Deloitte.
Together makes progress

KLME

Forensic insights on managing evolving Insider risks, threats & events

100 مئة عام
Years in the Middle East

Executive summary

In an era marked by digital transformation, Deloitte Forensic & Financial Crime recognizes the need to address the rising complexities of Insider threats in organizations. As companies increasingly rely on digital systems, Insiders—those with legitimate access to critical information—pose significant risks. This paper aims to equip C-suite and senior executives with the insights needed to manage these threats through innovative, behavior-centric strategies, moving beyond traditional approaches.

Organizations must adapt to the rapidly evolving geopolitical and technological landscape by enhancing their governance and compliance frameworks. Our analysis reveals the necessity of redefining Insider threat management to reflect the broader reality across regions and industries. Understanding Insider threats from both a data and human perspective fosters a corporate mindset shift towards analyzing individual behaviors, paving the way for robust Insider programs.

Globally, it's essential for organizations to learn from diverse regulatory frameworks, expanding their approach beyond regional insights. For example, frameworks from entities like the UK's National Protective Security Authority (NPSA) provide comprehensive definitions that cater to a wide range of sectors and industries. Effective Insider programs now demand multi-disciplinary oversight, empowered behavioral reporting, and strategic management of third-party relationships.

The influence of Generative AI further complicates Insider risk management. AI agents introduce novel challenges, prompting organizations to refine their strategies. The gap in AI-specific insurance products emphasizes the need for coverage related to regulatory compliance, extortion, liability, and business interruptions. Comprehensive compliance programs are becoming indispensable for navigating complex, multi-jurisdictional regulatory landscapes, ensuring thorough management of Insider threats.

Exploring Insider definitions

Understanding the Insider

What is "an Insider"? Broadly, an Insider an individual [within an organization] who has legitimate and authorized access to an organization's systems, networks, and data; someone who is privy to information that a third-party would not, and should not, have access to.

Most Insider definitions contain a certain degree of assumptions having by consequence an impact when it later comes to Insider threat management:

Employment: An Insider may be someone employed by, or contracted to provide services to the organization, and operates within the remit or confines of the organization's structure and policies

Access: An Insider was provided legitimate and authorized access to the organization's systems and uses or leverages this access for unauthorized purposes

Data: An Insider thereafter, or in parallel seeks to exploit weaknesses in the organization's infrastructure, systems, controls and networks to obtain data and send it outside of the organization's authorized framework.

Seniority: An Insider is usually an individual in a senior or experienced role with access to sensitive and confidential information and/or the ability to override controls that can cause serious damage to the organization

Expertise: An Insider is often a technically capable individual or subject matter expert in their given field or industry

Intent: An Insider may not necessarily be malicious in their intentions towards the organization and be set on causing it harm, but may also be negligent, or motivated by personal enrichment or another driver

Insiders have always been difficult to identify. The fluid, and sometimes uncertain nature of trust and control that organizations place on their employees and third-party contributors' changes on an almost daily basis. Most matrix organizations must grapple balancing employment rights with organizational efficiency, to grant employees' access to systems, networks and data required or deemed necessary for their core responsibilities.

Most information security frameworks require organizations to treat all requests for access as having originated from an untrustworthy source. Highly regulated industries such as financial services, telecommunications and energy service providers require a more rigid approach whilst fast-moving industries such as e-commerce require a flexible approach to considering requests for access but still require strong guardrails around systems and data lakes that process personally identifiable information (PII) at rest or in transit.

A real challenge with Insider threat management is adopting the right and most effective approach for the organization. Focusing on governance from a macro perspective or implementing broad system and data controls is symptomatic at best. Policies, procedures, and processes are preventive backboards against which employees are meant to function and if well-defined, can serve as potential enforcement mechanisms against Insiders. However, in our experience across numerous corporate misconduct, fraud and Insider event investigations, we find organizations grappling with the human factor, arguably the most difficult aspect to manage.

