INSIDER RISK TREND REPORT 2026

SIGNPOST SIX
www.signpostsix.com
info@signpostsix.com

WHAT IS INSIDER RISK?

Insider risk is increasingly recognised as a key security challenge for European organisations. It refers to the potential risk posed by individuals within or closely connected to an organisation - such as employees, contractors, or third parties - who have authorised access to sensitive information and systems and may misuse that access intentionally or unintentionally. Recent industry surveys indicate that 76% of organisations experience insider incidents in the past 12 months, up from 66% in 2019. At the same time, only 30% of high-risk European organisations have (partially) implemented an insider risk programme, underscoring a persistent implementation gap.

It therefore doesn't come as a surprise that **84% of organisations do not feel well equipped to detect and handle insider incidents.** Over the past years, we have seen insider risk move from a niche concern to a structural vulnerability shaped by wider economic, technological, and geopolitical pressures. Governments worldwide warn organisations about the growing number of threats from within, signalling that insider risk is no longer just a sector-specific issue but a systemic one that touches government, critical infrastructure, and the private sector alike. At the same time, many organisations still treat insider risk mitigation as non-essential, prioritising short-term financial performance over investment in resilience. This delay in adaptation is visible in the gap between the evolving threat landscape and the slower pace of regulation.

The Insider Risk Trend Report 2026 builds on Signpost Six's advisory work, drawing on the expertise of our advisers, our wide-ranging client portfolio, and close collaboration with knowledge partners to identify the key insider risk trends for 2026 that organisations should integrate into their security practices.

Signpost Six

TABLE OF CONTENTS

Signpost Six

FROM GEOPOLITICAL THREATS TO INSIDER RISK TRENDS

Geopolitical tensions have escalated rapidly over the past year. Intensified (hybrid) conflicts, disrupted global supply lines, and shifting power dynamics are reshaping the risk landscape. It is therefore essential to translate these macro forces into specific, actionable insider risk challenges.

By drawing on Signpost Six's extensive client experience across critical sectors, insights from our specialist advisers, and deep geopolitical knowledge, we have identified four key geopolitical developments that frame twelve insider risk trends for 2026. Each geopolitical development directly influences current insider risk trends by creating new entry points and pressure factors for insiders. The structure of the report addresses major systemic risks while highlighting the practical challenges they create for any organisations and how they should be addressed.

GEOPOLITICAL DEVELOPMENT I

HYBRID WARFARE IN THE COMMERCIAL DOMAIN

GEOPOLITICAL DEVELOPMENT II

GLOBALISED SUPPLY CHAINS AND SYSTEMIC FRAGILITY

GEOPOLITICAL DEVELOPMENT III

RISE OF IDEOLOGY AND ACTIVISM IN THE WORKPLACE

GEOPOLITICAL DEVELOPMENT IV

ACCELERATING DIGITAL TRANSFORMATION

Sign post Six

HYBRID WARFARE IN THE COMMERCIAL DOMAIN

GEOPOLITICAL DEVELOPMENT I

Traditional military confrontation is giving way to hybrid strategies. This entails combinations of cyber operations, disinformation, economic pressure, and proxy activity aimed at achieving political goals below the threshold of open conflict. At the same time, globalisation has expanded the strategic relevance of private companies. Tech firms, critical infrastructure operators, aerospace companies, and suppliers of essential materials now sit at the centre of geopolitical competition. Sabotage and espionage acts against these entities deliver high-impact disruption without prompting direct state-to-state escalation. As a result, commercial organisations are no longer peripheral observers but frontline terrain in hybrid warfare. As hybrid warfare increasingly targets and infiltrates commercial organisations, the human element becomes a critical vulnerability. State actors and their proxies rely on insiders for access, deniability, and operational leverage transforming insider risk from a primarily internal security to a broader business risk.

TREND 1
NEXUS NATION-STATE ACTORS AND ORGANISED CRIME

Hybrid warfare in the commercial domain increasingly relies on a nexus between nation-state actors and organised crime networks. State actors can activate criminal infrastructures to execute deniable operations against private or public targets. This emerging trend sees states leveraging established criminal groups for influence operations, disinformation, and sabotage. These methods substantially blur the line between state-directed action and independent crime. Russia, for instance, utilises its extensive global criminal networks very effectively to drive cyber-attacks and sabotage of physical infrastructure. Other powers such as China are developing similar capabilities through diaspora networks, commercial influence, and economic coercion, although the degree of integration varies per state actor.

Sign post Six

From an insider risk perspective, this nexus creates profound vulnerabilities by turning organised crime into a primary vector for state-sponsored threats. Criminal groups often recruit, coerce, or bribe insiders with offers of payment, protection, or ideological alignment. These insiders, like employees, contractors, or vendors, grant access to systems, facilities, or sensitive data, facilitating ransomware attacks tailored for espionage, supply-chain interference, or data exfiltration that advance both criminal profits and geopolitical aims. Unlike traditional state intelligence operations, these criminal tactics often rely on violent or blunt methods, directly endangering employees through intimidation, coercion, or retaliation.

SIGNPOST SIX ADVICE

The increasingly intertwined threat landscape demands proactive insider risk measures. Employees require targeted training to recognise distinct recruitment tactics, from financial incentives to ideological appeals. They should understand the consequences of engagement, such as personal liability or organisational sabotage. By building awareness, organisations can disrupt the nexus at its human entry point, turning potential insiders into sentinels rather than vulnerabilities.

CASE STUDY

In October 2024, Spanish police in Barcelona seized 13 tons of banned chemical solvent NMP (critical for nerve agents and missile components) from shipments orchestrated by the Oleinikov family, a Russian diaspora business network running wine exports as cover. Russian intelligence leveraged this established criminal smuggling channel to funnel dual-use goods via Armenia, Kyrgyzstan, and Belarus to sanctioned recipients like GosNIIOKhT, the "Novichok" developer. Katrosa Reaktiv, the end-user, supplied Russia's military-industrial complex. This illustrates Moscow's extensive criminal networks enabling hybrid warfare through deniable sanctions evasion. Insiders at logistics firms become unwitting or coerced vectors in instances like this geopolitical sabotage.

