

MITIGATING INSIDER THREATS



Cyber and Infrastructure Security Agency

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.



FEDERAL NETWORK PROTECTION



PROACTIVE CYBER PROTECTION



INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS



EMERGENCY COMMUNICATIONS



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



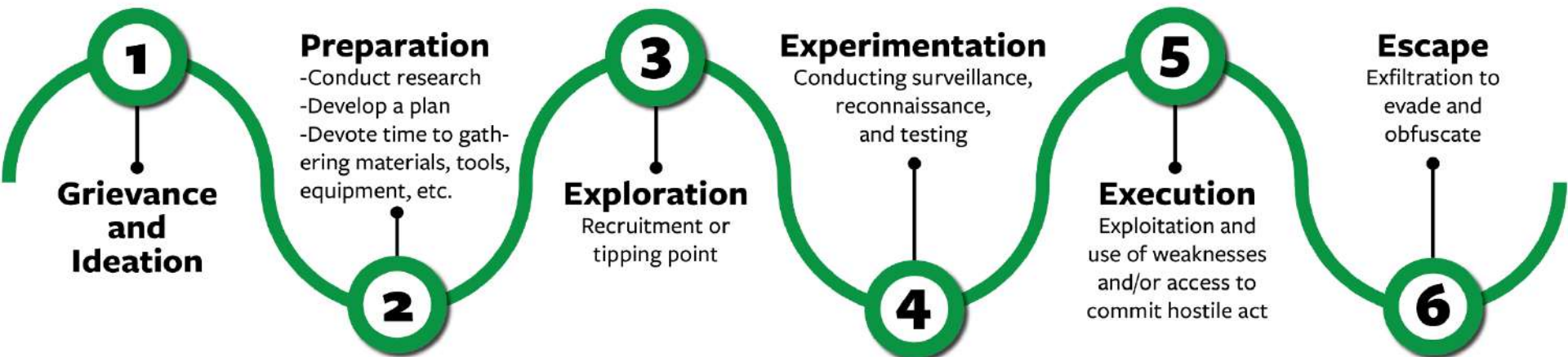
Moving from Idea to Action