Regional Insider definitions

Insider definitions in the region have been mostly contained in corporate governance codes and industry frameworks developed by the various regulators. In practice, regional regulatory frameworks often lack harmonization at the federal or national level. There are numerous industry-specific controls that organizations must comply with during regular audits, due diligence exercises, and site inspections by regulatory authorities.

Within this paper, we highlight securities and capital market authorities across the Middle East. This is by no means a complete and comprehensive list; and legal regulatory advice should be sought to tailor this information to acquirers or companies that operate within or expand into the Middle East. Some examples are detailed below:

Regional Insider definitions vary widely, and organizations must navigate multiple, industry-specific regulatory requirements

UAE

In Section 94 of the ADGM Legal Framework, FSRA Legislation, Part 8 Market Abuse, Section 94, The DFSA Markets Rules in MKT 4.2.7 (MKT 6.5.7 for Listed Funds) and the DSFA's Markets Law 2012 (Part. 6, s. 64 - 'Defences for market manipulation, insider dealing and providing inside information') all cover aspects of insiders.

Reporting Entities establish and maintain adequate systems and controls to enable it to identify at all times any Person working for it under a contract of employment or otherwise, who has or may reasonably be likely to have access to Inside Information relating to the Reporting Entity or, where applicable, the Listed Fund, whether on a regular or occasional basis.

KSA

Saudi Arabia's Central Bank (SAMA) mandates frameworks and regulations that address insider threats within financial institutions under SAMA's Cybersecurity Framework (CSF). These mandates aim to protect sensitive information and digital services from various threats, including those posed by negligent or malicious insiders. SAMA also emphasizes the importance of threat intelligence sharing and digital forensic incident response (DFIR) capabilities.

To counter fraud related to insider events, SAMA has implemented a Counter-Fraud Framework (CFF) to combat financial fraud within the Kingdom's financial sector.

Qatar

Qatar's approach to insider threats is embedded within its broader National Cyber Security Strategy and frameworks like the Qatar Cyber Security Framework (QCF) and the Qatar National Information Assurance (NIA). These frameworks emphasize prevention, detection, and response to security incidents, including those originating from within an organization. Key aspects include data protection, privacy, and the implementation of security controls to mitigate risks to critical assets. The Qatar National Cyber Security Agency (NCSA)'s primary mission is to protect Qatar's digital infrastructure and information systems from threats. The NCSA actively collaborates with organizations like CREST to develop accreditation programs.

Bahrain

The Bahrain Insider Framework refers to regulations and best practices designed to prevent insider trading and market abuse within Bahrain's financial markets. It encompasses rules about insider trading, market manipulation, and the misuse of confidential information. The Central Bank of Bahrain (CBB) plays a key role in establishing and enforcing this framework.

Article 57 of the CBB Rulebook, defines insider trading and prohibits the purchase or sale of securities based on undisclosed material information. This includes both direct trading by insiders and the act of "tipping," where insiders reveal confidential information to others who then trade.

Oman

Oman's approach to mitigate insider threats, is based on a combination of legal frameworks, regulatory guidelines, and organizational practices. Key elements include the Cybersecurity Law, the Information Security Framework, Data Protection Law and Central Bank of Oman (CBO) regulations. Organizations, particularly in critical infrastructure sectors are expected to develop and implement their own policies and procedures for insider threat management.

Broadening the Insider definition

Looking outside of the region, in March 2023, as part of an Integrated Review Refresh[1] by the government of the United Kingdom (UK), the National Protective Security Authority (NPSA)[2] absorbed the responsibilities of the Centre for the Protection of National Infrastructure (CPNI)[3] to cover a broader remit and reach beyond critical information infrastructure (CII).

This was recognition by the government that threats across all sectors had evolved beyond infrastructure and systems, and to effectively manage the threat landscape a shift in viewpoint was needed.