TREND 2
CRITICAL INFRASTRUCTURE AS TARGET IN HYBRID WARFARE

Across Europe and beyond, critical infrastructure is becoming a frontline in hybrid warfare. This trend particularly affects ports, energy facilities, logistics chains, telecommunications networks, and digital service providers. These sectors sit at the intersection of economic continuity and national security, making them attractive to a wide spectrum of actors, including state intelligence services, state-aligned proxies, and organised crime groups. The number of sectors affected has expanded significantly: ports face criminal infiltration for smuggling, while energy and telecom operators experience probing by state actors seeking leverage or disruption potential. This creates a complex threat environment for commercial operators, who must defend themselves against multiple adversaries simultaneously. Different actors may uses overlapping tactics like insider recruitment or sabotage, while pursuing different objectives such as competitive gain, geopolitical leverage or military advantage. It is important to highlight the importance of this trend, as critical infrastructure is structurally more exposed than at any previous moment in history.

In addition, digitalisation has fused physical infrastructure with tech infrastructure, meaning that operational continuity increasingly depends on a small number of technology platforms, such as cloud providers, identity-access managers, data-logistics systems, and industrial control software. These digital layers create high-value single points of failure, enabling hostile actors to cause large disruption through relatively small footholds. Attacks on a port terminal or logistics platform are no longer isolated physical risks: they are amplified by dependencies on digital systems that, if compromised, can cascade across national and international supply chains. This heightened sensitivity and interconnectivity make critical infrastructure an even more strategic target in hybrid warfare.

As a result, the targeting of critical infrastructure in hybrid warfare significantly elevates insider risk within these sectors. A single insider with technical, operational, or logistical access can trigger far-reaching consequences, whether acting intentionally or under manipulation. Foreign intelligence services increasingly view such insiders as efficient tools for reconnaissance. This insider risk manifests through subtle, non-destructive actions that lay the groundwork for larger campaigns. Insiders may map systems, copy access protocols, or quietly degrade response capacity, providing state actors with leverage without immediate detection.

These footholds enable disruptions across national and international networks when activated. Moreover, critical infrastructure employees often underestimate the potential geopolitical value of their work, creating a low-awareness environment that enables social engineering, recruitment through professional networking platforms, or covert influence. The complexity of modern infrastructure, where contractors, vendors, and third-party IT providers have access to core systems, amplifies this risk.

SIGNPOST SIX ADVICE

Organisations within critical infrastructure should develop or expand insider risk capabilities beyond traditional fraud and criminal prevention. This includes implementing insider risk awareness, mapping access pathways, and monitoring for unusual behaviour and social-engineering indicators, which reflect their frontline role in modern hybrid warfare.

CASE STUDY

Russian ransomware groups like LockBit have hit European hospitals, energy grids, and logistics firms since 2022, crippling operations while extorting ransoms. Europol confirms these attacks often align with Kremlin goals of economic disruption, with gangs enjoying safe haven and occasional tasking from Russian intelligence. From an insider risk perspective, criminals recruit or coerce company insiders, via bribes or threats, to deploy malware or leak access credentials, blending profit-driven crime with state-sponsored sabotage in commercial environments.

