Program Best Practices > Insider Threat >

Insider Threat is a Challenging Organizational Problem

Here's how to identify it, set up a plan and prevent failure points

Created by the Security Executive Council

Note: While "unintentional acts" can also be detrimental, in this article we specifically cover "malicious acts."

How do you define insider threat and who is responsible for an organization's insider threat risk management and planning? Insider threats are actually broader in scope than simply encompassing Information Technology (IT) and related data. Because of this, the most effective responses incorporate a cross-functional team approach in the design and management of successful mitigation strategies. Without collaboration and a clear definition of responsibility, even the most well versed and strategized management of insider risk won't succeed or will quickly exhibit points of failure.

Based on intensive research and insights from leading companies, the Security Executive Council (SEC) recommends a comprehensive monitoring and screening process to address ongoing perceived and real insider risk – requiring insights and cooperation from many different points and positions within an organization.

The risk of insider threat is real and escalating. In May 2016, the Department of Defense (DoD) published Change 2 to DoD 5220.22-M, "National Industrial Security Operating Manual (NISPOM)," requiring government contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats. This move garnered the attention of private business leaders and executives, with many companies beyond the government classification working to build or enhance their insider threat programs.

The State of Insider Threats

The risks have changed and no organization, large or small, is immune from the malicious acts of a determined individual or organization. In addition, the definition of insider threat actors has broadened simply from employees to include clients, customers, contractors, business and technology partners and others who maintain regular or sporadic contact with these companies. Insider threat puts organizations at risk from theft of intellectual property, information technology sabotage, fraud, espionage and unintentional acts or threats. These threats are highly fluid and increasing daily, yet only 14 percent of organizations have defined insider threat and those that do label it narrowly. In addition, according to research, “Privacy and information breaches are seen as the most significant threats (by 94 percent of respondents), followed by workplace violence (67 percent); fraud (58 percent); and

The SEC’s experts and thought leaders have defined insider threat as:

Any risk posed by current or formerly trusted individual(s) with access or privileged knowledge; used to damage, deprive, diminish, injure or interrupt organizational stakeholders, assets, critical processes, information, systems or brand reputation. Insider threats include any illegal, prohibited or unauthorized conduct (acts or omissions).

Situations typically thought of as insider threat have splashed recent headlines and garnered the public’s attention: Targeted information hacking included a fortune 50 company with customer records breached through a third-party vendor; the leaking of classified information to the media by a U.S. National Security Agency Analyst; and an individual with top security clearance who stole trade secrets from a major defense contractor. Other examples that may not be commonly referred to as insider threat losses but are equally damaging and destructive include: A Swiss bank’s loss of over $2 billion by a fraudulent rogue trader; a Massachusetts crime laboratory chemist accused of mishandling evidence and criminal cases; and a food producer’s employee who deliberately contaminated 27 tons of chicken.

These types of malicious behavior have broadened the potential consequences as well as the number of departments within an organization that may have control and mitigation responsibility. Malicious behaviors or acts can include ransomware, loss of information, credit card fraud, workplace violence, worker’s compensation fraud, embezzlement, loss of proprietary information or compliance control and more. As such, many different stakeholders within an organization play a role in mitigating insider threat and carry responsibility in creating a successful plan–extending beyond Corporate and IT Security to include HR, Legal, Purchasing, Audit, Finance, Supply Chain, Quality and other appropriate stakeholders.

Look Beyond Traditional Resources

Intentional malicious acts have been around forever. The SEC sees the goal as early identification of malicious intent through gathering pertinent behavioral indicators from internal and external information sources and analyzing it for inappropriate behavior.

These risks, and their evaluation, must also consider new tools to assess, monitor and maximize mitigation. Newer sources of early warning indicators can consist of: information from social media, "dark web" criminal activity monitoring, real-time reporting of arrests and associated information and civil court proceedings, and network and site access records. These emerging resources should be combined with internal corporate data, performance data and corrective actions taken. Combined, this compendium of information could potentially identify and communicate behaviors that could lead to a situation that could escalate to an insider threat action.

In addition, different mitigation controls can detect more than one kind of loss or intentional damage. Site access control logs could identify someone stealing information but it could also identify someone trying to sabotage products. If an organization is focusing on information loss only, they may miss other malicious intent.

The SEC has identified the following issues that contribute to a breakdown of an organization's malicious act/insider threat mitigation efforts:

- Failure to develop and implement a cohesive plan—confusion on what it should consist of or what it encompasses.
- Not defining insider threat within the organization or a failure to agree on the definition and approach.
- Operating in silos of responsibility. Lack of a coordinated approach, input and accountability between all roles in a company or organization.
- Failure to monitor or regularly assess current and new areas of information, such as the dark web or social media.
- Lack of a unified organizational approach with buy in from all stakeholders who need to work collaboratively to monitor, assess, reevaluate and recalibrate plans when new threats emerge.

Effective threat mitigation strategies require careful planning in the early phases, taking time to define, organize, plan, implement, manage and monitor what's in place. Stakeholders need to evaluate the process at hand to define the acts and actors of concern and define roles and responsibilities of key functional groups as well as any gaps that may exist. Silos of responsibility are ineffective and one of the biggest failures comes down to the organization itself and lack of a unified approach. A successful oversight model that includes all corporate stakeholders and all possible information sources will bolster the likelihood of avoiding significant losses or reduce the potential for insider threat incidents.

Visit the Security Executive Council website for other resources in the Program Best Practices: Insider Threat series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/