

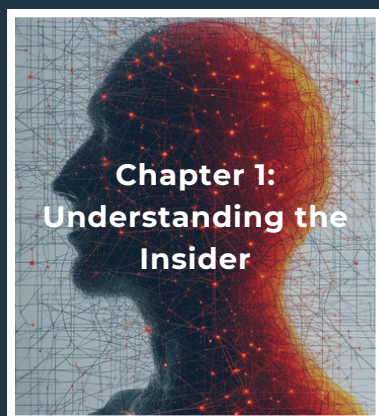
**INSIDER RISK
TREND
REPORT 2025.**

TABLE OF CONTENTS

	PAGE
• Introduction	
• Understanding the insider	
▪ Trend 1: Who is the insider?	3
▪ Trend 2: Financial stressors on the rise	4
▪ Trend 3: A shifting workforce	5
▪ Trend 4: Demand for insiders	5
• Organisational challenges	
▪ Trend 5: Organised crime	7
▪ Trend 6: The waterbed effect	8
▪ Trend 7: Managing third parties	9
▪ Trend 8 Critical Entities Resilience (CER)	9
▪ Trend 9: Augmented technological risks	10
▪ Trend 10: Physical identification	10
▪ Trend 11: Chatbot exploitation	10
▪ Trend 12: Insider trading	11
• Geopolitical challenges	
▪ Trend 13: Foreign sabotage operations	13
▪ Trend 14: Testing the waters	13
▪ Trend 15: Use of local citizens	14
▪ Trend 16: The false promise of screening	14
▪ Trend 17: Research under pressure	15
▪ Trend 18: Junior insiders	15
▪ Trend 19: Green targets	16
▪ Trend 20: The duality of protecting academia	16
• Have you thought about...?	
▪ CER-directive	18
▪ NIS2-directive	18
▪ Digital Operational Resilience Act	18

INTRODUCTION

The **Insider Risk Trend Report 2025** by **Signpost Six** delves into global trends on insider risk in a rapidly evolving and intricate risk landscape. Through our unique expertise, analysing our wide-ranging client portfolio and working closely with knowledge partners, we have identified **twenty key trends** that organisations should be aware of and incorporate into their security practices. We have organised these trends into three distinct chapters, each addressing a different layer of insider risk management: Understanding the Insider, Organisational Challenges and Geopolitical Challenges. To develop a comprehensive and up-to-date insider risk management programme, all of these levels should be carefully considered. Recognising that insider risk management can be overwhelming for many organisations, we have included key questions and relevant legislation to help you assess your organisation's security posture. This report is designed to support a structured evaluation and enhance your approach to insider risk management.



KEY FACTS

76%

of organisations experienced insider incidents in the past 12 months, up from 66% in 2019.

41%

of organisations have only partially implemented insider risk programmes.

29%

of organisations feel equipped to handle insider acts, leaving the majority vulnerable.*



Insider risk refers to the potential threat posed by any individuals within an organisation, such as employees or contractors, who have authorised access to sensitive information and systems and may misuse that access intentionally or unintentionally.

**based on a survey of 467 cybersecurity professionals by Cybersecurity Insiders and Securonix.*

Understanding The Insider.

- Trend 1: Who is the insider?
- Trend 2: A shifting workforce
- Trend 3: Financial stressors on the rise
- Trend 4: Demand for insiders

UNDERSTANDING THE INSIDER OVERVIEW

This chapter discusses the diverse motivations and circumstances that lead individuals to compromise their organisations. Understanding these psychological and situational drivers is essential, as a holistic approach to organisational culture is a key element of insider risk management. Diverse factors, such as financial pressure, disgruntlement, personal grievances, ideological beliefs, or even manipulation by external networks can impact the integrity of employees. Moreover, as organisations struggle with economic pressure and talent shortages, workforce instability has heightened risk factors, with departing employees and third-party contractors often posing unexpected vulnerabilities.

TREND 1: Who is the insider?

