HUMAN RESOURCES' ROLE IN PREVENTING INSIDER THREATS

OVERVIEW

Insider threats are a dynamic, ever evolving challenge to organizations. Along with their security counterparts, Human Resources (HR) professionals play an integral role in developing and contributing to multi-disciplinary threat management teams to effectively detect, deter, and mitigate insider threats.[1] As a central repository for personnel information, HR professionals are likely to identify patterns, behavior, and trends that will help mitigate potential harm to an organization and its employees. Depending upon the type and size of the organization, the financial and reputational losses associated with insider threats could cost millions annually.

An insider threat may be a current or former employee, business partner, or contractor who intentionally or unintentionally causes harm to an organization and its personnel using either physical or cyber-based methods:

Violence: Terrorism and workplace violence.

Espionage: Theft of a company's intellectual property associated with national security.

Cyber: Intentional or unintentional intrusions that breach or expose an organization's information technology infrastructure.

Sabotage: Physical or cyber acts that impact an organization's ability to function through subversion, obstruction, disruption, or destruction.

Theft: Stealing an organization's physical property, intellectual property, and/or financial information.

POTENTIAL INDICATORS

Whether negligent or malicious, insider threats pose serious security risks to an organization. The ability to proactively evaluate, identify, and mitigate workforce issues is crucial to ensuring a safe workplace. Knowing and recognizing the warning signs posed by malicious insiders is critical to prevention and mitigation. These potential warning signs or indicators may include, but are not limited to:

- Conflicts with co-workers or supervisors; chronic violation of organizational policies.
- Non-compliance with mandatory security training assignments.
- Disciplinary actions – suspensions, reprimands, removals, or reduction in title or pay.
- Use of social media to threaten the organization or its personnel.
- Observable or vocalized stressors, which may include personal, professional, financial, or unmet expectations that could increase the risk of an insider taking hostile or malicious action.

FACTS & EVENTS

- Between 2019 and 2022, while employed as a rehab manager for a local hospital, a Hospital Manager used a corporate credit card to make unauthorized purchases of prepaid credit and gift cards. He then converted funds from the fraudulently obtained cards to his personal accounts to conceal the scheme, make personal purchases, and withdraw large amounts of cash to gamble at casinos. Over that time period, over $607,000 was stolen and laundered.
- From June 2021 through May 2023, an employee of a city law department stole checks, including checks made payable to the law department's worker's compensation division. He then passed those checks onto other people, who deposited or attempted to deposit forged, altered, and fraudulently endorsed versions of those checks into third parties' bank accounts. Approximately 40 checks, totaling about $600,000, were stolen and deposited as part of the scheme.
- In April 2021, eight people were killed in a mass shooting by a former employee at a shipping facility in Indianapolis, Indiana. A year earlier, the former employee's mother contacted law enforcement to report he might try to attempt "suicide by cop" according to the FBI.

1 A threat management team is a multi-disciplinary governing body that includes representatives from HR, information technology, information security, physical security, legal, and other departments who focus on identifying, assessing, and mitigating potential insider threats.

MITIGATION STRATEGIES AND PROTECTIVE MEASURES FOR HUMAN RESOURCES

HR professionals should establish an evaluation framework that includes threat indicators and behavioral signals. HR departments play a critical role, as they are involved in all phases of an employee's work lifecycle: pre-employment, employment, and termination/post-employment.

ACCESS, PLANNING, AND PERSONNEL

Pre-Employment (Screening/Hiring)

- Probe red flags during the interview process, but be mindful not to violate relevant privacy or "ban the box" laws (state protections for prospective employees convicted of a crime against automatic disqualification).
- Verify accuracy of a potential hire's resume and contact references.
- Screen for potential negative indicators, including:
  - Past and relevant criminal activity (e.g.,conduct criminal background checks)
  - Reports of past violence
  - History of policy violations

Employment (including promotions and reassignments)

- Conduct routine, mandatory insider threat physical security and cybersecurity awareness training.
- Communicate clear organizational policies and follow established procedures.
- Create mechanisms for employees and managers to provide two-way feedback and share concerns.
- Establish a baseline of normal behavior for both employees and IT networks to help identify significant changes, including monitoring network activity for dangerous/inappropriate activity.
- Create a culture of shared responsibility, connection, and respect by ensuring that bystander-reporting is valued and treated with discretion while emphasizing that the focus is on helping your co-workers.
- Address potential grievances.
- Identify and report concerning behavioral changes to the Threat Management Team and appropriate departments.

Termination/ Post-Employment

- Deliver notifications of termination respectfully and in a manner that minimizes intrusiveness and embarrassment.
- Conduct an exit interview to gauge the separating employee's perspective.
- Have a plan to retrieve employee's personal belongings and to terminate their physical and digital access.
- Establish a procedure to inform other employees when termination occurs.
- Review intellectual property/nondisclosure agreements with the separated employee.
- Treat the separating employee with dignity and professionalism

ADDITIONAL RESOURCES FOR OWNERS AND OPERATORS

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

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