Prior to May 2023, the NPSA defined an Insider as 'a person who exploits, or has the intention to exploit, their legitimate access to an organization's assets for unauthorized purposes'.

This definition placed emphasis on actors and failed to separate the risks from the threat. It was also narrow in its focus on legitimate access and presupposed the use of assets for unauthorized purposes. An updated definition was developed to communicate 'a consistent lexicon' and sought to clarify the separation between Insiders, the risks, and the threats that would eventually be the cause of an Insider event. The language was designed to be forward-compatible in an evolving threat environment and recognized unintentional instances.

NPSA's key message in the definition is that 'If you have people, you have risk'.

Managing today's threat landscape requires looking beyond assets to the human element

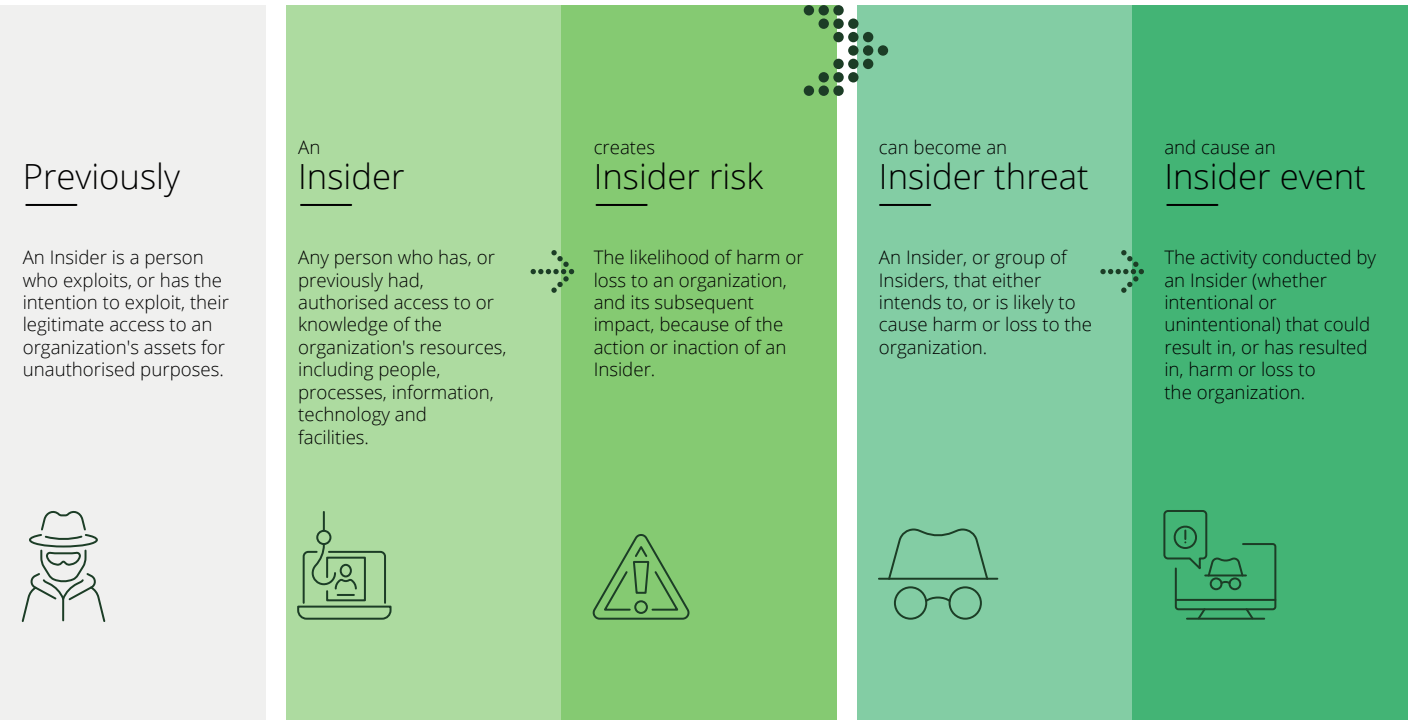

Figure 1: The 'new' Insider[4]

Building an Insider program

Mapping the Insider

While most organizations take a systems or data-based approach, a people-centric thought process around Insider programs, aligned with fraud risk frameworks tends to be more effective.

