INSIDER THREAT STARTER GUIDE
Insider Threat is a growing challenge and one that is not fully understood. Both surveys and studies suggest an increase in Insider Threat events and data strongly suggests insiders are responsible for most security events. Many organizations feel highly vulnerable to Insider Threats and few organizations have the necessary Insider Threat controls in place.

ENSURE FULL AWARENESS, UNDERSTANDING, AND VISIBILITY OF INSIDER RISK TO ENABLE THE BEST RESPONSE

Organizations must have full knowledge of employees, contractors, and business partners that have access to the organization's assets and to which they have access. Steps must also be taken to clearly identify different insider groups based on their level of access. Logical insider groups, based on both physical and electronic access, should be created to foster proper threat and risk identification and measurement. For example, such groupings should include at the minimum: insiders with super-user access, insiders with access to Crown Jewels, etc.

Awareness refers to the importance of developing a clear picture of an organization's insider population by ensuring a trusted workforce, providing insiders with resources to properly protect an organization's assets, creating a culture of transparency and responsibility, and developing workflows that foster the identification and mitigation of behaviors that may adversely impact the organization.

Understanding refers to the need to know what is important to an organization by identifying and denying critical assets; developing granularity about those assets; prioritizing them based on impact to the organization; and developing processes and procedures that foster knowledge of asset workflows, and incorporating this knowledge into risk management processes.

Visibility refers to the need to monitor insider behaviors that are indicative of a threat to an organization's assets; monitor interactions of insiders with identified assets; log asset accesses and movements; and analyze behaviors, interactions, and logs to identify risk through iterative and repeatable methods.

Response refers to the need to develop an effective balance of employee and security equities by supporting a governance framework that oversees compliance with established guidelines; developing unified workflows that leverage the collective expertise of ITP components and ensuring the ability to efficiently manage identified risks to organization assets.
A robust governance strategy is necessary to effectively create, employ, and manage an insider threat program. Strong governance and policy frameworks are the glue that holds the program together. Weak frameworks lead to ineffective and failed programs. Governance requires top-level awareness, understanding, authorization, and, most importantly, positive action. Therefore, senior leaders must take an active role in the development and implementation of the program. Similarly, strong policies will ensure parameters are followed and alignment of security and corporate objectives.

People are the first line of defense against Insider Threats. While there will be essential security awareness and training information that applies to all insiders (employees, partners, and contractors), you should strive to tailor it to the tasks of their specific roles and accesses. The goal should be to take your users beyond mere awareness of security policies and issues and truly educate them. They should be instructed on why and how to assess various situations’ risk and security implications. You should verify that they know how to apply security best practices as they perform their daily job duties.

Data protection becomes more challenging as networks become more distributed and dynamic. Security controls must be applied to digital and physical assets (including information and personnel) to ensure the ability to safeguard assets wherever they are accessed, used, transmitted, stored, or located.
IDENTITY & ACCESS MANAGEMENT

Insiders should have access to only those information assets for which they 1) have a need-to-know based on the role and duty and 2) that fall within the parameters of their risk profile. The integration of this analysis with data use provides real-time information for the Insider Threat management mission. Identity and Access Management (IAM) technology is the foundation of any robust access control and management strategy.

The IAM industry is evolving into new products and services focused on monitoring and controlling access for “privileged users.” The combination of user and role, identity, and data object-level access control provides granular control capability, thereby significantly reducing the potential impact of an insider data breach. Organizations can consider the role-based access control (RBAC) approach for use as an enterprise solution for both on-premise system data or a managed cloud-based service.

MONITORING

The employee monitoring market consists of technologies that collect data about the location, movement, communications, and actions of employees. Because of their narrow focus, these tools are often integrated with other tech stack tools to support broader purposes. The most prevalent use cases for EM products are optimizing employee, team, and process productivity and efficiency by tracking physical and electronic activities and reducing bandwidth costs emanating from the inappropriate use of devices and networks.
ANALYSIS

Successful implementation of an analytic capability for insider threat depends on knowing what data to collect. Organizations should strive for an integrated analytical capacity for Insider Threat detection prevention and response. Security and Incident Management feeds such as email, active directory, and network monitoring logs can provide critical indicators for insider threat behavior.

RISK ASSESSMENT

An enterprise insider risk assessment is an effective means to enumerate an organization's actual risk from employees and can be used to leverage the importance of having an effective program. The risk assessment process will also support an understanding of both organizational risk and operational risk. The assessment must be clearly outlined to support the organization's priorities, asset impacts, vulnerabilities, and threats are identified and used to measure insider risk.

PERSONNEL ASSURANCE

Employee support is a crucial part of any insider risk management program for myriad reasons. Most importantly, employees may leave the company for another place where they feel more comfortable without it. Employee turnover inhibits confidence and undermines morale. Their support is also necessary because many Insider Threats are discovered through the observations of managers and coworkers.

Effective employee support encompasses three pillars:
- They understand the importance of security.
- They agree to operate within the confines of security.
- They want to be an active participant in the security process.
INVESTIGATION

Organizations should strive to examine behaviors, actions, and insider threat indicators to mitigate threats following established policies, existing business objectives, risk tolerance, and legal parameters. Typical data loss, fraud, and intellectual property are the framework for investigative best practices; however, they can often miss critical data sources. Integrating evidence from HR, Legal, Cyber, and Security is essential consideration with investigative methods.

OVERSIGHT AND COMPLIANCE

A fundamental tenet of the Insider Threat ecosystem model incorporates an iterative learning capability. Organizations can only accomplish this through proper management and compliance that measures performance using appropriate metrics. This is more than merely conducting an impact analysis after a breach or related incident. The goal is to continuously learn from mistakes while striving to improve upon the successes of the program. Constant evaluation is key to "staying on course" and will provide continued legitimacy and efficiency to the program.
References and Further Resources:


Special Thanks:

The IT-ISAC team would like to thank all of the IT-ISAC Insider Threat Special Interest Group members who participated in the development of this product. We especially thank James Granger, Chief Operations Officer at Layer8, for proposing the idea of creating the guide and for his ongoing contributions to the Insider Threat Special Interest Group. We also thank Shawn Thompson, Founder and Director of the Insider Threat Training Academy and the Insider Threat Management Group, LLC, who contributed as an invited subject matter expert.