APRIL 2024 | SIGNPOST SIX

INSIDER RISK

TREND REPORT 2024

SIGNPOST SIX B.V.
WWW.SIGNPOSTSIX.COM

INTRODUCTION

In 2023, insider risks persisted, demanding a multidisciplinary approach across various sectors. Several key trends continue to emerge, emphasising the need for proactive prevention at the centre of insider risk management.

Collaboration became paramount, with organisations sharing information and best practices to address industry-specific challenges. As we confront insider risks, engaging in focused conversations around these trends is crucial. Insider risk management requires a sharp and proactive interdisciplinary strategy to effectively counter the evolving nature of these threats.

Below we outline the primary trends in managing insider risks across our wide-ranging client portfolio.

ABOUT SIGNPOST SIX

Signpost Six is Europe's leading insider risk expert, providing expertise in safeguarding your organisation's critical assets and personnel. Our focus spans the entire spectrum of insider risk, from complex issues like nation-state espionage to organised crime and beyond.

We deliver tailored, forward-thinking solutions, ensuring seamless integration with your organisational processes. Our team, equipped with diverse expertise and deep industry knowledge, is your strategic partner dedicated to enhancing your resilience and success in the face of evolving risks

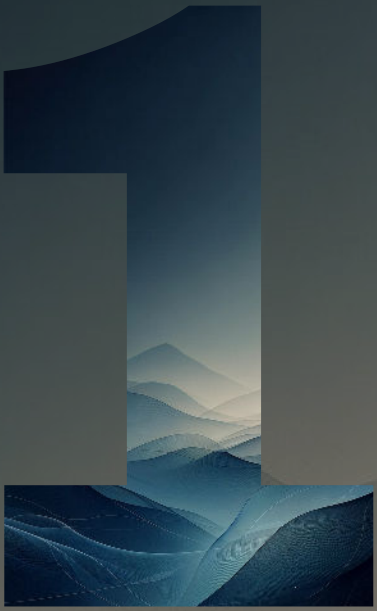
INSIDER RISK TRENDS

1. Employee Monitoring
2. Artificial Intelligence
3. Third-Party Dependency
4. Tendering

Signpost Six

Info@signpostsix.com
www.signpostsix.com

EMPLOYEE MONITORING



The demand for employee monitoring software is on the rise, mainly due to shifts in post-pandemic work dynamics and a continuous surge in data breaches within organisations. The adoption of employee monitoring tools has witnessed a significant rise in North American markets, Asia Pacific, and Europe.

A driving force behind this trend are companies seeking to enhance productivity in remote work settings, where trust between employees and employers has been compromised.

Simultaneously, the increasing prevalence of insider threats has led to a surge in organisations adopting insider risk programmes, with monitoring tools playing a crucial role in preventing and mitigating risks arising from within the organisation.

While there are situations in which employers can log and monitor the digital activities of employees and share personal data internally, how this information is collected and handled raises sensitive privacy concerns. Privacy and legal compliance are crucial factors woven throughout insider risk management programmes. These programmes encompass various elements, such as conducting background checks and screenings, implementing IT systems for logging and storing data, and conducting individual risk assessments to determine access to critical, confidential, and proprietary information, among other considerations.

Emphasising the crucial role of legal and privacy considerations within insider risk programmes and the broader insider risk approach is imperative. Anticipated for 2024 is a sustained increase in the quest for tools within the European market, where legal regulations are expected to present more significant challenges for organisations actively working towards insider threat detection and prevention.

ARTIFICIAL INTELLIGENCE

Opinions on the possibility of General Artificial Intelligence and its potential timeline differ wildly. What has become clear is that the acceleration in capabilities of Deep Learning, Machine Learning and Natural Language Processing models over the past 1,5 years is causing threats at a rate that is hard to keep up with for most organisations and people. The development of AI applications leads to very dangerous scenarios for any organisation. Examples of non-existing 'people' setting up fraud schemes through the use of voice and video generation, together with speech generation of trusted people are starting to surface and they are increasingly advanced.

Take the examples of HyperVerse for fraud or of the CNN Philippines anchors appearing to present fake stories through deepfake copies of existing anchors. The increasing prevalence of AI and technologies such as OpenAI and other language models introduces a persistent concern among several organisations: the possibility of employees misusing confidential data and the increasing number of data breaches.

Ultimately, the technological development of AI and predicted replacement of jobs will also have a direct impact on everyone in society and within organisations where stress and resentment will increase insider risk with those people who might fear losing their livelihood.

ⓘ **Hyperverse fraud case** | **Deepfake anchor**

THIRD-PARTY DEPENDENCY

Securing and retaining talent proves to be a challenge for organisations in specialised fields, with the dwindling population growth in developed economies adding to the scarcity of skilled professionals. To maintain operational continuity and reduce disruptions, organisations have increasingly turned to third parties or temporary workers, outsourcing critical services. The increasing dependence on external resources gives rise to potential issues from an insider risk perspective, particularly when these workers have access to sensitive areas within the business.

Since these workers are not fully integrated into the organisation and may lack a shared understanding of its vision and interests, trust can be weakened. In such cases, there is a risk that individuals in trusted positions could exploit their access. Likewise, malicious actors may attempt to exploit this potential trust gap with third parties, seeking to capitalise on workers' access to achieve their objectives.

Mature insider risk programmes have addressed their reliance on third-party systems by integrating third-party risk management strategies into their overall insider risk management approach. The impact of threats originating from third parties is anticipated to remain substantial in 2024.

TENDERING

Within the process of public solicitation for service, there are several security implications to take into account. We precisely want to highlight for 2024, the state-sponsor threat associated with tendering processes. As outlined by the AIVD (Dutch Intelligence Services), State actors are drawn to procurement and tendering processes, leveraging the wealth of information, especially from public documents made available. These documents explicitly outline businesses' expertise, making them identifiable targets.

Infiltration into procurement processes provides state actors with access to for example, sensitive systems and information, enabling them to establish control in the market over time, posing high-risk strategic and geopolitical dependencies in the long run. Additionally, the goods and services exchanged create opportunities for acts of sabotage and espionage. Recent years have seen reported instances of espionage risks in tendering processes involving the Dutch Ministry of Defence, the police, and other government authorities.

OUR SOLUTIONS

We are dedicated to reinforcing the security and integrity of public and private organisations. As Europe experts in insider risk, we offer three main market-leading and , customisable solutions:

Insider Risk Assessments

Insider Risk Programmes

Workshops & Training

Info@signpostsix.com
www.signpostsix.com