ATARC
Insider Risk Working Group

WHITEPAPER

Insider Risk Best Practices

Acknowledgments

ATARC would like to take this opportunity to recognize the following Insider Risk Working Group members for their contributions:

Michael Hudson, Clearforce, Insider Risk Working Group Advisor Chair
Shibu Thomas, Everfox, Insider Risk Working Group Industry Chair
Dr. Eric L. Lang, Insider Risk Working Group Member
Mitzi Mead, Anakim Consulting Incorporated
Hoke Smith, Nuix
Dr. Timothy Goss, U.S. General Services Administration Insider Threat
Dr. Liza Briggs, U.S. Patent and Trademark Office
Janel Olden, Department of Energy
Shawnda White-Drewery, Insider Risk Working Group Member
Chandra Smotherman, U.S. Air Force
Patrick G. Dauphinais Jr., U.S. Marine Corps
Timothy Amerson, CASMO Consulting
Diedra Bass, Navy Insider Threat Program, Navy
Benjamin Williams, Navy Insider Threat Program, Navy
David White, Everfox
George W. Costa, U.S. Census Bureau

Disclaimer: This white paper was prepared by the Insider Risk Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated.

Table of Contents

Overview

The purpose of this document is to provide government and industry leaders, managers and others with Government and Industry Subject Matter Expert informed recommendations to aid in designing and implementing a robust and effective Insider Risk (InR) mitigation program; Provide metrics and data to support requests for resources (funding, people and equipment); and assist the establishment of evidenced informed mitigation programs. Recommendations contained herein should be tailored to the organization's security posture, policies, and risk tolerance; encourage and support correct behavior; deter, detect and prevent people from wrongdoing; and mitigate the impact of insider risk.

Introduction

Insider Risk (InR) is defined as the risk of harm to an organization's mission, resources, personnel, facilities, information, equipment, network, or systems. Insider Risk is the potential for harm from individuals (employees, ex-employees, contractors or partners) with authorized access to a system, program, employees, or organizational property. This harm can be intentional, such as espionage, sabotage, or workplace violence or unintentional, such as negligence or failure to follow safety and security procedures.

Having an InR Program has been proven to significantly benefit the organization by identifying InR incidents or risk indicators as soon as possible, thus protecting the company's critical assets and reputation, reducing financial losses and legal risk.

Having a dynamic InR Program is a necessity in all organization. Each organization must tailor their InR program to align with their assessed most critical assets. A critical part of this assessment is your InR Program, which should help identify those critical assets, known risk vectors and best practices on how to protect them.

Insider Threats

A critical part of addressing InR is the connection with Insider Threats, while the precise definition of Insider Threat may vary slightly across organizations, the types of Insider Threat are commonly defined: intentional and unintentional (negligent or accidental).

Figure 4. Insider Threat Expressions

Taken from CISA Insider Threat Guide (Dated November 2020)[1]

Unintentional

Negligence - An employee, contractor, or partner ignore or become complacent about security and/ or IT policies thereby exposing the organization to risk. Examples include, but are not limited to: piggybacking, mislabeling or using portable storage devices containing sensitive information; failing to install updates and security patches without testing them first or not installing them in a timely manner; or failing to follow good cyber hygiene and physical security practices.

Accidental - These types of risks can be caused by anyone. Examples include but are not limited to: misconfiguring a device or firewall; inadvertently opening an attachment containing a virus; improperly disposing of sensitive information or physical safety accidents exasperated by being distracted.

(Note a growing risk to Unintentional is nation state social engineering attacks)

[1] https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

Intentional

Collusive Threats - These types of threats can occur when at least one person inside the organization becomes compromised. These types of threats frequently involve cyber or other types of bad actor coercion. An employee, contractor or partner becomes compromised because of activities outside the workplace such as gambling, excessive debt, criminal conduct or related activities. The goal of these types of threats is often sabotage, espionage, or theft.