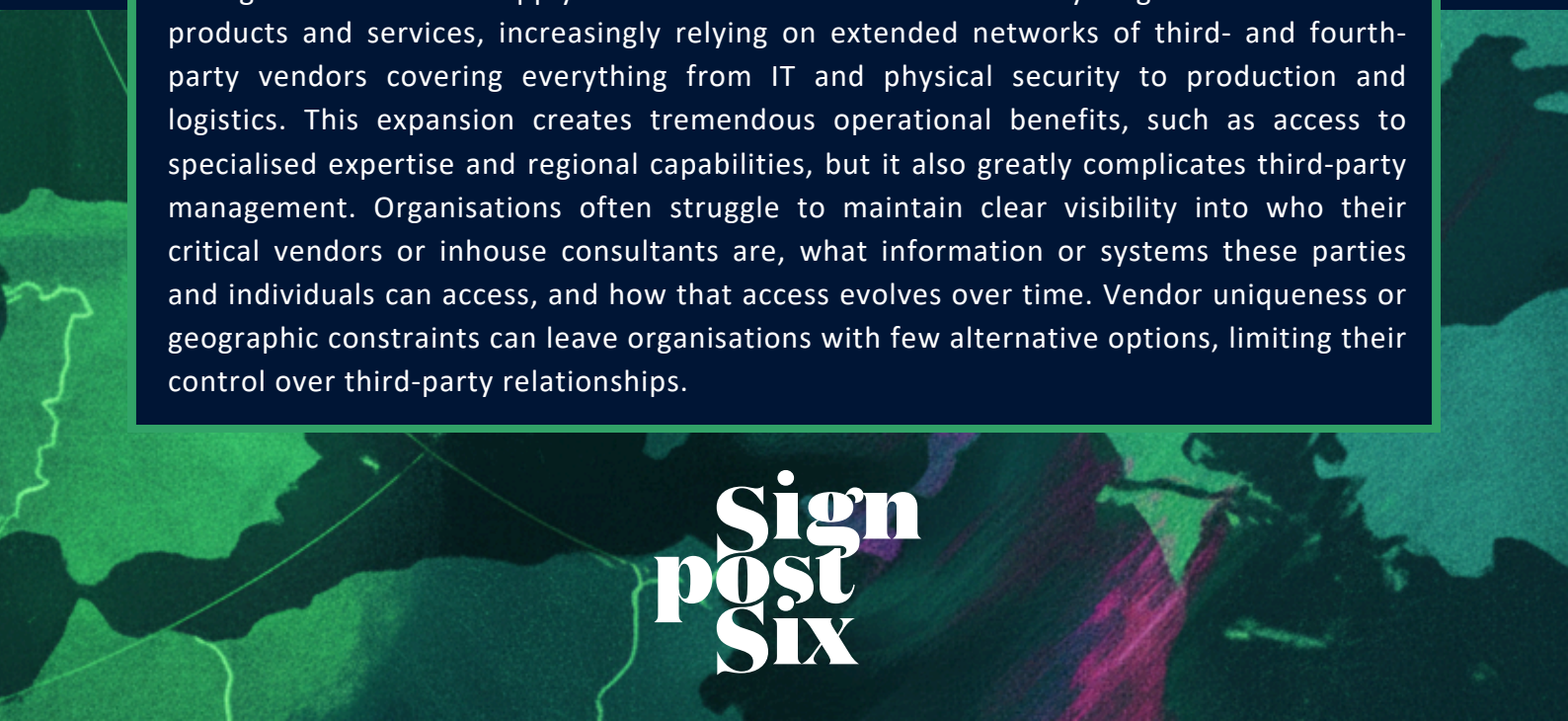
GLOBALISED SUPPLY CHAINS AND SYSTEMIC FRAGILITY

GEOPOLITICAL DEVELOPMENT II

The globalisation of supply chains has created vast, interconnected networks that enable unprecedented efficiency, scale, and specialisation. However, this complexity has also introduced systemic fragilities: organisations now depend on multi-tiered vendors, dispersed physical infrastructure, and fluid labour pools that they often struggle to oversee or control. As responsibilities diffuse across regions, agencies, and contractors, visibility into who has access to what and why, declines sharply. Recent geopolitical tensions and military posturing around critical chokepoints and regions, from manoeuvres near Taiwan to sanctions-enforcement seizures and inspections of tankers and other contested shipping corridors, further expose how quickly trade routes can be weaponised, amplifying systemic fragility and opening new areas of risk. These structural weaknesses directly translate into new insider risk trends. Third-party vendors, temporary workers, and supply chain partners now hold critical access, often without consistent screening, monitoring, or governance. Physical vulnerabilities across warehouses and transport routes further expand opportunities for insider-enabled theft, sabotage, or geopolitical exploitation. In globalised supply chains, insider risk is no longer confined within organisational boundaries but embedded throughout the entire operational ecosystem.

TREND 3
LACK OF OVERSIGHT OVER THIRD PARTIES

The globalisation of supply chains has transformed the way organisations deliver products and services, increasingly relying on extended networks of third- and fourth-party vendors covering everything from IT and physical security to production and logistics. This expansion creates tremendous operational benefits, such as access to specialised expertise and regional capabilities, but it also greatly complicates third-party management. Organisations often struggle to maintain clear visibility into who their critical vendors or inhouse consultants are, what information or systems these parties and individuals can access, and how that access evolves over time. Vendor uniqueness or geographic constraints can leave organisations with few alternative options, limiting their control over third-party relationships.



This complexity translates directly into heightened insider risk. Poorly tracked or unmanaged access rights create opportunities for misuse, errors, or infiltration. Examples include unrevoked building passes, shared consultant teams, or unexplained IT system access requests.The longer and more fragmented the vendor relationship, the more likely it is that vendors retain unnecessary access over time, increasing insider risk and vulnerabilities within external teams. Many organisations find themselves “hands-tied”, unable to enforce consistent security standards or behavioural monitoring across dispersed suppliers, especially when access requests lack clear justification or oversight.

SIGNPOST SIX ADVICE

Organisations should strengthen supplier risk management by incorporating insider risk considerations beyond organisational boundaries. Clear and consistent third party on- and offboarding processes, supported by robust access and contract management, are advised to reduce the likelihood of insider-related incidents and can prevent critical breaches.

CASE STUDY

In 2025, Marks & Spencer suffered a major outage when a criminal group compromised a third-party provider with trusted access into M&S core systems. The attack forced M&S to shut down large parts of its IT environment, pausing online orders for weeks and disrupting store availability, with tens of millions in lost sales. The incident illustrates how external technicians and vendor staff effectively become insiders: once their accounts are abused or hijacked, attackers move through the same remote access channels, change configurations, and reach sensitive customer and operational data. Weak oversight of who holds which access at suppliers turned one compromised partner into a systemic insider risk vector.

TREND 4
PHYSICAL SUPPLY CHAIN FRAGILITY

The globalised supply chain has enabled unprecedented efficiency and reach but has also introduced fragilities, especially in the physical infrastructure that supports production, storage, and transit. Physical supply chains involve warehouses, transport hubs, distribution centres, and critical infrastructure that are increasingly dispersed across multiple countries and controlled by various actors. This complexity creates vulnerabilities to theft, sabotage, and physical disruption. Such attacks, which may be criminal in nature or part of hybrid warfare campaigns, often require detailed knowledge of facilities, logistics, and timing, making insider knowledge or access critical for success. The physical fragility of supply chains is an inherent risk in globalised systems where security responsibility is diffused among numerous stakeholders.

As a result, insiders can become the linchpin in exploiting these vulnerabilities, whether as employees, contractors, or third-party personnel providing essential intelligence, access, or direct facilitation for theft or sabotage.Without effective insider risk controls organisations face heightened exposures to deliberate disruption, covert sabotage, or theft of valuable goods and information. These insider-enabled physical threats can be leveraged by organised crime groups or hostile state actors as part of broader geopolitical strategies targeting economic resilience and operational continuity.

SIGNPOST SIX ADVICE

Organisations should strengthen physical security measures at warehouses and transit points while ensuring that access to schedules and logistics information is tightly controlled. By aligning physical security practices with accountability, organisations can protect operational continuity.

TREND 5
GHOST WORKERS IN THE GLOBAL SUPPLY CHAIN

The globalisation of supply chains has accelerated the use of flexible labour models, with organisations increasingly hiring temporary workers, contractors, and specialists through third-party employment agencies and staffing firms. This approach provides rapid access to global talent pools, cost flexibility, and specialised skills needed for complex, and multi-regional operations, from manufacturing lines to logistics hubs. However, it often comes at the expense of visibility into workers' backgrounds. Agencies may conduct minimal or no screening, or withhold personal data due to privacy regulations, contractual limits, or competitive practices, leaving the hiring organisation without critical information on identities, prior employment, financial status, or affiliations.

This opacity translates into acute insider risk trends within globalised supply chains. Without personal data or vetting, organisations cannot assess key indicators for insider risk. Temporary workers gain physical or digital access to facilities, systems, or sensitive operations, yet remain effectively anonymous insiders. In supply chain contexts, this blind spot enables sabotage, theft, data exfiltration, or espionage, particularly when agencies source from high-risk regions. Geopolitically, adversarial states or organised crime can exploit these "ghost workers" to infiltrate critical nodes, turning labour flexibility into a strategic weakness.

