KPMG

Cyber security: managing the insider risk

Cyber security

kpmg.ch/cyber

Insider threat is often overlooked

While many attempts to obtain financial gain or sensitive information from your company will originate from outside the organization, the most devastating and successful ones often take place from within.

To positively manage the cyber risk as a whole, organizations need focus on their insiders. These can be defined as their current or former employees, contractors or business partners who have or had authorized access to the organization's network, system or data. Identifying and addressing these specific risks, require to leverage people, process and technology risks and appropriate controls in a framework that secures the business in a balanced manner where it also enables the business to operate at best.

Building agility into your insider risk strategy, anticipating change and disruption, enables you to architect an environment that is secure by design. Having a robust strategy and governance to mitigate or prevent incidents caused by employees or contractors, is key to remaining operational within the changing threat landscape and helps to achieve long-term business success.

Insider risk management: focusing on the organization

Managing insider risk is complex

The fact that risks originate from insiders is not a new issue, however the evolution of technology, communications, socio-economic climate and geo-political changes have increased the impact of these threats.

Unlike attacks originating from outside the company, insiders often have legitimate access to the premises and computer systems for genuine business reasons. They are also familiar with the company's intellectual property and sensitive information. Additionally, being an insider makes it easier to circumvent security controls.

Changing perspectives is key for success

To successfully mitigate this risk should require focusing on the people and the processes first, and only then on the technology. Such exercise must cover holistically each of the following dimensions:

- Prevent
- Detect
- Respond

This focus must be coordinated with each department throughout the organization in a people, process and technology systemic analysis.

Malicious insiders have caused serious incidents resulting in major consequences

- Loss of bids to competitors who become aware of your negotiating strategy
- Sanctions by authorities or regulator
- Inability to operate as critical systems are compromised
- Beaten to market by competitors who know your future product features and release dates
- Reduction in income due to loss of customer confidence
- Significant threat to share price
- Brand reputation damage

BALANCE PEOPLE, PROCESSES AND TECHNOLOGY TO MITIGATE THE RISK

Whereas cyber crime has a strong connotation with "technology", fighting it effectively requires an integrated and balanced approach involving both people and processes as well as technologies.

A step-by-step phased approach

Our step-by-step approach, enables to benefit from deliverables and quick-win features at the end of each phase allowing early returns-on-investment

.

Phase 1 **Know your company**

- Identify all the key components of the company such as strategic threats, assets, vulnerabilities and effectiveness of security controls vs the strategic threats.
- Ensure the organization's security measures are aligned with the company's strategic goals.

Phase 2 **Manage people risk proactively**

- Assistance in defining the company's people risk evaluation methodology across the organization and based on the board-level threats and aligned with the business needs and strategy
- Aligning/defining organizational, administrative or technical controls aligned in a risk-based approach to ensure highest cost efficiency ratio.

Phase 3 **Detect insider incidents**

- Our early warning system leverages the people, process and technology aspects which can help to prevent occurrence and mitigate the impact of incidents to the organization. Our model enables to shift from a response to a proactive culture to reduce operational losses and protecting your reputation.
- Facilitated by enterprise grade tools helps you address constantly changing threats aligned with the employee life cycle.

Means, opportunity, motive

In order to have a successful understanding of the threats by insiders, it is critical to focus also on the key realization factors being the means, the opportunity and the motive.

Means
Opportunity
Motive

Means: Insiders' ability to commit the incident is gained through electronic or physical access to the assets or target.

Opportunity: Lack of proper safeguards or controls in place will not only help a criminal-minded insider to achieve his goals but also often allow the incident to remain unnoticed for a long period of time.

Motive: Reason to commit the incident that can be politically, financially, psychologically driven.

Key benefits

People focused to address these specific threats and promoting a security risk culture within the organization.

Proven to be effective in enterprise production environments.

Incremental benefits allowing to realize security benefits and quick wins during every implementation phase.

Scalability and cost efficiency in performing daily security operation.

Enterprise grade tools to support the process and facilitate decision making.

Why kpmg ?

At KPMG, we believe cyber security should be about what you can do – not about what you can't.

Driven by business aspiration

We work with you to move your business forward. Positively managing cyber risk not only helps you take control of uncertainty across your business; you can turn it into a genuine strategic advantage.

Razor sharp insights

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance. Our people are experts in both cyber security and your market, which means we give you leading edge insight, ideas and proven solutions to act with confidence.

Shoulder to shoulder

We work with you as long term partners, giving you the advice and challenge you need to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with you to turn that into a real sense of security and opportunity.

Global reach

With have more than 2'000 security practitioners working in KPMG's network of firms, giving us the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programs, to technical assessments, forensic investigations, incident response, privacy, third party risk, training, ISO 27001 and privacy certifications.

Contacts

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

Rue de Lyon 111
PO Box 347
1211 Geneva 13

kpmg.ch/cyber

Marc Bieri
Director
Cyber Security

+41 58 249 64 05
marcbieri@kpmg.com

Matthias Bossardt
Partner
Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Gerben Schreurs
Partner
Cyber Security

+41 58 249 48 29
gschreurs1@kpmg.com

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 on such information without appropriate professional advice after a thorough examination of the particular situation.