IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

HUMAN RESOURCES' ROLE IN PREVENTING INSIDER THREATS

OVERVIEW

The insider is a dynamic, ever-evolving threat to an organization's personnel and critical information. 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 attacks 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.

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

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

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

POTENTIAL INDICATORS

Insider threat security practices are shifting from developing profiles of perpetrators to observing behaviors over time. 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

- In February 2019, an employee at an Illinois-based factory opened fire on his co-workers after his notice of termination, killing five co-workers, and wounding another employee and five law enforcement officers. The incident, deemed workplace violence by investigators, also found that the perpetrator had a history of domestic assault, which was not revealed by the initial employment screening.
- In June 2018, a lawsuit brought by a major automaker accused a former employee of sabotaging manufacturing operations by stealing trade-secret information that was sent to an unnamed third party and making false statements intended to harm the company. Prior to the alleged actions, the company moved the employee to a different position due to performance issues and combative behavior toward colleagues. This event caused a major disruption to the company's operations, finances, and reputation.
- In April 2017, a major healthcare insurance coordination service learned that a third-party employee was stealing and misusing thousands of members' personal sensitive health data, including Social Security information, for more than a year. This incident followed a previous breach that cost the company millions of dollars.

[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

While there is no single profile of an insider threat, HR professionals should establish an evaluation framework that includes threat indicators, data profiles, 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.
- Consider the use of automated, continuous monitoring services to notify HR when employees have become a post-hire security risk.

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 logistical access.
- Establish a procedure to inform other employees when termination occurs.
- Review intellectual property/nondisclosure agreements with the separated employee.

ADDITIONAL RESOURCES FOR OWNERS AND OPERATORS

For direct regional support, please visit cisa.gov/hometown-security.

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