Workplace Violence - Violence from an insider includes any act of violence, threat of violence or other intimidating, bullying, hostile or abusive behavior. Destructive workplace or individual threats often precede these types of threats. Hazing and harassment can be seen as precursor behaviors as can domestic or other interpersonal violence.

Espionage/ Financial gain - The practice of covert intelligence or information gathering by individuals or nation states. It can take the form of economic espionage (gathering intelligence on all forms of company trade secrets including financial, business, scientific, technical, engineering, or economic data not released to the general public); Espionage-intelligence gathering activities intended to gain political or military advantage.

Given the wide range of active threat categories, it is important for organizations to take a continuous and holistic view of InR mitigation. This approach provides the opportunity to leverage existing resources; create a security focused posture across the organization; and aid in incident mitigation and recovery.

Best Practices

1. Establish a multidisciplinary insider risk program and team

- **Designate Leadership:** Appoint an Insider Threat Program Senior Official (ITPSO) to oversee implementation and compliance. Designate a Program Manager to conduct day-to-day insider risk activities.
- **Cross-Functional Collaboration:** Form a multidisciplinary team with representatives from security (physical and cyber), HR, legal, IT, counterintelligence, law enforcement, and communications to ensure diverse expertise.
- **Identify Critical Assets:** Develop a clear understanding of your organization's "crown jewels". Gain consensus and align and prioritize program responses to mitigate risks that negatively impact key assets.
- **Identify Risks to Critical Assets:** Understand your sensitive data's vulnerabilities. As insider risk is predominantly a human problem, understand the different levels of risk represented by various categories of users such as clearance holders, departing users, and those with unique access to sensitive information or facilities.
- **Policy Development:** Define clear policies around acceptable use, access controls, data classification, data handling, and consequences of policy violations. Develop methods to continuously communicate policies to end users. Ensure your users are notified of monitoring in annual training.
- **Program Metrics:** Establish and link Key Goals, Resources, Metrics, and Timeline Milestones.

2. Implement continuous monitoring and vetting

- **User Activity Monitoring (UAM):** Implement user activity monitoring to identify anomalous behavior. Develop a process to continuously update UAM detections to reflect changes in threats, user behavior, and enterprise IT, and to control false positives.
- **Behavioral Analytics:** Leverage AI/ML to detect deviations from normal user behavior cyber and physical behavior patterns.
- **Continuous Vetting and Regular Reinvestigations:** Deploy continuous vetting of workforce, to include contractors, 1099s or others that have physical or cyber access to organizational property. Conduct ongoing personnel evaluations and background checks for those gaining new access to critical assets.
- **Privileged User Management:** Prescribe access controls and privileged user management for those that have elevated access to your most sensitive information. (i.e., System/network admins, sensitive financial and personnel data). Consideration to more inclusive continuous vetting.

3. Foster a culture of security

- **Leadership Engagement:** From the c-suite to the front line mangers/ supervisors need to reinforce through action and words the critical role that each employee, contractors plays in setting the conditions for safe and secure work environment.
- **Training Programs:** Deliver recurring insider threat training with role-specific content and countermeasure to address dynamic risk vectors. Plus include how to identify and report potential risk indicators.
- **Conduct regular internal testing of security systems and processes** to include tabletop and red team exercises and model on current and past attacks to ensure efficacy of the program. Update policies and training informed by these reviews.
- **Insider Threat Messaging:** Ensure that your program has a mechanism to communicate insider threat training awareness, and outreach to the workforce; recognizing the workforce is the first line of defense.
- **Cultural Assessments:** Conduct baseline and follow-up security culture assessments. Customize interventions based on organizational strengths, weaknesses, and systemic "friction" points. Use small group discussions to build grassroots support for improvements.