SIGNPOST SIX ADVICE

Organisations should prioritise employee lifecycle management for all workers with access to facilities, transport routes, and logistics operations. This includes pre-employment vetting, solid on- and offboarding processes, and ongoing review of access for temporary, contracted, and agency-supplied personnel.

TREND 6
FRAGMENTED DEFENCE SUPPLY CHAIN RISKS

Shifting geopolitical priorities are particularly visible in transatlantic relations: recent US foreign and defence policy signals have made clear that sustaining the EU–US security alliance, including commitments within NATO, is no longer treated as an unquestioned long-term priority, even as Europe faces an active war on its own continent. This has pushed EU states to accelerate defence industrial cooperation, seek greater strategic autonomy, and reduce dependence on US-origin capabilities, directly influencing how they design and localise their defence supply chains. At the same time, a shift in warfare away from exclusively traditional hardware towards dual-use technologies such as drones, satellites, and AI-enabled systems has further expanded the range of capabilities required. Defence firms therefore no longer source from a limited number of traditional suppliers focused mainly on tanks and weaponry. Instead, Europe's defence sector increasingly relies on a sprawling network of hundreds of regional and global suppliers, including commercial and dual-use technology providers, to modernise and diversify capabilities while reducing single-country reliance.

This burgeoning and fragmented defence supply chain creates significant insider risk challenges. The sheer number and variety of suppliers greatly increase the potential for access misuse, espionage, or sabotage. Many of these suppliers operate under commercial arrangements that are not custom-designed for defence security. Organisations face difficulty auditing and monitoring thousands of tiered suppliers, many with highly sensitive knowledge or capabilities critical to military operations. The insider risk surface thus broadens beyond government or prime contractors to include a diffuse ecosystem of tech firms and subcontractors operating under varying regulatory and cultural norms.

SIGNPOST SIX ADVICE

Defence-sector organisations, in particular, should set clear expectations regarding security and insider risk standards for all collaborating suppliers, ensuring that third- and fourth parties adhere to best practices that mitigate insider risk and protect national security amid growing geopolitical tensions.

INTERESTED IN LEARNING MORE ABOUT INSIDER RISK IN THE DEFENCE SECTOR? READ OUR INDUSTRY ANALYSIS HERE

RISE OF IDEOLOGY AND ACTIVISM IN THE WORKPLACE

GEOPOLITICAL DEVELOPMENT III

There is a global rise in visibility of ideology and activism that represents a profound shift in public engagement. This is driven in part by social media, which amplifies opinions and accelerates mobilisation. At the same time, generational value differences and increasingly polarised debates on social, ethical, economic, and geopolitical issues shape how people see institutions and authority. Movements mobilise rapidly around labour rights, climate action, migration policies, national sovereignty, and international conflicts, challenging traditional institutions and norms with unprecedented visibility and intensity.

This phenomenon translates directly into insider risk trends within organisations, as employees increasingly filter corporate practices through personal ideological lenses. Staff may view employers as complicit in objectionable policies, leading to leaks of sensitive data, operational sabotage, or alliances with external activists. Polarisation erodes internal trust, while activism creates exploitable fractures that adversaries can target. These dynamics underscore the need for clear conduct guidelines, neutral conflict resolution, and cultural safeguards to transform potential threats into managed risks.

TREND 7

POLITICAL POLARISATION INSIDE ORGANISATIONS

Political debates around economic inequality, immigration, climate change, national sovereignty, and international conflicts have gained visibility online. Once more contained within specific communities, these discussions now dominate mainstream and online spaces, amplified by politicians, media outlets, and digital platforms. This heightened visibility increasingly seeps into workplaces, where employees may bring political views into meetings, internal communications, and collaborative environments. This often also manifests on the internal communication platforms within companies, which can be used as spaces for political expression or discussion. When such exchanges become heated and unaddressed, they can erode teamwork, trust, and morale, thereby undermining organisational cohesion and effectiveness.

Sign post Six

From an insider risk perspective, polarisation in the workplace can have serious implications. Employees who feel fundamentally at odds with their organisation's stance on political or ethical matters may engage in harmful acts, such as leaking information, sabotaging projects, or colluding with external groups to advance an ideological cause. Escalated tensions can also lead to instances of harassment or workplace violence, particularly when polarisation interacts with personal stressors or external propaganda. In tense geopolitical situations, hostile actors may even attempt to exploit these divisions to stir unrest or manipulate insiders for their own goals

SIGNPOST SIX ADVICE

Organisations should watch for signs of rising tensions, set clear rules for communication, and manage conflicts fairly to keep the workplace stable and safe. Moreover, organisations are encouraged to invest in a workplace culture that is based around values that are shared among employees and are well communicated within the organisation.

TREND 8
VALUE-BASED TENSIONS AROUND WORKING CONDITIONS

Growing global awareness about working conditions is a significant part of the broader rise in visibility of ideology and activism. Employees today are increasingly informed and concerned about how labour is conducted, extending beyond their immediate organisation to the entire supply chain. Social media and transparency initiatives shed light on labour practices worldwide, inspiring activism aimed at fair treatment, sustainability, and ethical business conduct. At the same time, inside organisations, expectations around work-life balance, flexible hours, and respect for personal well-being have shifted profoundly, driven in part by generational differences. Younger employees tend to advocate for greater autonomy and hybrid work options, viewing these as fundamental rights, while some older workers may feel sidelined or undervalued amid technological and cultural changes. The traditional hierarchical workplace is giving way to more open dialogues, though tensions remain.

From an insider risk perspective, we see that these shifts create new challenges. Discontent stemming from perceived unfair treatment or unmet expectations can lead to insider grievances, reduced loyalty, and higher turnover. Employees may become more prone to sharing sensitive information externally, disengaging from security practices, or sabotaging operations. Additionally, activism can motivate insiders to expose or disrupt business if they believe organisational practices conflict with their values.

SIGNPOST SIX ADVICE

Organisations should recognise the risks arising from ideological and generational divides. Proactive engagement with employees' expectations, supported by transparent communication enables organisations to identify emerging concerns early and mitigate vulnerabilities before they escalate.

