Deloitte.

CFO Insights
Unmasking insider threats

As workplaces become more complex and insider threats become more difficult to detect, a program to mitigate those threats, which include fraud, espionage, workplace violence, information technology (IT) sabotage, intellectual property, and research-and-development theft, can bolster deterrence by providing an early-detection and response mechanism. Moreover, by viewing insider-threat mitigation more broadly than as a cybersecurity challenge, CFOs—working with their CIOs—can help assure the business, protect employees, and safeguard critical data, systems, and facilities.

The goal of insider-threat mitigation is to detect anomalies as early as possible and investigate leads before assets, data, or personnel are compromised. Staying in front of an insider's exploitative tactics, however, requires quick responses, real-time data feeds, and the analysis of behavioral indicators. And in this issue of *CFO Insights*, we'll outline actions to consider when designing, building, and implementing a formal insider-threat mitigation program.

- **Define potential insider threats:** An insider can be an employee, contractor, or vendor who commits a malicious, complacent, or ignorant act using their trusted and verified access. Still, few organizations have a specific internal working definition, as security and IT budgets have historically prioritized external threats. Defining potential insider threats for the organization is a critical first step to formulating a program, and will inform the size, structure, scope, and phasing plan for the program, aligned to business risk priorities.

- **Define the organization's risk appetite:** Define the critical assets that must be protected—whether they are facilities, source code, or customer information—and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in the business and in the way business is conducted. Tailor the development of the program to address these specific needs and threat types, and take into account the organization's unique culture.

- **Leverage a broad set of stakeholders:** An insider-threat mitigation program should have one owner but a broad set of invested stakeholders, as well as leadership support. Consider establishing a cross-disciplinary insider-threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholders. The working group should assist in addressing common concerns (for example, privacy and legal) and support the development of messaging to executives, managers, and the broader employee population.

- **Take a people-centric approach:** The insider-threat challenge is not a purely technical one, but rather a people-centric problem that requires a broad and people-centric solution. Organizations should avoid the common pitfall of focusing on a technical solution as the silver bullet. An insider-threat mitigation program should include critical business processes, such as segregation of duties for critical functions, technical and nontechnical controls, organizational change-management components, and security training programs.

powered by
The CFO Program

Who is an insider threat?

Insider threats are seldom impulsive acts. Employees wishing to harm a current or former employer, business partner, or client—whether by stealing trade or government secrets, sabotaging information systems, or even opening fire on colleagues—usually plan their actions. And regardless of their motivation, their plans often percolate for some time, and they typically share the following traits:

Insiders move along a continuum from idea to action. They don't wake up one morning and decide to exploit confidential information. They get an idea, ruminate, and then begin testing the waters to see if they can execute the idea—maybe by trying to access sensitive data or a secure facility.

Insiders leave evidence. Red flags frequently take the form of changes in attitude or behavior: the insider may grow frustrated or disgruntled, begin violating corporate policies, come in or stay late at the office, show "undue interest" in information that may not be relevant to his or her work, or attempt to access physical areas where he or she doesn't typically—or shouldn't—work.

Motivations vary. Some insiders who are a threat wish to get revenge against an organization they believe wronged them. Others seek some kind of personal or financial gain or to point out a perceived injustice. Still others may operate as spies for a foreign government.

There is no standard profile. An individual's personality isn't nearly as important as his or her actions. That said, you're not looking for a specific behavior, but a pattern of behaviors that may indicate a potential insider threat.

To detect insiders' actions before they do harm, organizations should establish a series of threat indicators, such as policy violations, job performance difficulties, or disregard for rules, based on high-value assets they wish to protect. For example, manufacturers seeking to safeguard new product designs might keep an eye on insiders trying to access or download those plans, traveling to countries where intellectual property theft is prevalent, or experiencing financial difficulty.

With insider-threat indicators established, companies can then begin to collect and correlate virtual and nonvirtual data about employees. Virtual data refers to the digital trails employees leave, say, when they log on and off the corporate network. Nonvirtual data includes information about an individual's role in an organization, performance ratings, and work habits.

While today's insider-threat monitoring systems are effective in establishing a baseline for "normal" employee behavior and tracking deviations, organizations should not rely solely on technology to mitigate insider threats. Instead, as outlined in the main article, they should consider instituting an insider-threat program that defines the assets a company wants to protect; establishes policies, procedures, controls, and training designed to protect those assets; and brings together stakeholders and data owners from a variety of functions, including HR, legal, compliance, finance, and administration.

- **Trust but verify:** Establish routine and random reviews of privileged functions, which are commonly done to identify insider threats across a broad spectrum of areas in a variety of industries. Organizations should trust their workforce, but balance that trust with verification to avoid the creation of unfettered access and single points of failure. Reviews are particularly essential in areas that are defined as critical.

- **Look for precursors:** Case studies analyzed by Carnegie Mellon University's Computer Emergency Response Team program have shown that insider threats are seldom impulsive acts. Instead, insiders move on a continuum from the idea of committing an insider act to the actual act itself. During this process, the individual often displays observable behaviors that can serve as risk indicators for early detection, such as requesting undue access or violating policies, for instance (see sidebar, "Who is an insider threat?"). According to the Federal Bureau of Investigation's Insider Threat Program, detection of insider threats should use behavioral-based techniques, looking at how people operate on the system and off the network, and then build baselines in order to identify anomalies.

- **Connect the dots:** By correlating precursors or potential risk indicators captured in virtual and non-virtual arenas, organizations can gain insights into micro and macro trends regarding the high-risk behaviors exhibited across the organization. Using an advanced analytics platform that correlates outputs from a variety of tools can be helpful, and the output can, in turn, be used to identify insider-threat leads for investigative purposes. Analytics can also shed new light on processes and policies that are either missing or could be improved upon.

- **Stay a step ahead:** Insiders' methods, tactics, and attempts to cover their tracks will constantly evolve, which means that the insider-threat program and the precursors that it analyzes should continually evolve as well. A feedback mechanism that includes an analysis of ongoing and historical cases and investigations can help organizations adapt their insider-threat programs to address new threats.

- **Set behavioral expectations:** Define the behavioral expectations of the workforce through clear and consistently enforced policies that define acceptable behavior and communicate consequences for violating policies. Policy areas might include social media, reporting incidents, and bring-your-own-device, for example.

- **Provide customized training:** One size does not fit all. Customize training based on the physical and network access levels, privilege rights, and job responsibilities. Train the workforce to the specific insider-threat risks, challenges, and responsibilities for each position.

Mitigating insider threats requires sponsorship from executive leadership and broad participation, from human resources to IT to operations and finance. In addition, to be effective, insider-threat programs should strike the proper balance between countering the threat and accomplishing the organization's mission. Too many security controls can impede the mission, while too few increases vulnerabilities and leaves the organization exposed.

Primary Contacts
Adnan Amjad
Partner
Deloitte & Touche LLP
aamjad@deloitte.com

Michael Gelles
Director
Deloitte Consulting LLP
mgelles@deloitte.com

Deloitte *CFO Insights* are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; and Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP.

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career – helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's CFO Program, visit our website at: www.deloitte.com/us/thecfoprogram.

Follow us @deloittecfo