The insider risk landscape has become increasingly complex in recent years, with risks that range from unintentional actions - like accidental data leaks due to negligence - to calculated, malicious acts aimed at harming the organisation. Insiders can be current or former employees, contractors, and business partners who, by virtue of their authorised access, can compromise the confidentiality, integrity, or availability of an organisation's systems. While some insiders act out of personal motives like frustration, political beliefs, or financial gain, others may be coerced due to stressors or personal vulnerabilities. Besides, the rise of sophisticated technologies, including artificial intelligence, has blurred the lines between genuine insiders and external actors masquerading as insiders. Exploited chatbots and deepfake technology, for example, may impersonate employees, making it difficult to distinguish between genuine staff and malicious actors. This adds a layer of complexity to insider risk detection and highlights the importance of continuous vigilance for unusual behaviour.

TREND 2: Financial stressors on the rise.

Financial distress stands out as the most significant driver of insider risk, leading individuals to make desperate decisions and engage in malicious activities towards their organisations. With inflation climbing and housing prices rising - 74% of global housing markets saw increases in 2024 - more people are facing serious financial pressure. This vulnerability is heightened for those with lower incomes or substantial debt, who may seek financial gain from selling company data or disclosing other confidential information to external actors. Additionally, financially stressed individuals are more susceptible to coercion, potentially making them targets for manipulation by criminal networks.

Recognising stress indicators amongst colleagues, friends, and family can be key in preventing harmful actions. Coworkers and close contacts should be encouraged to report signs of distress, which may help guide individuals away from risky behaviour and toward supportive resources. This awareness, coupled with a strong organisational support system and a comprehensive insider risk program, is essential for safeguarding organisational security.

THE CRITICAL PATHWAY TO INSIDER RISK (CPIR)

The Critical Pathway to Insider Risk shows how a person might develop into a risk for your organisation. The pathway starts with personal predispositions, such as lacking social skills or a history of violence. These predispositions are concerning when combined with personal and organisational stressors like financial pressure or feeling treated unfairly by colleagues. Challenges like these can lead to unhealthy coping, with warning signs like hateful language or unusual sick leave. In these cases, it is essential that your organisation responds in an appropriate manner, without ignoring or inflating the situation at hand. By understanding the Critical Pathway, organisations can spot early warning signs, take steps to prevent risks, and create a more supportive workplace to stop issues from escalating. This shows that a human-central approach to insider risk is essential for mitigation.



TREND 3: A shifting workforce.

Post-pandemic, the job market has transformed drastically, favouring flexibility and redefining priorities. Frequent job changes have become the norm for many and secondary employment benefits, such as remote working policies and a good work-life balance, now play a critical role in job satisfaction. With nearly half of employees in 2024 considering a career shift, a new "Great Resignation" is looming. These developments, coupled with Europe's declining working-age population, create a dual challenge for organisations: filling positions in an increasingly fluid talent pool whilst maintaining robust screening processes - even under hiring pressure. To bridge gaps, companies are increasingly relying on freelancers, third parties, and artificial intelligence, underscoring the need for vigilant risk management across all workforce segments.

Whilst new hires and partnerships bring potential risks, the most significant vulnerability for many companies comes from departing employees. Disgruntled or disengaged workers may damage the organisation through unauthorised data disclosures, espionage, sabotage, or other insider acts. As employees exit, they carry critical institutional knowledge, making intentional or unintentional intellectual property violations and reputational damage a real concern. Strengthening offboarding protocols, implementing data access controls, and fostering a positive workplace culture are essential strategies to mitigate these insider risks.

TREND 4: Demand for insiders.

With companies continuously enhancing their cybersecurity and physical security, external actors are finding it increasingly challenging to breach defences directly. As a result, malicious actors are turning to a more effective strategy: recruiting insiders to gain access to confidential information or to conduct sabotage, fraud, and other harmful activities. Many clients report a marked rise in insider recruitment attempts, underscoring the need for internal security measures, including thorough background checks, behavioural monitoring, and secure access protocols, to safeguard against insider risk. However, whilst these hard controls are essential, creating insider risk awareness through training and communication is equally important. Organisations should aim to build resilience amongst employees, by making them aware of concerning behaviours and reporting mechanisms.



Would you recognise the early signs of recruitment by external actors amongst your employees?

