Deloitte.

12 considerations

To mature an insider threat program

September 2016

Insider threat mitigation is a people-centric challenge requiring a holistic approach that encompasses polices, business processes, security education and awareness, and technology.

Organizations are increasingly evaluating their security programs to navigate the ever-changing landscape of insider threats. In this context, an insider threat is a person with knowledge or access who either deliberately or unwittingly puts an organization’s assets (e.g., data, facilities, systems, and personnel) at risk. Types of insider threats include theft of information, fraud, sabotage, espionage and workplace violence. Today, organizations face new challenges in preventing, detecting, and responding to insider threats. Namely, an increasingly mobile workforce, evolving workforce dynamics, and the digital reach of technology pose additional risks to an organization’s critical assets. Consequently, an effective insider threat program should take a holistic, proactive and risk-based approach to insider threat mitigation.

Over the past three years, Deloitte has designed, built, and implemented insider threat programs across a myriad of industries in both the public and private sectors (e.g., Federal government, oil and gas, technology, financial services, insurance, law enforcement). Establishing a secure, vigilant, and resilient program requires a carefully guided implementation and the maturation of three core insider threat capabilities: prevention, detection, and response. While it may not be realistic to interrupt every potential insider attack before damage is inflicted, it is possible and prudent to build an early detection capability into an organization’s operations to increase resiliency with the goal of limiting damage. The following twelve considerations represent lessons learned, specific insights, and leading practices from our extensive experience maturing insider threat programs.

01. Focus on prevention

Many insider threat programs allocate a disproportionate amount of time and resources on detection methods, but not enough on programs that emphasize prevention. Focusing only on detection fails to address preventative measures that can disrupt insider acts before they occur. Common prevention efforts include counseling programs (e.g., employee assistance programs) that help individuals cope with crises or loss, policies that set behavioral expectations across the workforce (e.g., IT acceptable use polices), and technical controls that block common exfiltration methods (e.g., removable media) without impeding employees’ abilities to perform the mission.

02. Prepare before you purchase

Some organizations will select a behavioral analytics tool without adequately defining critical assets, capturing the organization’s risk tolerance, defining Potential Risk Indicators (PRIs), and creating a structure to organize PRIs within the technology. Organizations that implement a technical solution before addressing these requirements often fail to separate the signal from the noise once they implement the tool. Consequently, the behavioral analytic tool generates little value in mitigating threats.

03. Separate the signal from the noise

As organizations mature their insider threat programs, an essential shift involves advancing beyond the use of just volume thresholds to detect exfiltration. While volume-based alerts (e.g., moving files above a certain size) can be helpful, it is equally important to create tripwires associated with specific words within content (e.g., e-mail subject heading, file name, or document contents). Creating controls that evaluate both content and volume can reduce false positives by auto- suppressing alerts regarding benign activity (e.g., employee sends vacation pictures to their personal e-mail address) and detecting true anomalies (e.g., employee separates from the organization and transfers pricing models to their personal e-mail).

04. Look beyond endpoints

Data exfiltration continues to rise due to changing workforce dynamics, a transient workforce, and advances in technology. According to one study by the Ponemon Institute, approximately 60% of employees who quit or are asked to leave take sensitive information with them[1]. Despite this clear threat, many insider threat programs only focus on the egress points (e.g., e-mail, removable media) and fail to incorporate security measures for shared work sites and databases that store sensitive information. A mature insider threat program should incorporate anomalies (e.g., large downloads, failed access attempts) from specific systems and applications that contain critical data.

[1] “Data Loss Risks During Downsizing.” The Ponemon Institute. February 2009.

05. Understand exfiltration methods

Based on analysis of leading public, private, and academic insider threat practices, as well as our experience designing, building, and implementing insider threat programs, we identified five common methods insiders use to remove information from the secure environment: (1) removable media, (2) e-mail, (3) cloud transmission, (4) transmittal devices (e.g., printers, copiers, faxes, scanners), and (5) file transfer protocol. The insider threat program should develop a plan to prevent, detect, and respond to insider threats by securing each egress point as part of the organization's overarching risk mitigation plan.