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

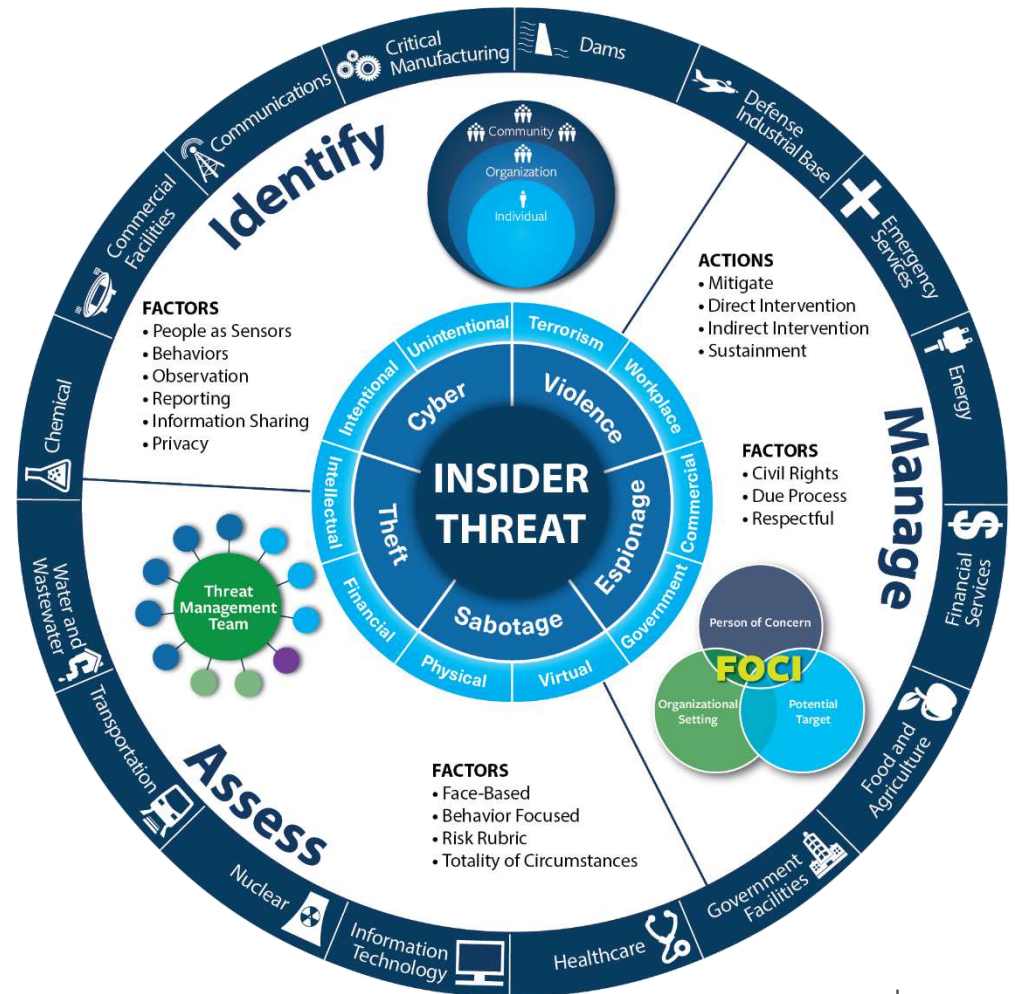
Environmental

- 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

Notice the Incident or Event

Recognize it as a Problem

Assume Responsibility

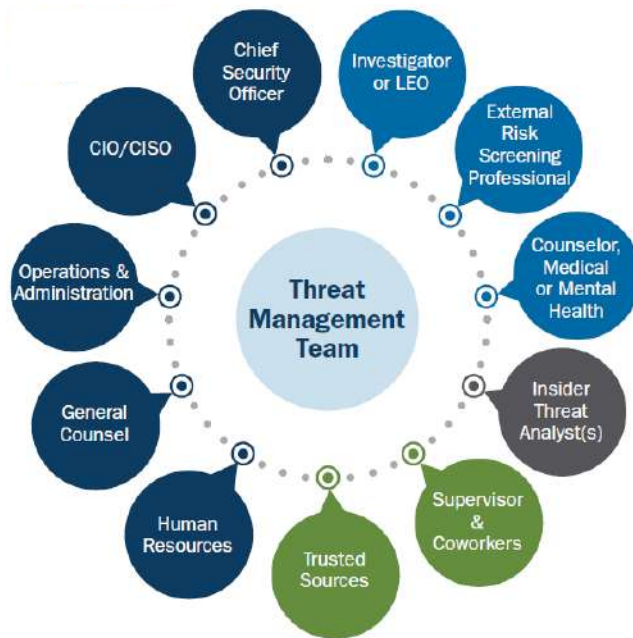
Know How to Help

Act



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

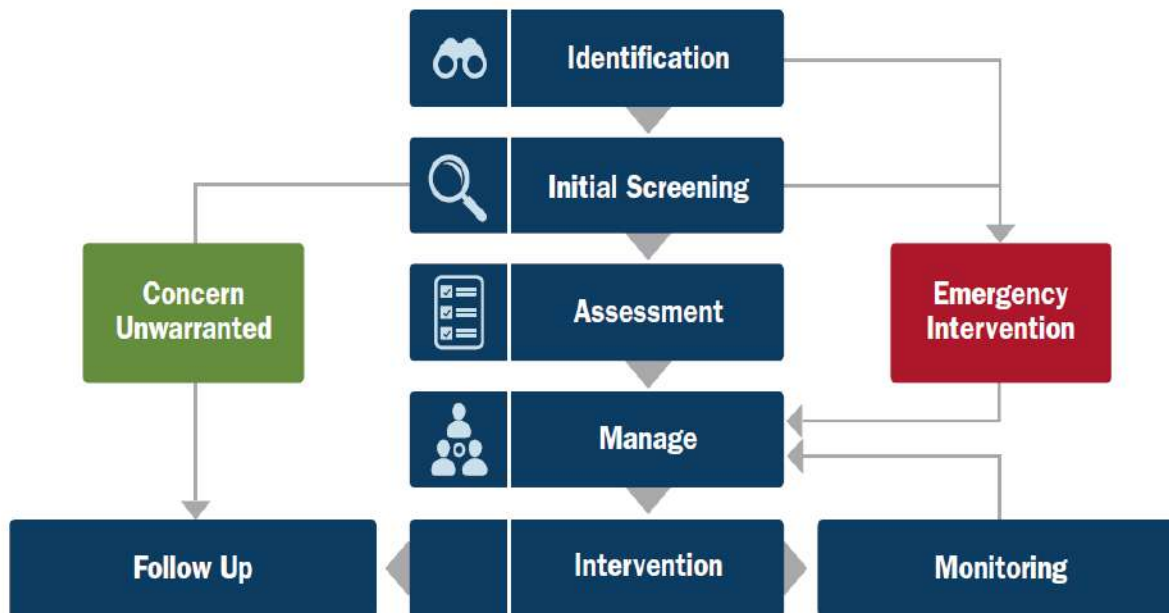
Management Strategies:

- 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

INSIDER THREATS 101
WHAT YOU NEED TO KNOW

OVERVIEW
Organizations of all sizes are vulnerable to an insider threat. An insider threat is the potential for an individual to use their authorized access or special understanding of an organization to harm that organization. This term can include malicious, negligent, or inadvertent acts that negatively affect an entity's integrity, confidentiality, and availability of the organization's data, systems, facilities, and business operations.

RELEASING AN INSIDER THREAT MITIGATION PROGRAM
Successful insider threat mitigation programs employ practices and systems that limit or monitor access points, organizational functions, and threat detection programs needed to detect and respond to insider threats. Regular access reviews, access audits, and employee training are key to success. The potential consequences of an insider threat. Organizations should have a multi-layered threat management team to create an effective response plan, ensuring their response to an insider incident or potential threat is coordinated, repeatable, and consistently applied.

How to Support Your Organization's Security

- Identify and mitigate high-risk activities and systems.
- Develop a robust insider threat program designed to detect, prevent, and respond to insider threats.
- Develop a culture of shared responsibility designed to help the individual and the organization succeed.
- Develop a robust insider threat program designed to detect, prevent, and respond to insider threats.
- Develop a culture of shared responsibility designed to help the individual and the organization succeed.

Insider Threat Quick Facts

- More than 100 million employees are at risk of an insider threat.
- \$4.45 billion in damages from insider threats in 2019.
- 90% of all insider threats are preventable.
- 2 million people are at risk of an insider threat.
- 25% of all insider threats are preventable.

CISA | DEFENDING ROYALTY SECURITY TOMORROW

Insider Threat Mitigation Guide

NOVEMBER 2020

Cybersecurity and Infrastructure Security Agency

HUMAN RESOURCES' ROLE IN PREVENTING INSIDER THREATS

OVERVIEW
The insider is a dynamic, man-made threat to an organization's personnel and critical information. Along with their security counterparts, human resources (HR) professionals play an integral role in detecting and responding to insider threats. HR management teams, in conjunction with other organizational teams, are responsible for identifying and mitigating insider threats. As a critical component of an organization's overall security posture, HR professionals are best positioned to detect and prevent insider threats. HR professionals can help to identify potential threats and prevent them from occurring. HR professionals can help to identify potential threats and prevent them from occurring. HR professionals can help to identify potential threats and prevent them from occurring.

FACTS & FIGURES

- In January 2020, an insider threat was the most common cause of a data breach, according to a report by Verizon's Data Breach Investigations Report (DBIR).
- In 2019, 90% of all insider threats were preventable.
- In 2019, 25% of all insider threats were preventable.

POTENTIAL INDICATORS
Insider threat security policies are not enough to prevent insider threats. HR professionals should be aware of potential indicators of insider threats. HR professionals should be aware of potential indicators of insider threats. HR professionals should be aware of potential indicators of insider threats.

CISA | DEFENDING ROYALTY SECURITY TOMORROW





www.cisa.gov/insider-threat-mitigation

David Johnston
Protective Security Advisor

david.johnston@cisa.dhs.gov
202.597.4518