Organisational Challenges.

- Trend 5: Organised crime
- Trend 6: The waterbed effect
- Trend 7: Managing third parties
- Trend 8: Critical Entities Resilience (CER)
- Trend 9: Augmented technological risks
- Trend 10: Physical identification
- Trend 11: Chatbot exploitation
- Trend 12: Insider trading

ORGANISATIONAL CHALLENGES

OVERVIEW

This chapter explores the most pressing organisational challenges related to insider risk today. As companies face a sophisticated array of risks, implementing all-encompassing security controls has become exceptionally demanding. Organisations need to consider the possibility of legitimate business creation and infiltration as covers for illegal operations, whilst upholding supply-chain efficiency and maintaining a competitive market position. Correspondingly, insider risks no longer stem predominantly from direct employees; they now encompass a vast network of third-party vendors, contractors, and even AI-driven systems, all of which can be exploited by malicious actors. This chapter ties into these different vulnerabilities, offering insights into organised crime tactics, third-party risk, and augmented technologies.

TREND 5: Organised crime.

From logistics to finance, pharmaceuticals, tech, law, and even agriculture, criminal organisations rely on insider access to exploit and manipulate these sectors for their own gain. As demand for illicit goods and services surges - whether for narcotics, counterfeit products, or financial schemes - criminal networks strategically embed individuals within companies or coerce existing employees to aid their operations. This multifaceted infiltration spans supply chain monitoring, sensitive data extraction, operational disruptions, and the insertion and extraction of illicit goods, making undermining one of the most critical challenges for logistical industries today. Understanding and mitigating this pervasive risk requires a holistic view of how organised crime intersects with everyday business functions, blurring lines between legitimate operations and illicit intent.

Much like consumer expectations for package tracking, criminal organisations desire precise knowledge of their product's location and timing, making insider infiltration essential to the operation. This type of insider wants the legitimate business it exploits to run smoothly, so they can run their criminal operations long-term. Without adequate prevention and early detection controls, the impact of organised crime can be substantial, leading to financial, operational, and reputational damage. This need for tight control underscores how illegal networks manipulate legitimate trade systems, making use of weaknesses in security and leveraging key personnel at multiple stages to ensure smooth and secure transport of their illegal products.

TREND 6: The waterbed effect.

Over the past years, many shipments of contraband have been intercepted by customs in Europe and elsewhere, leading to an increase in awareness and physical security measures. However, when security measures tighten in one area, criminal activity often spikes elsewhere - known as the waterbed effect. In the context of insider risk, increased physical security checks or border controls push external actors to recruit more insiders within companies to bypass these defences. As external options become limited, insiders become a critical asset, allowing attackers to maintain access, control, and valuable information across operations despite heightened security barriers in other areas. This dynamic underscores the need for a balanced approach to both external and insider-focused security strategies.

CASE HIGHLIGHT: "THE MISSING CHURCHILL"

Organised crime does not only target logistical industries for the smuggling of counterfeit goods. Museums, galleries, and even hotels can fall victim to the practice of illegal art trafficking, where famous artworks get stolen and occasionally replaced with replicas. In 2024, the famous 'Roaring Lion' portrait of Churchill was finally returned to the Fairmont Château Laurier hotel in Ottawa, Canada. After a thorough investigation by the OSCE's Heritage Crime Task Force it was discovered that the missing portrait was indeed replaced by a fake one, whilst the real one was auctioned through Sotheby's. The magnitude of this case, involving a unique network of law enforcement, illustrates the complexity of organised crime and the sophisticated tactics that are used in illicit art trafficking.



Have you identified the vulnerabilities to organised crime within your organisation?

TREND 7: Managing third parties.

Current organisational developments reveal a concerning disparity: whilst third-party workers are often treated socially and operationally like internal employees - with similar access privileges and integration within teams - they undergo far fewer screenings and security checks. This gap creates vulnerabilities, as organisations grant third-party vendors, such as software providers, elevated access without extensive due diligence. Many of our clients express increasing concern over the lack of visibility into these third-party entities and their potential impact on security, particularly as companies may depend on the expertise of external organisations when specific technical or logistical problems arise.