TREND 9
ACTIVISM AS A WORKPLACE RISK

Building on the broader rise of political polarisation within organisations, a growing number of employees are now moving beyond internal disagreement to active participation in ideological causes. This shift reflects a more assertive form of values-based engagement, where employees see their workplace not only as a professional environment but also as a platform for moral or political expression. Movements across the ideological spectrum, from environmental and social justice campaigns to nationalist and conservative causes, are increasingly influencing employee behaviour.

From an insider risk perspective, activism blurs the boundaries between personal conviction and organisational responsibility. Employees who view their organisation's business practices, clients, or partnerships as conflicting with their personal values may resort to disruptive acts such as leaking information, damaging company assets, or coordinating internal protests and digital mobilisation. This risk extends beyond the workplace: external activism, especially when directed at or conflicting with the organisation's activities, can heighten exposure by creating reputational, operational, or data-security vulnerabilities. Incidents like these show how moral conviction can escalate from expression to direct insider risk, particularly in sectors linked to geopolitically sensitive contracts.

SIGNPOST SIX ADVICE

Organisations should have structured internal channels in place where employees can voice ethical concerns. Encouraging dialogue within defined boundaries allows employees to voice disagreements constructively while maintaining organisational integrity. In addition, high-target organisations may consider social media screening to spot potential ideological perspectives that pose a threat to the organisation's security.

CASE STUDY

In August 2025, Microsoft employees staged protests at company headquarters in Redmond, Washington, occupying a senior executive's office and raising a Palestinian flag to oppose Microsoft's cloud contracts with the Israeli military. Organised by "No Azure for Apartheid," the activists demanded an end to ties enabling surveillance and operations in Gaza. Four staff were fired following the sit-in, amid escalating internal tensions.

From an insider risk perspective, this demonstrates how ideological opposition to corporate partnerships can lead to direct confrontation. Office occupations and public statements risk operational disruption, reputational damage, and potential leaks of contract details or client data to external groups. In tech sectors with geopolitical contracts, such activism creates vulnerabilities where disaffected insiders may escalate from protest to sabotage or information sharing.

ACCELERATING DIGITAL TRANSFORMATION

GEOPOLITICAL DEVELOPMENT IV

Accelerating digital transformation is reshaping how organisations operate by embedding advanced technologies like AI, cloud computing, and remote collaboration into core business processes. This global trend expands operational efficiency and workforce reach but also creates complex ecosystems where data, access, and trust span internal teams, external vendors, and digital platforms worldwide. As digital tools become deeply integrated in hiring, onboarding, and IT management, the insider risk landscape evolves dramatically.

From an insider risk perspective, this transformation opens new vulnerabilities while amplifying existing ones. Sensitive data is increasingly handled by AI systems with limited transparency, remote employees operate beyond conventional supervision, and third-party vendors often retain elevated access to networks and information. These developments make it harder for organisations to maintain visibility and control over who has access to what, and why. To stay resilient, insider risk management must evolve alongside digital transformation, embedding governance, monitoring, and access control into every stage of technological adoption.

TREND 10

RECRUITMENT AUTOMATION AS AN INSIDER RISK VECTOR

AI's rapid spread into hiring and workforce management is a clear expression of the broader global push towards digitalisation. Organisations under cost and talent pressure increasingly automate recruitment steps: CV screening, video interviewing, candidate scoring, and even chat-based "first-round interviews" are delegated to AI-driven platforms. At the same time, employees and recruiters' experiment with public AI tools to draft job ads, refine CVs, or prepare interview questions, often with little governance. This creates dense digital hiring ecosystems in which large volumes of personal and organisational data circulate across tools and vendors, frequently outside clear security or compliance frameworks.

Sign post Six

From an insider risk perspective, this digitalisation trend produces several specific vulnerabilities. First, sensitive information (about roles, systems, assessment content, and internal processes) is pasted into AI tools, unintentionally feeding external models with data that can later be exploited for profiling or social engineering. Second, AI-led interviewing and scoring can weaken effective screening: automated systems are poor at detecting inconsistencies, behavioural red flags, or geopolitical risk indicators in high-risk roles. Third, hostile actors can weaponise the same technologies: deepfake video and synthetic audio make it possible to pass remote interviews under a fabricated identity, including for IT, finance, or critical infrastructure positions. Together, these developments turn AI in hiring and screening from a neutral efficiency tool into a strategic insider risk vector that organisations cannot afford to ignore.

SIGNPOST SIX ADVICE

Organisations should establish AI acceptable use guardrails, such as defining approved tools, data-sharing limits, and governance for recruitment AI to counter these risks. For high-risk roles, organisations may consider requiring fully in-person recruitment processes to ensure thorough vetting. Similarly, implement mandatory in-person ID verification for all hires before onboarding.

CASE STUDY

North Korean IT workers systematically exploit automated hiring platforms, using ChatGPT to generate fake resumes, LinkedIn personas, and culturally fluent interview responses while applying to dozens of jobs en masse. Browser histories from Democratic People's Republic of Korea (DPRK) computers reveal heavy AI faceswap software, VPNs, and ChatGPT, not just for code, but to fabricate entire identities, rehearse small talk (Thanksgiving greetings, football rules), and pass video screens. Their mass applications overwhelm outsourced recruiting systems unable to detect geopolitical actors. Cybersecurity company Palo Alto Networks confirms DPRK's early, prolific AI adoption even contributed to model training we use today. This reveals recruitment automation's core insider risk: AI tools that hostile actors weaponise become perfect camouflage for state-backed infiltration, bypassing human vetting entirely.

TREND 11
REMOTE WORK'S VULNERABLE FOUNDATIONS

Remote and hybrid work have become a permanent feature of the digitalised global economy, rather than a temporary response to the pandemic. Large organisations increasingly run entire teams, projects, or functions fully remotely, from recruitment and onboarding to daily collaboration and performance management. This supports global talent sourcing and cost-efficiency, but also normalises relationships where key contributors are never physically met, devices are personally owned, and most interactions occur through easily spoofed digital channels such as video calls, messaging apps, and email. As more of the organisational lifecycle moves online, trust is mediated through screens and credentials rather than shared physical environments or social cues.

This shift creates distinct insider risk patterns. Fully remote hiring and onboarding make it easier for impersonators and shell entities to embed themselves in organisations, as seen in the trend 10 case study. Remote workers operating from home or public networks increase the attack surface: compromised Wi-Fi, shared devices, and weak endpoint controls can be exploited by external actors, who then pivot through legitimate insider accounts. At the same time, managers have fewer opportunities to notice behavioural changes, access misuse, or subtle indicators of coercion, stress, or divided loyalties. In combination, these factors mean that remote work, if not governed with robust verification, monitoring, and access control, can turn legitimate employees or contractors into powerful enablers for espionage, data theft, fraud, or politically motivated disruption.

SIGNPOST SIX ADVICE

Organisations should train hiring managers on recognising red flags and require at least one-time in-person ID verification for high-remote roles. Organisations should also define clear exception policies informed by country risk assessments and enforce minimum controls for remote working, like privacy screens and the use of mobile hotspots over public WiFi networks.

TREND 12
FRAGILE VENDOR DEPENDENCE

The global digitalisation trend has driven many large organisations, including government agencies, to outsource significant portions of their IT infrastructure and access management to third-party vendors. This strategy provides technical expertise, scalability, and operational efficiency, but also introduces complex layers of external access points. These vendors often have broad system privileges without adequate transparency or control, and organisational oversight over who holds ongoing access (especially after employee offboarding) is frequently limited. This creates vulnerabilities that traditional perimeter and internal controls may not fully address.

From an insider risk perspective, third-party IT providers and vendor dependence create serious new vulnerabilities. External vendors gain deep access to systems and data, essentially becoming insiders, but without the same loyalty, training, or oversight as your own staff. Their global teams, differing security standards, and complex contracts make it hard to enforce strict access rules or spot unusual behaviour. These structural weaknesses become even more acute when vendors change ownership. Mergers and acquisitions can quietly shift who ultimately controls your data and admin access, often before contracts or oversight are updated. Geopolitical issues, such as foreign acquisitions (as in the Zivver case), therefore add another layer: laws like the US CLOUD Act could compel vendors to hand over data, even if stored in Europe.

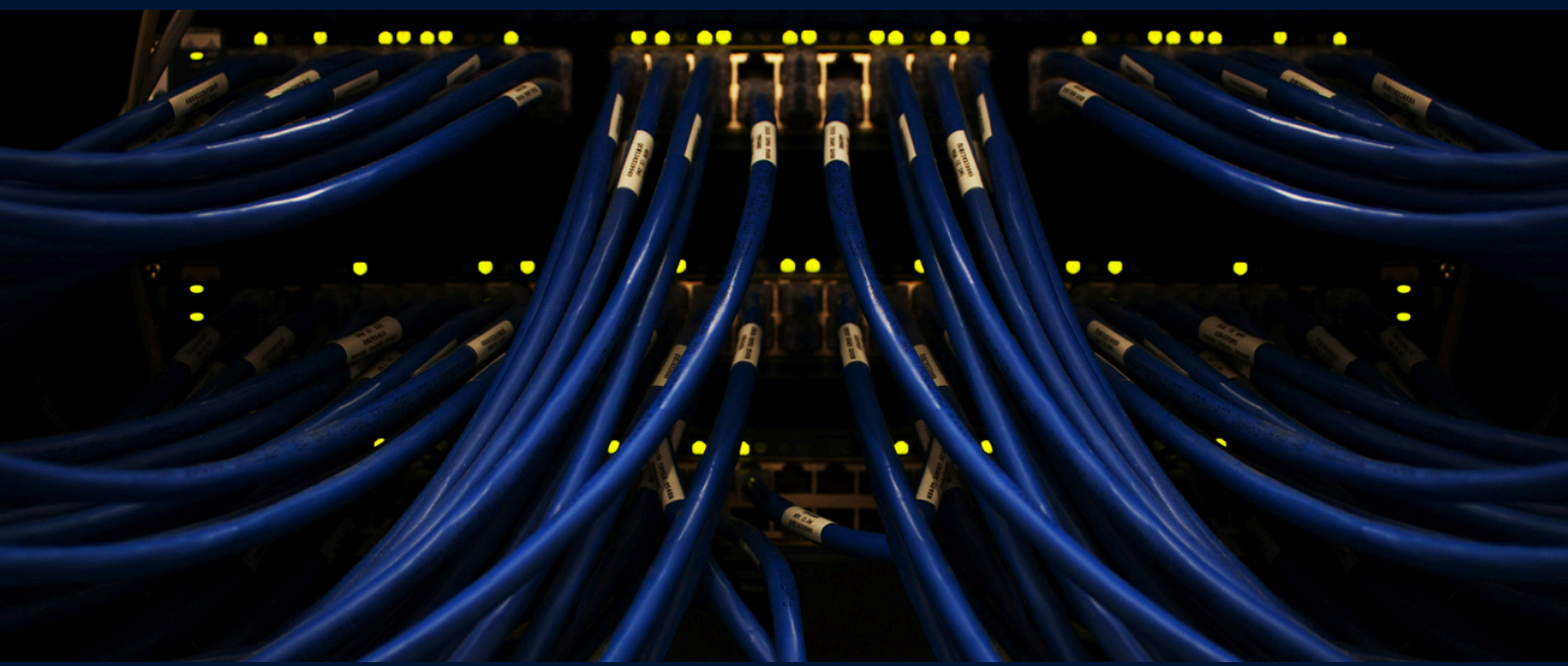
SIGNPOST SIX ADVICE

Organisations should recognise that attackers may exploit vendor employees through social engineering, bribery, or error, turning trusted partners into threat vectors. This broader attack surface is often missed by inward-focused security, making supplier monitoring, regular access reviews, and geopolitical and M&A risk assessments essential.

CASE STUDY

The acquisition of Zivver, a trusted European secure communication platform used extensively by municipalities, ministries, courts, and healthcare institutions, by the US-based company Kiteworks exemplifies the insider risk challenges stemming from IT outsourcing and vendor dependence. Zivver's robust security features, including two-factor authentication, end-to-end encryption, and compliance with GDPR and BIO, have made it a cornerstone of sensitive government and healthcare communications across Europe. Crucially, Zivver and its parent company do not hold encryption keys, and data is stored within Europe using private cloud and on-premise hosting, reducing third-party access risks.

However, the transfer of ownership to a US firm raises serious jurisdictional concerns, mainly due to US laws like the CLOUD Act, which can compel access to data regardless of its physical location. This legal overreach risk threatens digital sovereignty and could potentially expose sensitive information to foreign government demands. For public sector organisations, this case underscores the need for stringent contract management, transparency demands, and exploring European alternatives to mitigate the insider risks introduced by foreign IT vendor dependencies. It illustrates how digitalisation combined with globalised vendor ecosystems can erode control over critical data flows and insider risk governance.



HOW TO MANAGE INSIDER RISK
COMMON CHALLENGES IN INSIDER RISK MANAGEMENT

Against the outlined backdrop, many organisations recognise insider risk in theory but remain ill-prepared in practice. Organisations with a high risk profile, such as high-tech corporates and critical operators, may already run insider risk programmes. Yet, these efforts are often siloed and reactive due to a lack of governance and effective strategy. Insider risk programmes tend to be anchored in a single function, such as security, HR, or risk, without a truly holistic, organisation-wide approach. As a result, programmes concentrate on point solutions (background checks, monitoring tools, disciplinary procedures) rather than an integrated framework that spans culture, governance, access management, legal foundations, and response capabilities. This chapter highlights common organisational challenges in insider risk management.

STRATEGIC OWNERSHIP OF INSIDER RISK

"Who owns the problem?" is the question that poses a recurring issue in insider risk programmes. In some cases, governments and regulators are the main drivers and funders of insider risk initiatives, especially where national security or organised crime is at stake. Organisations follow when external funding or compliance pressure exists, but do not always prioritise insider risk as a strategic risk. However, for any effective insider risk programme it is essential to have a strategic ownership on a leadership level, instead of parking the responsibility within specific departments.

Ownership is also frequently pushed to security, or risk teams, whilst these domains may have competing priorities, different professional languages, and fragmented information flows, resulting in weak communication and a lack of shared situational awareness. This can lead to inconsistent decision-making, gaps between policy and practice, and missed warning signs when no single function has a full view of insider incidents. Rather than leaving insider risk dispersed and reactive, organisations should designate a senior accountable with a clear mandate, budget, and authority to coordinate across HR, security, risk, legal, and operations.

INSIGHT INTO BASELINE MATURITY LEVELS

For effective insider risk management, having a clear insight into organisational maturity against insider risk is essential, yet remains a common challenge for both public and private organisations. Without an understanding of their current maturity, organisations lack visibility into where their critical vulnerabilities lie and how insiders could realistically exploit weaknesses across people, processes, and technology. This absence of insight makes it difficult to prioritise controls, allocate resources effectively, and measure progress over time. As a result, insider risk management efforts are often reactive rather than strategic, compounded by the absence of basic building blocks that form the foundation of effective mitigation.

HOLISTIC APPROACH OF INSIDER RISK MITIGATION

Insider risk management requires a holistic approach that integrates both preventive and reactive controls across multiple organisational domains, including governance, culture, human resources, cybersecurity, and physical security. In practice, many organisations experience difficulty in designing and implementing such an integrated framework, as responsibilities and controls are often distributed across separate functions and managed in isolation. This fragmented approach limits the effectiveness of insider risk mitigation.

ONLY 16% OF ORGANISATIONS FEEL CONFIDENT IN HANDLING INSIDER RISK

MEASURABILITY OF IMPACT

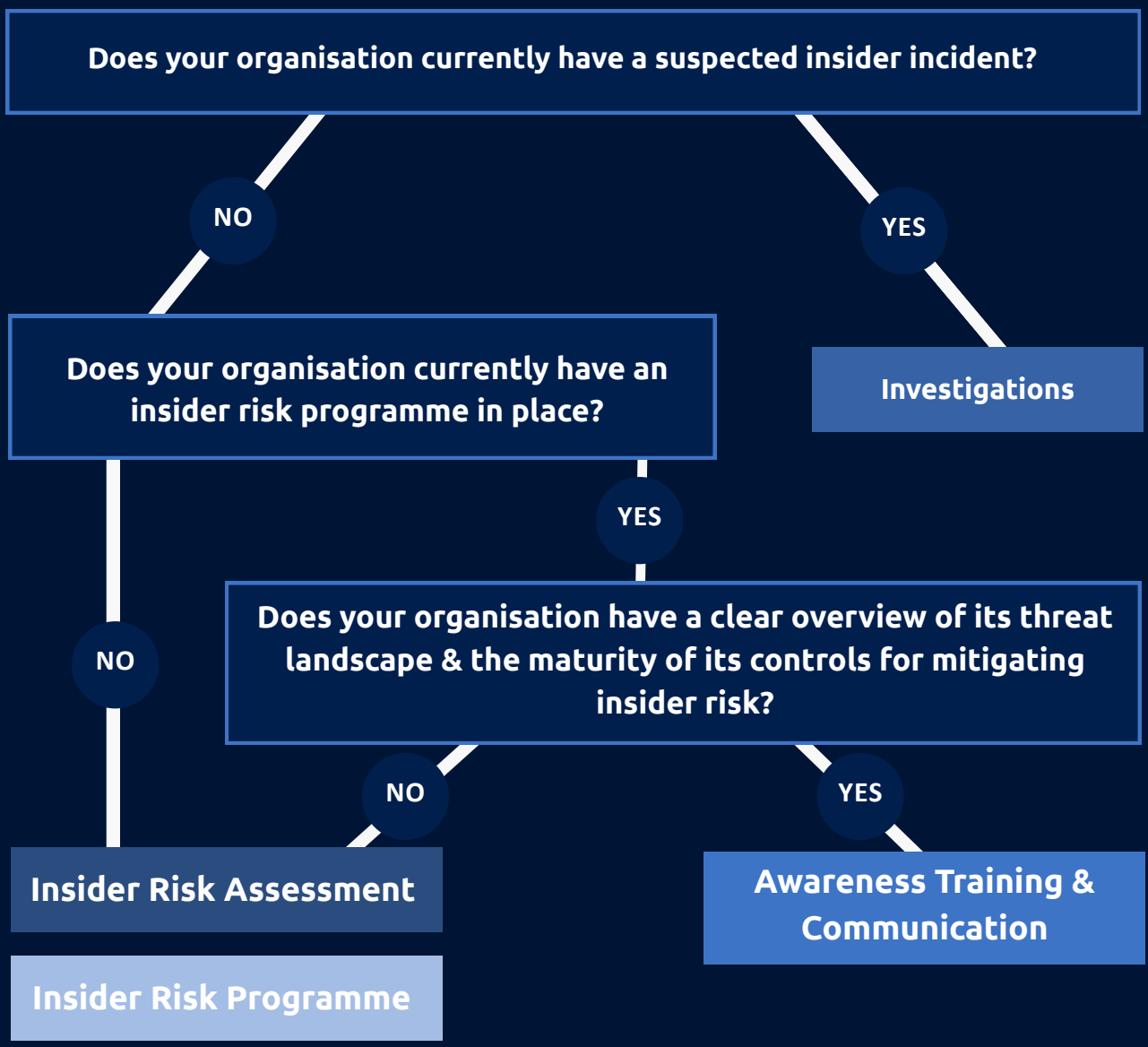
Another key challenge in insider risk management is the limited measurability of impact, as many organisations fail to define and track meaningful metrics. Without clear indicators to assess effectiveness, such as reductions in risk exposure, behavioural improvements, or response efficiency, insider risk initiatives remain difficult to evaluate and justify. This lack of measurement hinders informed decision-making, weakens accountability, and prevents organisations from demonstrating progress or value to senior leadership.

