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 insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources.

BUILDING AN INSIDER THREAT MITIGATION PROGRAM

The Cybersecurity and Infrastructure Security Agency (CISA) assists critical infrastructure stakeholders with building or expanding their insider threat mitigation programs. Successful insider threat mitigation programs employ practices and systems that limit or monitor access across organizational functions. Insider threat mitigation programs need to be able to detect and identify improper or illegal actions, assess threats to determine levels of risk, and implement solutions to manage and mitigate the potential consequences of an insider incident.

Organizations should form a multi-disciplinary Threat Management Team to create an Incident Response Plan, ensuring their response to an insider incident or potential threat is standardized, repeatable, and consistently applied.

To effectively establish an insider threat management program, organizations should:

Obtain Support from Organizational Leadership

Start small—leverage existing capabilities and resources.

Define the purpose of the program, and highlight the return on investment by revealing what could be lost in a successful insider threat incident.

Identify what the organization values, and its physical and intellectual critical assets to protect against insider threats.

Maintain Pathways for Reporting

Develop a culture of shared responsibility designed to help the individual and the potential insider.

Develop confidential reporting pathways that are easy to find, understand, and use.

Provide Training and Awareness

Train employees to recognize insider threat indicators and the concerning behaviors that could lead to an incident in the organization.

INSIDER THREAT QUICK FACTS

The total average cost of an insider risk increased in 2023 to

$16.2 million per organization

(taking an average of 86 days to identify and contain)

Source: Ponemon 2023 Insider Threat Report, *2023 Cost of Insider Risks Global Report*

90%

of cybersecurity professionals believe their organizations are vulnerable to insider threats

Source: Crowd Research Partners, *Insider Threat 2018 Report.*

$121 billion

was the estimated annual nationwide cost of workplace violence in 2021

Source: National Safety Council, Workplace Violence, *A Universal Threat, 2022*

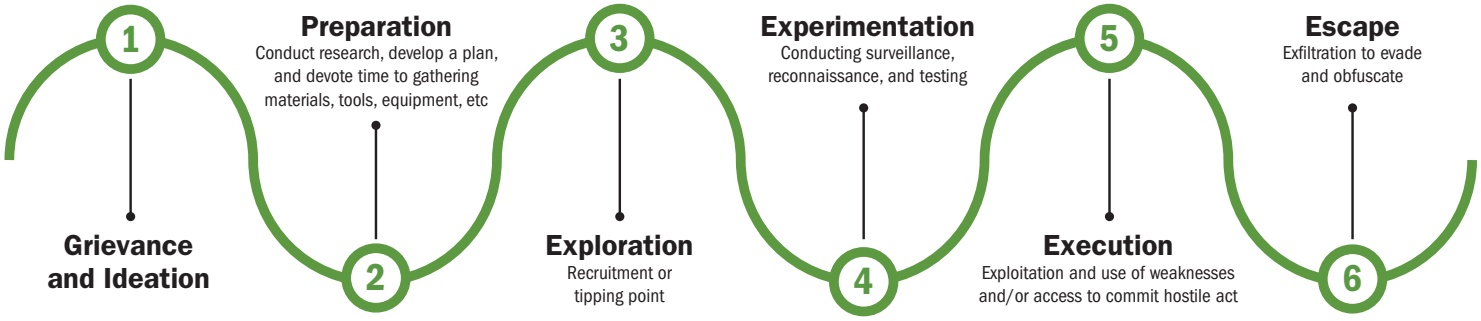
25%

of workplace violence goes unreported

Source: AlertFind, *Workplace Violence Statistics 2018*

PROGRESSION OF AN INSIDER TOWARD A MALICIOUS INCIDENT

Malicious insider activity is rarely spontaneous; it is usually the result of a deliberate decision to act. A potential insider threat progresses along an identifiable pathway to a malicious incident.[1] A deeply held grievance or humiliation, whether real or perceived, is often the first step on a journey toward intended violence.[2]



> Everybody is the insider threat team, not just the police or security personnel. It is everyone's responsibility to keep the agency and the mission safe."
>
> – GOVERNMENT SUBJECT MATTER EXPERT
> (FROM A "STRATEGIC PLAN TO LEVERAGE THE SOCIAL & BEHAVIORAL SCIENCES TO COUNTER THE INSIDER THREAT," PERSEREC OPA-2018-082)

ADDITIONAL RESOURCES

Learn more about Insider Threats with some of our other resources below.

INSIDER THREAT MITIGATION GUIDE

INSIDER RISK MITIGATION PROGRAM EVALUATION

HR'S ROLE IN PREVENTING INSIDER THREATS

INSIDER THREAT MITIGATION WORKSHOP

For direct regional support, please visit cisa.gov/about/regions.

For additional Insider Threat resources and other Infrastructure Security products and information, please visit cisa.gov/insider-threat-mitigation.

1. Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 24). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Retrieved from fbi.gov/file-repository/making-prevention-a-reality.pdf/view.
2. Grievance as used here should be distinguished from the formal filing of a grievance by an employee based upon instances of discrimination or other inappropriate workplace conduct directed at them. The filing of a formal grievance should not be construed as indicative of an insider threat.