TREND 8: Critical Entities Resilience (CER).

The extensive implementation of the Critical Entities Resilience (CER) directive in Europe, which will be explained in detail in the final chapter, will place greater emphasis on third parties. This legislation will require critical entities - such as energy providers, hospitals, government bodies, financial institutions, and food suppliers - to prevent, detect, control, and report incidents to safeguard European society against critical infrastructure collapse. The directive concentrates on a large range of risks, including natural disasters, terrorist attacks, and insider risk. As these critical entities will strengthen their security practices, following the CER directive, their third parties may become an appealing point of entry for criminal networks, offering easier access to sensitive information and systems. This shift highlights the need for robust third party risk management to ensure that all connected entities, both internal and external, meet stringent security standards.

THIRD-, FOURTH- AND FIFTH PARTIES

It is a common misconception that third-party risk management pertains solely to the external organisations directly associated with your business.

Comprehensive due diligence and security requirements should encompass the entire supply chain, including relevant external parties with whom your third parties engage.



Do you have solid due diligence, screening, and monitoring procedures in place for the third-parties that your organisation depends on?

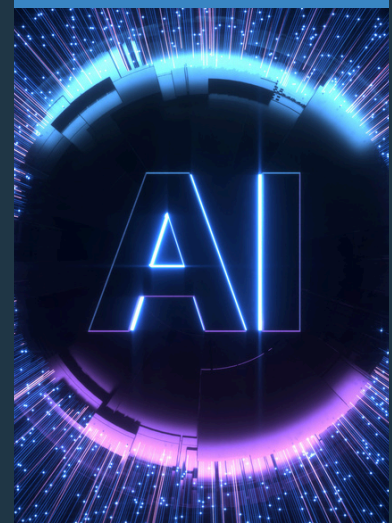
TREND 9: Augmented technological risks.

Augmented technological risks refer to vulnerabilities introduced by advanced technologies, such as AI, automation, and remote access systems. These technologies amplify insider risk, as they can grant employees broader access to sensitive data and systems. This can lead to potential misuse, whether intentional or accidental. Intentional insiders may exploit chatbots to extract personal data or create algorithms that facilitate insider trading. Moreover, malicious actors may coerce or manipulate employees into providing access to these technologies for unauthorised actions. Mitigating such risks requires organisations to adopt comprehensive security frameworks, monitoring, and employee awareness programmes that address both human and technological vulnerabilities.

TREND 10: Physical identification.

In large organisations with extensive facilities, security cameras and their surveillance footage serve as vital control mechanisms. However, these tools are increasingly susceptible to manipulation, raising serious concerns about their reliability. Techniques such as image alteration can erase individuals from footage, whilst advanced deepfake technology allows the insertion of fabricated personas, making visual verification less trustworthy. Moreover, the rise in CEO fraud - where perpetrators impersonate executives to request fund transfers via email or messaging apps - has become alarmingly prevalent, particularly within financial departments. As a result, traditional methods of authentication, such as video calls, message approvals, and even passport checks, are proving inadequate in the face of evolving risks. Given this risk landscape, we anticipate a significant return to interpersonal checks, emphasising the importance of physical identification processes.

Chatbots, designed to enhance customer service, are extremely vulnerable when not properly secured.



TREND 11: Chatbot exploitation.

The exploitation of AI chatbots represents a serious threat to data security, as malicious entities can manipulate these systems to access sensitive information. Since chatbots are designed to serve as digital employees, one might even argue that they can become insiders themselves.

This situation raises important questions about accountability: who bears responsibility when internal or external actors exploit these systems to harm the organisation? Is it the software service provider, the chatbot itself, the supervisor overseeing its use, or an internal or external malicious actor? Chatbots, designed to enhance customer service and streamline operations, are extremely vulnerable when not properly secured. An insider or outsider with knowledge of the system can exploit its functionality to elicit confidential data. Even when the chatbot is hosted internally, having access to it might also give access to sensitive company data that the chatbot is trained on, providing confidential information to individuals in your company. As organisations increasingly integrate AI chatbots into their operations, robust oversight and stringent access controls are essential to mitigate these risks and protect sensitive information.

