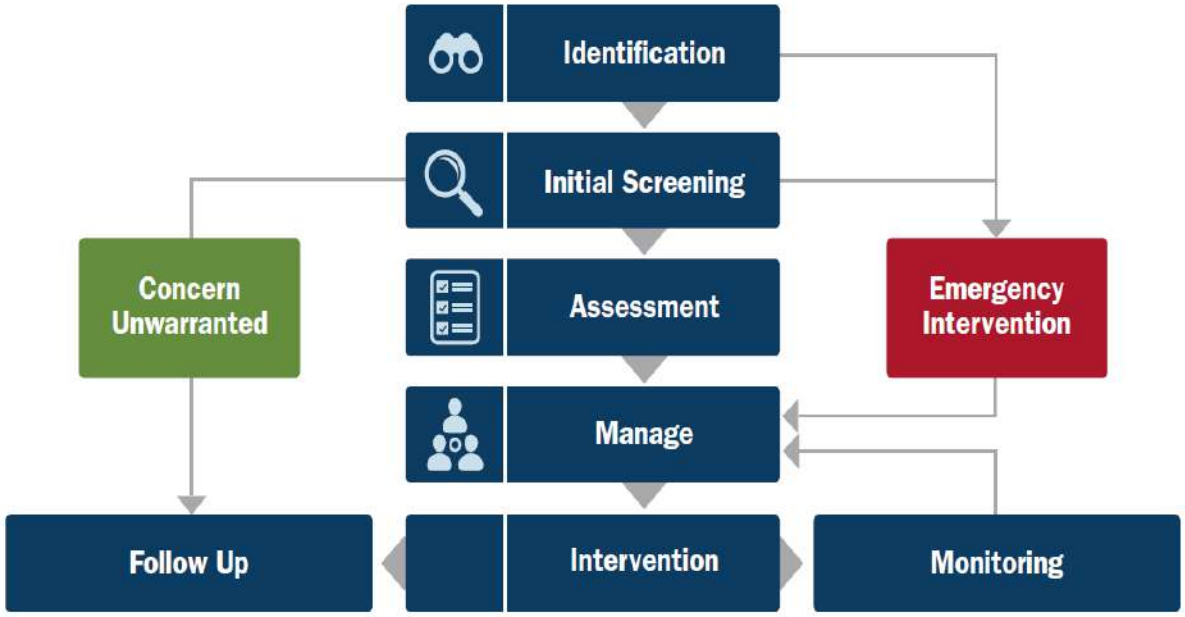
Management Strategies:

- Are holistic
- Sometimes require multiple concurrent intervention strategies
- Short-term or long-term
- Active or passive
- Require continual reassessment, adjustment, and follow-through
- Allow each team member to offer a solution
- May not work as planned
- Must be flexible and sustainable



Threat Assessment Process

- Standardized, repeatable, defensible
- Pre-established set of operational activities employed by TMT
- Combines investigative process and information-gathering
- Applies in both urgent/emergency situations and in non-urgent/non-emergency situations



Preventing the Next Insider Threat

1

Train employees to recognize behaviors that indicate a progression

2

Instill a positive culture for reporting

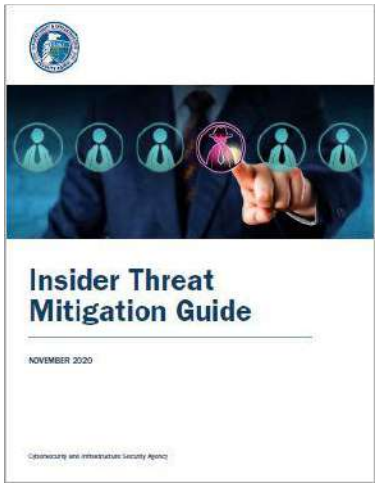
3

Establish Threat Management Team and develop intervention capabilities

Awareness + Action = Prevention

CISA Resources

- Insider Threat Mitigation Guide



- Insider Threats 101- What You Need to Know

- Human Resources' Role in Preventing Insider Threats

www.cisa.gov/insider-threat-mitigation

David Johnston
Protective Security Advisor

david.johnston@cisa.dhs.gov
202.597.4518


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY