KPMG

Insider threats

Malicious attacks from within are on the rise. How well is your organization prepared?

Managing insider risk is complex

Your organization's private, sensitive, and mission-critical information is increasingly coming under attack—from within.

The possibility of insider threats—that is, actions by employees who either maliciously or carelessly circumvent security controls—are on the rise, fueled by innovative technologies, new methods of communication, an evolving socioeconomic climate, and geopolitical changes.

The damage from these breaches can wreak havoc on any organization. Just consider Bradley Manning's WikiLeaks scandal, Edward Snowden's release of secret documents, and Aaron Alexis, the Washington Navy Yard shooter.

And expectations are high

Following a series of these high-profile incidents, President Obama issued an executive order that established the National Insider Threat Task Force (see below chart). Its mission is to deter, detect, and mitigate actions by insiders who may represent a threat to national security by developing a national insider threat program with supporting policy, standards, guidance, and training.[1] New standards and expectations will continue to evolve as leading practices are identified.

Federal policy Executive Order 13587	Mandates that agencies not only have an insider threat detection program, but that internal organizational security meets specific functioning standards. The National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs direct government departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect sensitive data.
The National Insider Threat Task Force (NITTF)	Under joint leadership of the Attorney General and the Director of National Intelligence, the NITTF is responsible for developing a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels as well as the distinct needs, missions, and systems of individual agencies.
The National Institute of Standards and Technology (NIST)	Added insider threat guidance into its NIST Special Publication 800-53, Revision 4, which includes security controls related to the adversaries that have achieved a significant presence within organizations and its information systems—organizations dealing with an advanced persistent threat.
National Industrial Security Policy	Requires cleared industrial, educational, commercial, or other entity to establish and maintain an insider threat program to detect, deter, and mitigate insider threats.

1. Source: National Insider Threat Task Force, Washington, D.C. (2012).

Getting started

Ensuring the safety of critical resources is every executive's job. What is your organization doing to protect the people, property, and resources it is responsible for? To meet these new insider threat requirements, organizations will need to transform their security, privacy, and continuity controls, while maintaining the confidentiality, integrity, and availability of critical business functions. As a start, organizations can take a number of immediate steps to assess and lessen their vulnerability to insider-threat risks.

Inventory sensitive assets and rate the risks—First, an organization needs to identify the assets—people or technology, for example—that are critical to carrying out its mission. Once those assets have been identified, the organization needs to rank them according to their importance.

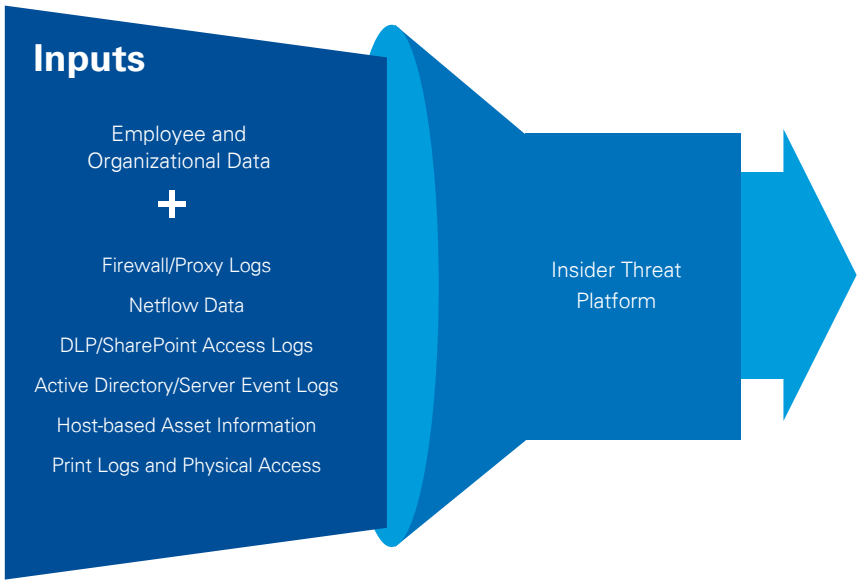
For the most critical assets, the organization needs to discern their vulnerabilities to attack. To do so, it should ask what would be the consequences if these assets were attacked, knocked offline, or otherwise eliminated. The organization also must ask who among their employees has access to those assets and then evaluate and categorize the potential threat from each one of these individuals. Then, it needs to rank those individuals, from those presenting the highest threat to the lowest.