TREND 12: Insider trading.

The rise of AI-driven trading systems has the potential to increase global market efficiency. However, its widespread implementation also causes great ethical and security concerns, particularly when insiders leverage non-public information to program bots for strategic trades. This convergence of technology and finance poses challenges for regulators, who must now navigate the complexities of algorithmic trading, ensuring that the integrity of the market is maintained while preventing abuses that could arise from exploiting insider knowledge. As artificial intelligence continues to evolve, the lines between legitimate trading strategies and insider trading will increasingly blur, prompting urgent discussions on regulatory frameworks and ethical standards in the financial landscape.

CASE HIGHLIGHT: "GOOGLE'S GEMINI AI MANIPULATED TO LEAK USER PASSWORDS"

In March 2024, cybersecurity researchers from journal HiddenLayer exposed a critical vulnerability in Google's Gemini AI. The chatbot could be manipulated to disclose personal data, such as passwords, when prompted in a specific indirect manner. This flaw raised serious concerns, given Google AI's strong reputation for safeguarding user data. The incident underscores the importance of testing and refining AI models to prevent exploitation through indirect or unexpected prompt methods. If your organisation uses a chatbot, it is critical that the chatbot meets the highest security standards, whilst maintaining its functionality and reliability.



Do you have an overview of the tools that your employees use and what happens to the company data that is inserted into them?

Geopolitical Challenges.

- Trend 13: Foreign sabotage operations
- Trend 14: Testing the waters
- Trend 15: Use of local citizens
- Trend 16: The false promise of screening
- Trend 17: Research under pressure
- Trend 18: Junior insiders
- Trend 19: Green targets
- Trend 20: The duality of protecting academia

GEOPOLITICAL CHALLENGES OVERVIEW

This chapter explores how growing geopolitical tensions are defining the insider risk landscape for businesses and academia. It will focus on how nation-state actors, particularly from Russia and China, are testing infrastructure vulnerabilities to increase their sphere of influence on Western societies. Moreover, this chapter explains the continuous battle for academic institutions to balance openness with securing vital research.

TREND 13: Foreign sabotage operations.

Foreign sabotage operations present a significant risk to organisations and can be executed by foreign nationals or proxies acting on their behalf. Such operations may involve insiders who either knowingly or unknowingly support the hostile agenda of the nation-state in question. Objectives can include a disruption of specific operations, damage to infrastructure, or economic sabotage. Tactics used for sabotage are diverse and range from physical damage to cyberattacks, depending on the actors' capabilities and targeted information or systems. As geopolitical tensions rise, insiders become more and more attractive to hostile nation-state actors, making it essential for organisations to implement stringent security measures.

TREND 14: Testing the waters.

It will have escaped no one's attention that Russian and Chinese adversary groups have set their sights on destabilising European infrastructure. Through a series of ongoing, small- and medium-scale acts of sabotage, they are testing the limits of their abilities to disrupt Western society and assessing the potential reach of their influence, should they choose to escalate current conflicts. Many organisations encounter these forms of micro sabotage but often fail to recognise the potential future impact of these insider acts. Foreign adversaries use probing tactics to identify vulnerabilities, laying the groundwork for more substantial, damaging attacks in the future. It is therefore crucial to treat incidents of sabotage with the attention they deserve and to build security policies on past incidents - no matter how innocent or insignificant these incidents might seem at glance.

TREND 15: Use of local citizens.

Western organisations often fall into the misconception that nation-state sabotage operations are primarily carried out by foreign nationals or obvious insiders with ties to hostile foreign entities. Their screening procedures tend to focus heavily on identifying high-risk nationalities or personal connections to suspicious foreign groups or organisations. However, this narrow focus can lead to significant blind spots, overlooking the sophisticated strategies of foreign actors to recruit and manipulate local citizens who lack apparent foreign affiliations. This strategic integration of malicious groups not only broadens the reach of foreign interference but also complicates the detection of insiders.

TREND 16: The false promise of screening.

Tying into the previous observation, screening procedures are not the be-all and end-all for insider risk prevention. Screening is a must-have safeguard for each organisation but does not guarantee the loyalty and integrity of workers during their employment. As you can see in the Critical Pathway to Insider Risk, individuals may take a wrong turn because of personal predispositions combined with personal or organisational stressors. Any employee, under the wrong circumstances, is capable of committing an insider act. Security measures should thus reach far beyond initial screening and include behavioural monitoring of employees to an appropriate degree for the organisation in question, compliant with GDPR.

Sphere of influence

Employees are often unaware of their sphere of influence within their organisation. Operational staff, for example, may overlook the risks of actions as simple as opening the door for an unfamiliar face or sharing sensitive information with colleagues with different levels of authorisation. Raising employee awareness is therefore essential to preventing sabotage. Management, in turn, may fail to identify the extent of influence held by operational employees as well. Cleaning staff, for instance, might have similar access rights to logistical personnel, yet lack the necessary security clearance.



Does your organisation log and follow up on each security incident, no matter how minor the damage?

TREND 17: Research under pressure.

Research security is essential for protecting valuable data, intellectual property, and the safety of individuals in both academic and corporate environments. The current increase in protectionist economic measures in the United States and Europe are heightening competition, spiking an increase in espionage and sabotage incidents. At academic institutions, students, teachers, or researchers who have legitimate access to valuable research or hold significant influence, may be strategically used for espionage or propaganda. These insiders may be motivated by state interests or personal factors, such as student loan debts. Similarly, insider acts compromising corporate R&D security can lead to the unauthorised transfer of proprietary information or sensitive technologies, with potentially serious implications for the economic position of an organisation or nation-state.

“At the Technical University Eindhoven, we are used to handling knowledge with care, as we frequently conduct research with companies where safeguarding Intellectual Property is of critical importance. It is now key to broaden this approach to also consider sensitive information in relation to state actors.”

Research Security Professional
@TU/e



TREND 18: Junior insiders.

In the realm of economic espionage and corporate research security, we are observing significant shifts in the types of employees and organisations targeted by state-sponsored actors. Nation-state actors are increasingly targeting junior staff, including interns and new hires, to exploit their access to sensitive projects. These employees are often overlooked in security screenings or monitoring processes due to their assumed limited access. Junior employees, often less aware of security policies and eager to establish their careers, can be unwittingly drawn into information-sharing that ultimately benefits foreign adversaries. Organisations should therefore carefully consider screening procedures across all seniority levels.

TREND 19: Green targets.

On an organisational level, we see that emerging green R&D industries are attractive targets for economic espionage. As governments focus more on green technology, renewable resources, and food security, nation-states have intensified espionage efforts in sectors such as battery technology, sustainable agriculture, and energy-efficient materials. R&D units working on environmentally focused technologies may have less robust security as they are less traditionally associated with espionage, making them surprising but lucrative targets. Moreover, start-ups in sustainable and sensitive technologies might experience rapid organisational growth, focusing on acquiring a competitive market advantage rather than implementing security protocols. Venture capital firms and international alliances, such as NATO, have the task of supporting entrepreneurs in this process of protecting their organisations from insider risk.

TREND 20: The duality of protecting academia.

Research security presents a complex challenge for academic institutions striving to balance the principles of academic freedom and openness with the need to protect vital knowledge from malign foreign influence. Where research and development departments within companies apply the strictest security measures to protect their innovations, universities are designed to be transparent and aim towards sharing knowledge as widely as possible. However, in the current geopolitical environment, where critical innovations and knowledge are a direct target for nation-state sponsored espionage and sabotage, academic institutions must revise their policies. Students and staff find themselves increasingly pressured by state actors, threatening the social safety and integrity of university environments. Insider risk impacts not only technical university studies, but also other research fields, such as language and culture programmes.

STRATEGIC INFILTRATION

The research security landscape extends beyond espionage and sabotage; academic institutions also face risks from the strategic infiltration of individuals into board-level, teaching, or research positions. Through these roles, infiltrators may aim to influence academic discourse by promoting specific ideologies or propaganda, subtly impacting the perspectives of professors, researchers, and students. This form of manipulation threatens the objectivity and integrity of academia, potentially reshaping the educational environment to serve the interests of foreign or ideological actors.



Does your organisation actively manage and monitor access to valuable information?

HAVE YOU THOUGHT ABOUT...?

As a result of the organisational and geopolitical developments that we discussed in this report, European legislative bodies are tightening their controls on infrastructure, innovation, and national security. Essential, important and financial entities are now required to adhere to strict security directives aimed at safeguarding both their organisations and European society.

Meanwhile, in the United Kingdom, the limits of intelligence-gathering capabilities are actively expanded. The UK's Investigatory Powers Act grants authorities extensive surveillance capabilities, allowing for the mass collection of British citizens' communications data, including social media posts, facial images, and internet connection records. Whilst intended to bolster national security, critics argue that this level of surveillance is overly intrusive and lacks sufficient oversight. Similarly, on an organisational level, many companies are ramping up internal monitoring using tools. Although, to remain compliant with GDPR, these measures require bespoke solutions rather than a one-size-fits-all approach. Conducting a Data Protection Impact Assessment (DPIA) is essential for GDPR compliance, as it ensures that monitoring practices respect privacy standards.

Navigating regulatory compliance can be complex, but is essential, as both insufficient safeguards and excessive monitoring can lead to substantial fines for non-compliance. The next page outlines three key pieces of legislation that your organisation should be aware of regarding insider risk.

CASE HIGHLIGHT: "ENORMOUS FINES FOR NON-COMPLIANCE"

In October 2024, TD Bank was fined \$3 billion dollars due to inadequate anti-money laundering controls in the United States, including weaknesses related to unauthorised account access and fraudulent activities. The penalty also resulted in an asset cap, which limited the bank's ability to grow in the U.S. market, significantly impacting its expansion plans. TD Bank was then faced with increased regulatory scrutiny of its operations, forcing the bank to allocate substantial resources to compliance reforms, whilst also addressing reputational challenges. This case illustrates the critical financial and reputational impact that non-compliance can have on your organisation.

Critical Entities Resilience Directive (CER)

The Critical Entities Resilience (CER) Directive focuses on enhancing the resilience of critical infrastructure against a broad range of threats, including natural hazards, terrorist attacks, and insider risk. Disruptions caused by malicious insiders or negligent employees can threaten essential services like energy, healthcare, and transportation. Critical entities must therefore proactively identify vulnerabilities through insider risk assessments and develop an insider risk management programme, that includes employee vetting for sensitive roles, comprehensive security awareness trainings, access management, and other important countermeasures. By combining physical and cybersecurity measures with organisational security policies, businesses can address insider risks and ensure compliance under CER. The directive was introduced in 2022 and is now transposed to national legislation for member states.

Network and Information Security (NIS) 2 Directive

The Network and Information Security (NIS) 2 Directive aims to strengthen cybersecurity for essential and important entities. Insiders, whether negligent or malicious, pose a significant cybersecurity risk as they can compromise networks, leak sensitive data, or enable cyberattacks. Companies must therefore integrate insider risk into their cybersecurity risk management frameworks, implementing access controls, activity monitoring, and incident detection systems. To comply, organisations must train employees on cybersecurity best practices to reduce errors and negligence whilst promoting vigilance. The directive was introduced in 2023 and is currently transposed to national legislation,

Digital Operations Resilience Act

The enforcement of the Digital Operations Resilience Act (DORA) started on January 17, 2025 and places operational resilience at the forefront for financial institutions, where insider risks pose a serious threat to stability. Insiders with access to critical systems or sensitive data can disrupt operations and services, whether intentionally or through negligence. Whilst external cyber threats often dominate focus, insider risks are just as important to identify and address. A maturity analysis, targeted countermeasures, incident management and regular resilience testing through scenario-based assessments help identify and tackle weaknesses in systems and overall security culture. Financial institutions must also extend security requirements to third-party providers, ensuring insider risks are mitigated across the entire digital ecosystem.



Sign post SIX



www.signpostsix.com



info@signpostsix.com



+31 (0)70 2211 940

**LEADING IN
INSIDER
RISK**