4. Manage emerging threat vectors

- **Information Leaks:** Establish monitoring and response protocols for potential leaks on public forums (e.g., Reddit or Discord).This should include intentional and unintentional leaks.
- **AI/GenAI Use (Deep Fakes):**
  - Evaluate how generative AI is used internally (e.g., productivity, code generation). such as data exfiltration, model manipulation, and unsanctioned information sharing
  - Develop governance policies for AI use that align with insider threat
  - Ensure ongoing Identity resolution to reduce risk of deep fake, synthetic identities
- **Data Exfiltration:** Those with ill intentions are always seeking ways to circumvent security processes and protocols. Implement a red cell team to identify new and emerging ways of data exfiltration.
- **Social Engineering:** Nation states and other threat actors are consistently targeting the weakest link in the security chain, which is the human.

a. Awareness Campaign

- **Insider Threat Bulletin:** Use this internal communication tool to distribute updates on threat trends, tips, and case studies.
- **External Events:** Participate in National Insider Threat Awareness Month and run organization-specific campaigns.
- **Strategic Communication:** Use intentional messaging strategies that reinforce the importance of vigilance, accountability, and reporting, while accounting for the organization's level of exposure and awareness to insider risks.
- **Reporting Mechanisms:** Create clear procedures for "how" to report potential insider threat concerns that could be witnessed by coworkers and supervisors in the work environment both remote and in office, plus external behaviors. Utilize several methods of reporting for all types of your population (i.e. anonymous hotlines, email distro lists and in-person reporting).

5. Leverage public-private partnerships

- **Collaborative Forums:** Actively participate in groups like Advanced Technology Academic Research Center (ATARC) Insider Risk Working Group (IRWG) to share insights and best practices.
- **Information Sharing:** Join interagency and industry-specific threat-sharing programs to stay current on evolving tactics.
- **Joint Exercises:** Conduct table-top exercises and red/blue team simulations with public and private partners to test readiness.

6. Review established frameworks and guidelines

- **CERT Practices:** Integrate guidance from the CERT Common Sense Guide to Mitigating Insider Threats.
- **NITTF Standards:** Ensure alignment with National Insider Threat Task Force (NITTF) minimum standards and utilize their templates (and the NITTF Maturity Framework).
- **CISA Resources:** Reference the CISA Insider Threat Mitigation Guide for scalable implementation strategies.
- **NIST:** Cybersecurity Framework (CSF), Risk Management Framework (RMF) and SP 800-53 are important guidelines for Insider Risk programs.

7. Integrate legal and privacy considerations

- **Privacy Protections:** Maintain transparency in monitoring and clearly communicate how data is used.
- **Legal Compliance:** Stay compliant with regulations such as GDPR, HIPAA, FCRA, EEOC and CCPA.
- **Ethical Standards:** Develop ethical guidelines to ensure the insider risk program earns and sustains employee trust.
- **Ensure all action are auditable:** Organizations need clear policy - assessing culture.

8. Conduct regular assessments and continuous improvement

- **Program Evaluation:** Perform regular assessments of program effectiveness through KPIs and audit findings.
- **Incident Reviews:** Conduct after-action reviews for insider incidents to identify lessons learned and root causes.
- **Continuous Improvement:** Update protocols and tools based on new technologies, emerging threats, and employee feedback.
- **Group Meetings:** Establish quarterly Insider Threat Working Group meetings for entire team with established agenda to keep insider threat top of mind.

Conclusion

Insider risk is an age-old dilemma that challenges many organizations both inside government and in industry. Each organization must weigh the cost of having—and more importantly not having—an insider risk program. Only risk owners can assess a mature program's value to the safety of its employees and protection of its critical assets. With that, we argue that there is more to lose by not having a competent program than to merely evade the topic and hope the risk bypasses your organization. With dedicated professionals, strong policy and protocols, use of pertinent technology and the necessary "buy in" from key stakeholders, risk owners can lower—though never eliminate—the risk that their own trusted people can cause. A mature insider risk program is a journey not a destination, and one where no perfect state exists.