Implement monitoring program—Once mission-critical assets have been identified and potential insider threat risks categorized and ranked, the organization needs to implement a program that will enable it to mitigate and monitor those risks. In creating such a program, the organization must first develop a policy and guiding principles that are compatible with its culture and meet national standards.

This policy then needs to be communicated, understood, and embraced by the organization. First, all stakeholders will need to completely support the effort. That will include buy-in from not only the director of security, but also HR, legal, and leadership. Equally important, the organization must engage the workforce in the program and require adherence to policies. A thorough communications plan may be needed to explain to employees how security threats have evolved and how much more vulnerable entities are today than just a few years ago.

Continuous Monitoring and Evaluation—As depicted in the illustration below, continuous monitoring is one option organizations can consider to help identify suspicious activities that might presage an insider event. Because so many employee tasks today are carried out through an organization's internal networks and over the Internet, monitoring that digital activity can provide organizations with far-reaching insights into employee behavior.

Anomaly Detection Methodology



Potential Insider Threat Behavioral Indicators	Score	John	Amy	Phil
Anomalous data bandwidth to personal e-mail	5	x		
Access to fileshares not typically accessed by role	5		x	x
Systems access outside of typical user work hours	10	x		
Irregular VPN access outside of typical user work hours	5	x		x
Improper sentiment/language	2	x		
Aggregate Risk Score		**22**	**5**	**10**

Using information they already maintain, organizations can begin to understand whether certain internal activity represents a potential risk. Behavioral scientists have already identified what outlier actions can be red flags for possible threats. Advanced data analytics can render indicators that management can consider for follow up.

Although the chief goal of this kind of monitoring is to preempt an attack, it is important to remember that not all such activity may have a malicious intent. Sometimes, people can be duped or exploited by others into performing actions that would present a threat to an organization.[2] Intervention can help save "an employee's career, save lives, and protect national security information."[3]

Evidence suggests that continuous monitoring programs can be effective and show results quickly.

KPMG: Flexible implementation through core capabilities

Whether you require an assessment of insider threat risks, design and implementation of an insider risk threat program, implementation of an automated insider threat tool, or an evaluation of your insider threat program and how you are mitigating risks—KPMG LLP's (KPMG) services are designed to be targeted, scalable, and tailored to your needs.

- As the trusted advisor to more than half of cabinet-level agencies, we have deep insight into the business of government. We know the threats facing business operations and government programs.
- We work with technology companies to successfully design, implement, and sustain government-wide insider threat systems.
- We use a multidisciplinary approach. KPMG can leverage its breadth and depth in areas ranging from risk management to organizational change, and from forensic investigation to user adoption of complex systems.

For more than 100 years, KPMG has assisted the federal government in the civilian, defense, and intelligence sectors. Our nearly 1,000 dedicated partners and professionals possess the knowledge, insight, and awareness of pertinent legislation and regulatory implications needed to address the special needs of the public sector.

2. Ibid.
3. Ibid

Contact us

Laura Price
Partner
Federal Risk Consulting Leader
M: 301-706-8525
O: 703-286-8460
lprice@kpmg.com

David Buckley
Managing Director
Federal Forensic Advisory
M: 703-626-2811
O: 703-286-8489
davidbuckley@kpmg.com

Nirali Chawla
Director
Federal Cybersecurity Advisory
M: 443-691-8544
O: 703-286-6694
niralichawla@kpmg.com

kpmg.com/socialmedia