ONTIC®

Checklist

Insider Threats: Protecting Against the Enemy Within

BROUGHT TO YOU BY THE CENTER FOR PROTECTIVE INTELLIGENCE

There are few things more unsettling than learning that trust has been compromised between an employee or business partner and their company. This scenario, referred to as an insider threat, has grown in prevalence and can be defined as a "user with legitimate access to company assets who uses that access either maliciously or unintentionally, to cause harm to the business." (Security Intelligence)

Here's some guidance on how to protect against insider threats, resulting in safeguarding reputation, positive workplace morale, increases in productivity, among other benefits:

SECTION 1 PRE-EMPLOYMENT / PARTNERSHIP SCREENING

☐	**Criminal Records Check** — Check for reports of past violence in the last seven years.
☐	**Public Records Search** — Review undisclosed listings on government watchlists, national sex offender registries, motor vehicle records, civil records and credit history.
☐	**Reference Checks** — Conduct resume verification that includes education, past employment, co-worker conflicts, and title discrepancies. 38% of candidates tend to have discrepancies in their reported education history (HireRight, 2020).
☐	**Interview Process Observations** — Discuss any red flags, being mindful to not violate relevant privacy or "ban the box" laws.
☐	**Social Media Activity** — Review for criminal activity or behavior that goes against company values. This is often dependent on the company's HR and legal departments.

SECTION 2 POST-CONTRACT CONSIDERATIONS

☐	**Insider Threat Training Program** — Recognize aberrant behaviors and identify tactics that can lead to malicious attacks, with leadership setting an example.
☐	**Signs of Deceptiveness** — Be aware of any signs of suspicious behaviors such as time logs and expense reports, co-worker conflict, vocalized stressors or negative online behavior. These indicators may differ by department or context, so remain adaptive to the changing threat environment.
☐	**Anonymous Reporting** — Promote a supportive reporting culture that protects employees' privacy. This should include easily accessible feedback channels to share information to leadership.
☐	**Continuous Review Across Systems** — Review systems regularly - from visitor management, to access control, to HR portals and video management - to detect unusual patterns and uncover additional information related to a threat signal.

SECTION 3	POST-EMPLOYMENT OR PARTNERSHIP TERMINATION
☐	**Threat Assessment** — Conduct a threat assessment on the employee or business partner if determined necessary. (e.g. How does their behavior compare to the Pathway to Violence?)
☐	**IT Access** — Shut off access simultaneously to the notification. Doing this too early will likely "tip off" the individual.
☐	**Personnel Change** — Communicate the personnel or partnership change to the affected team(s).
☐	**Continuous Monitoring** — Consider what resources are in place for continuous monitoring of former employees or business partners that pose a legitimate threat.
☐	**Technology** — Utilize a technology solution to collect, store, and manage threat data through the threat lifecycle — paying specific attention to termination anniversary dates.

SECTION 4	SUMMARY QUESTIONS
☐	**Is your insider threat program tailored to your organization's needs?**
☐	**Do you have technology in place to surface alerts in real-time?** The longer an insider threat attack goes undetected, the greater the damage to the company.
☐	**How linked are cyber and physical teams?** How can cyber-physical processes and measures serve as an important foundation to mitigate insider threats?
☐	**Do your efforts to monitor for insider threats comply with federal and state regulations?** Knowing the laws of your state and municipality will put you in a more confident (and legally compliant!) position to assess threats.

Use this checklist as a guide to assess how you are protecting your organization against insider threats, and reach out to the Center for Protective Intelligence for support from our team of corporate security experts.