Deloitte.

Top 10 considerations for building an insider threat mitigation program

Introduction

Organizations continue to face a variety of insider threats, as demonstrated by a string of high profile cases where employees in pursuit of validation or affirmation have used their knowledge and access to physical and/or information systems to cause significant damage. These cases highlight vulnerabilities and underscore a historical perception that insider threat mitigation is predominately a cyber-security challenge, and categorized as a strictly information technology responsibility. This approach will leave the organization vulnerable to existing and emerging insider threats. Deloitte takes a fundamentally different view that insider threats are more effectively addressed as part of a holistic and risk-based program with broad participation required (e.g., legal, information assurance, human resources, physical security, information technology, etc.) and sponsorship by executive leadership. Deloitte has developed a top ten list for leaders to consider as they design, build and implement a formal insider threat mitigation program. At a time when accountability is a primary leadership responsibility, an insider threat mitigation program can bolster deterrence and provide an early detection, prevention and response mechanism assuring the business, protecting employees, and safeguarding critical data, systems and facilities. This guidance was informed by the development of insider threat programs across a diverse range of organizations in the commercial and public sector.

Key considerations

1. Define your insider threats — Don't be surprised if your organization hasn't defined what an insider threat is. The reality is few organizations have a specific internal working definition as security and IT budgets have historically prioritized external threats. An insider can be an employee, a contractor, or a vendor that commits a malicious, complacent or ignorant act using their trusted and verified access. Defining the threats for your organization and specific business environment is a critical first step to formulating a program, which will inform the size, structure, scope, and phasing plan for the program, aligned to business risk priorities.

2. Define your risk appetite — Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) that must be protected and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in your business and in the way you do business. Tailor the development of the program to address these specific needs, threat types and take into account your organization's unique culture.

3. Leverage a broad set of stakeholders — The program should have one owner but a broad set of invested stakeholders. Establish a cross-disciplinary insider threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholder (e.g., legal, physical security, policy, IT security, human resources, ethics, etc.). The working group's support will be critical to building the insider threat mitigation capability and securing data needed for the program. It should assist in addressing common concerns (e.g., privacy and legal) and support the development of messaging to executives, managers and the broader employee population.

4. Technology, alone, won't solve the problem — The insider threat challenge is not a purely technical one, but rather a people-centric problem that requires a holistic 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 key business processes (e.g., segregation of duties for critical functions), technical and non-technical controls (e.g., policies), organizational change management components, and security training programs needed to promote an environment of security awareness and deterrence.

5. Trust but verify — Establish routine and random auditing of privileged functions, which is commonly used to identify insider threats across a broad spectrum of threats in a variety of industries. Organizations should trust their workforce but balance that trust with verification to avoid instances of unfettered access and single points of failure. This auditing is particularly essential in areas that are defined as critical.

6. Look for precursors — Case studies analyzed by Carnegie Mellon University's Computer Emergency Response Team (CERT)[1] program have shown that insider threats are seldom impulsive acts. Rather, insiders move on a continuum from the idea of committing an insider act to the actual act itself (e.g., fraud, espionage, workplace violence, IT sabotage, and intellectual property and research and development theft). During this process, the individual often displays observable behaviors (e.g., requests undue access, violates policies, and demonstrates disgruntled behavior) that can serve as potential risk indicators for early detection. According to the FBI's Insider Threat Program, detection of insider threats should use behavioral-based techniques. This includes looking at how people operate on the system, off-the network, and then build baselines in order to identify anomalies.

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

8. 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 continuously evolve as well. This can be achieved through a feedback mechanism that includes an analysis of on-going and historical cases and investigations.

[1] Common Sense Guide to Mitigating Insider Threats, 4th Edition, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34017

9. Set behavioral expectations — Define the behavioral expectations of your workforce through clear and consistently enforced policies (e.g., social media, removable media, reporting incidents, BYOD, etc.) that define acceptable behavior and communicate consequences for violating policies.

10. 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 (i.e., the data administrators' curriculum should be different from the sales representatives' curriculum).

Conclusion

Mitigating insider threats requires a comprehensive, risk-focused program involving a wide range of stakeholders and operational areas. As the workplace becomes more complex and insider threats become more difficult to detect, the tools and detection techniques must become smarter and capable of adjusting to the evolving threat. Having too many security controls can impede the mission. Having too few increases vulnerabilities and leaves the organization exposed. Insider threat programs should strike the proper balance between countering the threat and accomplishing the organization's mission. Quick responses, real-time data feeds, and analysis of behavioral indicators are imperative to stay in front of the insider's exploitative tactics. The goal is to detect anomalies as early as possible and investigate leads in order to interrupt the forward motion of potential insider threats before assets, data or personnel are compromised.

For more information, please contact:

Adnan Amjad
Partner
Deloitte & Touche LLP
aamjad@deloitte.com
+ 1 832 863 4165

John Cassidy
Senior Manager
Deloitte Consulting LLP
jocassidy@deloitte.com
+1 571 814 7196

Mike Gelles
Director
Deloitte Consulting LLP
mgelles@deloitte.com
+1 202 251 9615

Kwasi Mitchell
Senior Manager
Deloitte Consulting LLP
kwmitchell@deloitte.com
+1 703 945 7951

Keith Brogan
Senior Manager
Deloitte & Touche LLP
kbrogan@deloitte.com
+1 908 400 3455

Borna Emami
Manager
Deloitte Consulting LLP
bemami@deloitte.com
+1 202 957 3165