06. Apply the two person rule

Critical business processes and privileged functions (e.g., modifying source code, large funding authorization) should require additional oversight from a supervisor. Avoid falling into the trap of focusing solely on detection capabilities — e.g., advanced analytics tools — and ignoring preventative measures, such as role-based access. Strict segregation of duties, or the 'two-person rule,' is one of the most impactful deterrents, as it forces the insider to collaborate across multiple actors, which can reduce the likelihood that a single individual can effectively commit an insider act..

07. Reinvestigate routinely

Mature insider threat programs should adopt the use of periodic or aperiodic reinvestigations to capture significant changes in behavior and unreported life events. While many organizations implement policies requiring self-reporting of specific behaviors, they often fail to take the next step to establish technical controls, such as recurring background checks that go beyond self-reporting. These reinvestigations provide critical data needed to identify changes in financial status; life events, such as divorce; and criminal activity — all of which can serve as PRIs to detect emerging insider threats.

08. Plan response protocols

The ability to institute clear protocols for escalation and triage of identified insider threats drives the insider threat program to engage the right personnel within the organization efficiently and decisively. Creating a nimble triage process requires predetermined agreements among program stakeholders and a keen understanding of the organization's risk tolerance. Mature programs also build in resilient capabilities through the use of war-gaming exercises to reveal issues in responses through practice, using real-life scenarios to test and refine triaging protocols.

09. Secure the Supply chain

The rising interconnectedness of organizations and increasing reliance on complex supply chains pose a significant insider threat risk. Mature insider threat programs should invest in measures to secure their supply chain. An organization is only as secure as its riskiest vendor, and adversaries only need a single point of access to exploit an organization and pose an insider threat. To address potential risks posed throughout the supply chain, organizations should conduct third-party risk assessments to identify areas of increased insider threat risk.

10. Train management

A vigilant manager workforce and a culture of security are critical aspects of insider threat mitigation. The insider threat program should include role-based training for managers to help the workforce recognize signs that an employee is stressed and/or may be going through a crisis (factors that can contribute to insider threats). Program managers should also be aware of guidelines and reporting mechanisms, including anonymous reporting methods and the responsibility to report.

11. Address Lagging Access

Many organizations struggle to ensure separated personnel do not maintain physical and/or logical access after the employee's last day. Separation status is critical to insider threat mitigation, as it represents a window of increased likelihood for insider threat acts to occur (e.g., sabotage and theft of information). Lagging access is a specific vulnerability that allows insiders to exploit information, critical assets, and facilities once they have left the organization. Organizations should map out the separation process to identify vulnerabilities, connect stakeholders involved, and design a timely process to proactively terminate access at the right point in time.

12. Quantify Progress

Security is often viewed as a cost and drag on revenue. To shift these perspectives, insider threat programs should capture the return on investment through the use of metrics, such as the number of leads generated, cases opened, risk mitigation steps taken, law enforcement referrals, documents prevented from exfiltration, and technical control updates. Routine reporting of these metrics to executive leadership will elevate the visibility and importance of the insider threat program.

For more information, please contact:

Mike Gelles Managing Director Deloitte Consulting LLP mgelles@deloitte.com +1 202 251 9615	**Kwasi Mitchell** Principal Deloitte Consulting LLP kwmitchell@deloitte.com +1 703 945 7951	**Deborah Golden** Principal Deloitte & Touche LLP debgolden@deloitte.com +1 571 882 5106
Rebecca Tyler Principal Deloitte & Touche LLP rtyler@deloitte.com +1 571 814 6886	**Borna Emami** Senior Manager Deloitte Consulting LLP bemami@deloitte.com +1 202 957 3165	

Contributing authors

Brock Krawczun
Hannah Carlisle

For further information, please visit **www.deloitte.com/insiderthreat**.

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit and enterprise risk services; and Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing and human capital consulting services. Deloitte Consulting LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.