Insider threat and end-of-service assessments

October 2021

KPMG in the UAE and Oman

What is an insider threat?

An insider threat is a security risk that originates from within a targeted organization. While business face challenges on a daily basis, few are as difficult to manage as the threat posed by disgruntled or malicious employees. Their goal could be to make financial gains or cause damage by profiting from their knowledge and position.

These culprits have the capability to expose a business to an extensive range of financial, reputational and cybercrime threats, purely because they are considered trustworthy or close to sensitive data or systems. It is imperative to understand the intent of insider threats. If businesses comprehend how and where such threats may arise, they will be better positioned to protect their systems and data. The more insight a business has into its employee behavior, the more likely an entity is to identify signs of an insider threat.

What is the threat?

An insider threat can materialize when someone near to a business, with authorized access, misuses their position of trust to harm business-critical data or systems. This does not mean that the threat actor must be a current employee in the organization. They could be a consultant, former employee, business partner, board member, or a third party associated to your business.

In order to protect your business, it is vital to understand what an insider threat looks like. There are two main types: turncoats and puppets – malevolent insiders and coerced partakers, respectively.

Managing the business risk of employee wrongdoing can be a difficult and potentially challenging exercise. A key aspect is the potential for staff members to undertake malicious action against the business prior to their exiting, leaving little time for a company to identify or undertake the necessary actions to mitigate the risk involved.

Indicators of an insider threat

Behavioral warning signs include:

- Regularly in the office outside working hours
- Displays or expresses displeasure with the organization and/or other employees
- Breaches corporate policies, procedures and processes
- Attempts to circumvent security
- Deliberates resigning or new opportunities

Although behavioral warnings can indicate potential problems, digital forensics and analytics are the most efficient and effective ways to identify insider threats.

Digital warning signs include:

- Copying key documents such as client lists, intellectual property or other sensitive information to external sources
- Accessing substantial amounts of data
- Accessing sensitive data not associated with their role in the business
- Accessing data that is outside of their behavioral profile
- Multiple requests for access to resources not associated to their role
- Using unauthorized storage devices
- Emailing sensitive data outside the organization
- Disrupting or blocking a company's use of its systems
- Suspicious network and internet activity

What we do

Our insider threat or end-of-service gap and impact assessment conducted in partnership with clients, will achieve the following:

- Raise the cybersecurity levels and the ability of the business to respond to insider threats
- Identify where the organization is exposed to an insider threat, and determine potential risks
- Determine how to establish a foundation for in-house investigative and forensic capabilities
- Establish the required roles and responsibilities
- Understand what policies, procedures, processes, workflows, best practices and guidelines need to be amended or created
- Assist in shaping the required frameworks and processes

KPMG's Cyber Investigations team conduct insider threat and end-of-service assessments. Our experts forensically image and analyze targeted employees' business-related devices (laptops, file share folders, server mailboxes, external computer storage media, mobile phones, etc.) and quickly provide a report detailing areas of concern. This will provide peace of mind in situations which could have financial, legal or reputational implications.

In the current climate of remote working, it can be challenging for businesses to review case data effectively. Whether it be a hard drive full of documents, a tranche of loose information, or perhaps investigative related information that cannot be easily searched. Our KPMG Discovery team can assist with an insider threat assessment using KPMG's document review system, which allows quick access and assessment of any suspicious documents no matter where you are in the world.

KPMG's objective

KPMG's cybercrime service professionals strive to make the client's experience during a cybercrime and in particular an internal data loss, regardless of how big or small, is a positive one. As part of the engagement process, our team actively solicits feedback throughout an investigation. This is reviewed at all levels, to manage expectations, improve satisfaction and build long-standing relationships.

Our objective is to make it as easy as possible for our clients to call on us in the event of data loss through internal threats. Our standard operating model is to provide a single point of contact for any queries, issues or assistance required.

KPMG

Contact us

Nicholas Cameron
Partner, Head of Forensics
Forensic Technology
KPMG Lower Gulf Limited
e: nicholascameron@kpmg.com
t: +971 4 424 8992

Alan Zhang
Associate Director
Forensic Technology
KPMG Lower Gulf Limited
e: azhang68@kpmg.com
t: +971 4 405 0935

kpmg.com/ae
kpmg.com/om
Follow us on:

Designed by KPMG Lower Gulf Creative team.

Publication number: 2984

Publication date: October 2021