INVESTIGATION SKILLSET

Many organisations struggle with a limited availability of appropriate investigation skillsets to address insider incidents or suspicions. Insider cases require a different approach than traditional security or cyber incidents, combining behavioural analysis, legal awareness, and HR sensitivity. When these capabilities are lacking, organisations risk ineffective follow-up, inconsistent decision-making, or inappropriate escalation, ultimately weakening the credibility and effectiveness of insider risk management.

WITH YOU EVERY STEP OF YOUR JOURNEY

Our Signpost Six decision tree is designed to help organisations determine the next steps in their insider risk journey. The questions below will help you identify the best course of action for robust insider risk management. Each of the solutions presented in the decision tree will be outlined in more detail on the next page.



Info@signpostsix.com
www.signpostsix.com

INSIDER RISK SOLUTIONS

This section of the report highlights Signpost Six insider risk solutions and how they contribute to robust insider risk management.

Insider Risk Assessment

The Insider Risk Assessment evaluates organisational maturity to ensure key controls are in place to protect the organisation and its people from insider risk. It starts with translating the organisation's threat landscape into concrete insiders types and associated behaviours. The maturity of all relevant controls is then assessed based on our proprietary framework.

Any identified gaps are turned into actionable, prioritised recommendations with a clear roadmap. The maturity scores are also benchmarked against sector peers.

What you would get:

- Threat landscape & types of insiders
- Gaps & maturity analysis
- Industry benchmarking
- Mitigation roadmap

Insider Risk Programme

Signpost Six offers a holistic, structured Insider Risk Programme designed to enhance your organisation’s insider risk maturity. Following an initial assessment, we translate identified gaps into a clear, actionable roadmap, with countermeasures mapped to the domains of our Control Framework. Delivered in three phases: Foundation, Controls Implementation, and Consolidation, the programme strengthens governance, embeds proportionate safeguards, and ensures sustainable risk mitigation. Collaborating closely with your leadership and business partners, we reinforce resilience through tailored controls, policies, and awareness initiatives aligned with your organisation’s unique risk profile.

Info@signpostsix.com
www.signpostsix.com

Investigations

Signpost Six provides independent, and professional incident investigation services designed to restore control, create clarity, and and ensure an objective, traceable record of the investigation. We lead live investigations with integrity and confidentiality, working closely with your team so you remain in command while benefiting from our expertise. In addition to incident investigations, we offer Investigation Process Assessments and targeted trainings for corporate investigators. Examples of our training modules include:

- Investigations Planning & Governance
- Digital & Physical Evidence Handling
- Cognitive & Behavioural Interviewing
- Case Building & Reporting

Awareness, Training & Communication

Signpost Six delivers an end-to-end insider risk awareness solution that combines expert communication, practical trainings, and data-driven insights to strengthen security culture and reduce risks from within. Acting as a single partner for planning, delivery, analytics, and ongoing support, Signpost Six helps organisations turn awareness into measurable behavioural change. Our flexible and scalable approach provides organisations with a holistic understanding of insider risk, engages cross-organisational stakeholders, and builds practical skills, such as recognising insider risk signals and knowing when and how to act. Examples of our awareness and training offerings include:

- Online Insider Risk Management Training
- Interactive Insider Risk Workshop
- Serious Game for Case Management
- Measurable insider risk communications strategy
- Custom communications content development

TESTIMONIALS

WHAT OUR CLIENTS SAY

"Managing insider risk requires a delicate balance of empathy and vigilance. Signpost Six has become a true extension of our team, providing high-quality, actionable insights that allow us to stay ahead of potential risks. Their professionalism and specialized knowledge have made them an invaluable partner in our security strategy."

Head of Information Security, Robin Radar

robin
radar systems

"The Insider Risk Programme with Signpost Six led to a dramatic shift in the number of detected cases, and therefore increased visibility and the possibility to prevent and recover related losses"

Information Protection and Insider Risk Programme Head, Sanofi

sanofi

"The collaboration between Signpost Six and TU Eindhoven has created the foundation for a comprehensive and effective Knowledge Security Programme."

TU Eindhoven

TU/e

Sign post Six

Info@signpostsix.com
www.signpostsix.com

Signpost Six

ABOUT SIGNPOST SIX

.Signpost Six is Europe's leading insider risk management firm, helping public and private organisations detect, prevent and mitigate threats from within. Founded in The Hague, the firm brings together behavioural science and intelligence expertise to deliver comprehensive, people-centred security programmes.

CONTACT US

www.signpostsix.com

info@signpostsix.com

Talk to an expert