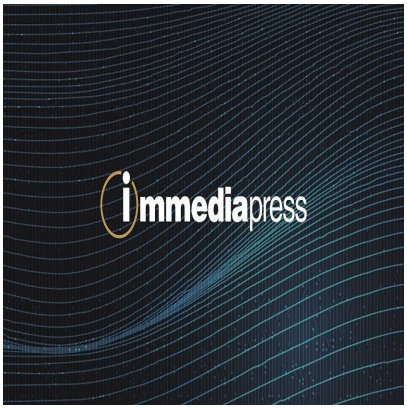


Human behaviour remains a critical blind spot in insider risk, new Signpost Six report warns

Descrizione

default watermark

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

THE HAGUE, Netherlands, Nov. 18, 2026 /PRNewswire/ â?? European organisations, particularly those in defence, critical infrastructure, and transport and logistics, are currently prime targets for disruption in the context of ongoing geopolitical conflicts. Although organisations invest in physical and digital security measures, human behaviour remains the crucial factor in every security challenge. Signpost Sixâ??s new report, The Psychology of Insider Risk, shows how human behaviour and organisational dynamics create the most significant and difficult-to-address vulnerabilities across different sectors.

The findings underline a central message: insider incidents rarely develop overnight. Psychological and behavioural factors, ranging from workplace conflict to financial pressure, personal crises, external influence and human error, can gradually change an individualâ??s behaviour and increase vulnerability to insider risk.

Insider risk is fundamentally a people-centred organisational challenge. Organisations, whether private companies, critical infrastructure operators or government institutions, now operate in an environment where hostile actors such as foreign intelligence services, organised crime groups and commercial competitors actively target employees within those organisations. These employees possess something technology cannot provide: contextual knowledge, operational insight and legitimate access.

The scale of the challenge is significant, as confirmed in a recent publication by the Netherlandsâ?? General Intelligence and Security Service (AIVD). According to other sources cited in the Signpost Six report, 83% of organisations experienced such incidents in the past twelve months, while only 23% say they are sufficiently equipped to prevent them effectively. The average cost to an organisation can reach â?¬17.5 million annually, with the impact of incidents becoming increasingly sensitive in the defence and critical infrastructure sectors.

The report shows that organisations cannot rely solely on technical security measures to address a fundamentally people-centred risk. Having the full overview of existing vulnerabilities is an essential starting point. An effective approach to insider risk requires organisations to recognise and analyse behavioural changes and technical anomalies.

In addition, physical security measures must be combined with monitoring unusual behaviour, strengthening employee resilience, and the ability to respond rapidly. Against the backdrop of the current geopolitical situation, it is becoming increasingly urgent for European organisations to rapidly strengthen awareness and resilience in relation to insider risk.

Full report: The Psychology of Insider Risk

View original content to download multimedia:https://www.prnewswire.co.uk/news-releases/human-behaviour-remains-a-critical-blind-spot-in-insider-risk-new-signpost-six-report-warns-302942479.html

Copyright 2026 PR Newswire. All Rights Reserved.

default watermark

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE: Immediapress Ã¨ un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dallâ??ente che lo emette. Lâ??Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi

â??

immediapress/pr-newswire

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Novembre 18, 2026
Autore
redazione