Most organizations have their guard up to protect against external hackers breaking into their systems and accessing their private, sensitive and mission-critical assets. But another, potentially more ominous, menace exists much closer to home—the insider threat.

While the vast majority of employees will work conscientiously and honestly, a growing number of workers are breaking into secure areas of their employer’s systems with clearly malicious intent. So while potential damage from external threats receives most of the attention, insiders are actually at the core of many of the worst incidents of misconduct. Why? Because you trusted them and you weren’t paying attention.

Insider threats are on the rise

Insider threats continue to grow. In 2015, IBM\(^1\) reported a shift in the cyber landscape where insider attacks began to outnumber outside hacking. A year later, a Mimecast\(^2\) survey found that 99 percent of respondents had experienced some form of insider security incident in the past two years and Intel reported that internal actors were found to be responsible for 43 percent of all data loss. Yet despite this alarming rise in insider threats and activities, most companies are still focusing most of their security efforts externally. Typically, less than 20 percent of organizations’ security budget goes toward insider threats, according to Dr. Eric Cole\(^3\) of SANS.

Why the increase?

Insider threats are growing for a number of reasons—sociological, demographic and technological.

— *Changes in the workforce*—Today’s workforce is increasingly transitory and prone to high turnover; employees accordingly see themselves as “free agents” with less loyalty to employers. Knowledge and information is often seen as open source—to be shared rather than owned.

— *Changes in work environment*—Work from home and bring-your-own-device practices have eroded traditional network defense. Companies are increasing their use of third-party contractors, who need access to company information but are not vetted or monitored properly. All the while, the growing use of the cloud puts more information outside of the company’s immediate control.

— *Changes in the world*—Increasing global competition, polarized geo-political tensions and a growing distrust for big governments and corporations in many individuals create a fertile field for divided allegiances prompting insiders to act in ways that put an organization at risk.

— *Changes in technology*—Business and government entities have become increasingly dependent on interconnected technology and mass data storage. While that offers great conveniences, it also makes organizations increasingly susceptible to risk with the potential for larger impacts when breaches and other abuses occur.


Who are the insiders?

An insider threat is any person in a position where insider credentials, status, or access is used to cause any sort of harm or loss to an organization. Insiders are generally trusted by their organization and given some level of authority and access to its resources. They not only include current employees but also former employees, third-party partners and contractors, as well as outsiders who have obtained credentials (whether through theft, coercion, or an insider’s neglect) and are now de-facto insiders.

Insider motives and targets

What motivates an insider to commit or enable a crime? It varies: sometimes it is clearly malevolent but there are a range of motivations all the way down to simple carelessness or a lack of knowledge of policy and safeguards.

Insider motives

- Revenge
- Political or social agenda
- Financial
- Career advancement
- Empowerment (or perception of)
- Sense of entitlement
- Blackmail
- Ease or speed of doing their job
- Personal problems
- Lack of knowledge
- Mistakes from policy or system inadequacies

Increasingly malicious

Critical assets

People
Information
Operations - Physical and technical
Financial
Reputation

Threats

Workplace violence
Espionage
Leakage
Thief of IP
Sabotage
Business disruption
Fraud
Reputational Harm

Where can insiders cause harm and how? Insiders can pose a threat to an organization’s people, information, trade secrets, operations, finances and reputation using vectors such as theft, fraud, sabotage, workplace violence, etc.
What can you do?

Addressing insider threats is complex and multifaceted. Defining and understanding the elements involved and how they interact is the first step in building an insider threat program.

KPMG has developed an Insider Threat Management Framework that follows the National Institute of Standards and Technology (NIST) concepts of Protect, Detect and Respond but with facets and aspects unique to the insider perspective as defined by authorities including CERT, INSA, NISPOM, etc.

These concepts are supported by proper Governance and stakeholder engagement.

In addition, there are areas outside the insider threat program proper that are both influenced by and influence the potential success of an Insider Threat program. We refer to these areas as Foundational Elements. Together, all of these elements must be addressed in order to successfully mitigate insider threats.

**KPMG’s Insider Threat Program Framework**

**Building a program: the critical factors**

KPMG defines seven critical factors to consider when setting out to build an effective Insider Threat Management program:

1. Secure executive sponsorship and proper governance and policies
2. Use an established, risk-driven methodology
3. Create a dedicated insider threat team with cross-discipline perspectives and abilities
4. Communicate and coordinate across the entire enterprise
5. Understand the indicators of insider threats
6. Consider the cultural and legal implications of the program
7. Leverage the right tools in the right way
Vendor-agnostic perspective — KPMG’s vendor-agnostic view of the landscape of Insider Threat related tools (User Entity Behavioral Analytics, etc.) will speed your understanding of which products would be most effective for your organization. This gives KPMG clients a clear advantage in quickly understanding and navigating the hundreds of choices in the complex analytics market and choosing from among the best solutions for them.

Proprietary toolkits: KPMG has developed an Insider Threat Readiness Assessment toolkit to guide you in quickly gaining an understanding of where you are at risk to insider threats, how ready you are to deal with them and what road map will help you most effectively deal with these threats.

Contact us

Shane Sims
Principal
Cyber Security Services
T: 703-286-8738
E: shanesims@kpmg.com

David Buckley
Managing Director
Federal Forensic
T: 703-286-8489
E: davidbuckley@kpmg.com

Bill Bonde
Director
Physical Security
T: 757-616-7043
E: wbonde@kpmg.com

L. Travis Canova
Director
Commercial Forensic
T: 713-319-2731
E: LCanova@kpmg.com

Michael Thompson
Director
Insider Threat Program Mgr
T: 713-319-3159
E: mdthompson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 692396