This starts with a thorough understanding of the business, employees, clients and customers, subcontractors, vendors and stakeholders of the organization. Any individual who interacts with the organization and has access to or knowledge of the organization's resources is potentially an Insider and essentially poses a degree of risk.

It takes a concerted effort between departments such as HR, IT, Compliance, Legal, Operations, etc, to clearly map out the roles and responsibilities of individuals, understanding the type of data (both generated and handled) within each department pertaining to business lines and or the internal organization and its strategy and the corresponding classification for each data set.

Building trust in Insider programs

A crucial goal of an Insider program should be to build trust and offer support to employees, not just to identify and act on every instance of an individual toeing the line or going off-script. This means being alert to changes in colleagues' behaviours, such as declining attendance, requests for access beyond the job scope, expressing dissatisfaction towards the organization, etc. and knowing how to communicate and address these.

Remote and hybrid working arrangements does make this harder because interactions follow different patterns and opportunities for taking note of behavioural deviations may be often limited. It's important to be cognizant of both modern workforce trends and organizational security challenges effectively.

To do so, there's been a shift towards using technology and data to monitor employee behaviour. While this provides valuable insights, it's important to remember that Insider threats are about people, and people are complex and unpredictable. Technology alone can't always identify when an employee poses an undue security risk or a clear threat. Deloitte's view is that it is crucial to keep people at the centre of Insider threat programs while balancing innovative technologies and data-driven approaches.

Preliminary risk assessment & risk-based onboarding: Understand the organization's risk tolerance and enterprise risk management framework to tailor the Insider program, aligning with available in-house forensic resources and legal teams and external counsel to build a comprehensive, impactful Insider threat management framework.

Multi-disciplinary oversight: Enable information sharing processes across functions to build a collective understanding of objectives. Fusion teams are particularly successful in this regard, combining the technological know-how of the organization with business-led subject matter expertise to help identify risks.

Empower behavioral reporting: Implement appropriate reporting mechanisms for employees to express their concerns, raise grievances and prompt internal investigations. In numerous industry reports, it is found that anywhere from 40-50% of fraud and misconduct within an organization is caught via whistleblowing channels, more so if anonymous reporting is allowed.

Third-party vendor management: With the broader Insider definition, identifying, assessing, mitigating, and monitoring risks associated with engaging with external vendors and service providers becomes even more crucial. Ensuring that the Insider program and frameworks include third-party relationships, where external providers inadvertently gain Insider knowledge, ensures an alignment with business objectives, compliance with regulations, and helps to prevent exposure to undue risk. Organizations need to understand that vendor relationships are not static.

The proliferation of AI and Insider risks

Future of work
AI took a major leap with the general availability of ChatGPT and generative AI platforms in 2023. We refer to AI to include generative AI, predictive AI (predictive analytics) and machine learning. Generative AI and its ability to disrupt the way we work because of its ability to augment human expertise and to automate tasks which are both complex and non-revenue generating.

It would be prudent for leaders to be prepared for boardroom conversations concerning the safety of AI, responsible AI practices, and how to mitigate risks that AI will exacerbate Insider threat risks.

Using GenAI in a corporate environment
Uncontrolled and unmonitored use of AI within the workplace arise because of a misaligned assumption that inbuilt guardrails will cause an AI to regulate itself. Thought experiments such as the 'paperclip maximizer' demonstrate that the risks of an AI 'going rogue' can become very real.

There are numerous published transparency notes and studies about the risks of using AI. More recent studies have highlighted agentic misalignment, where autonomous AI agents engage in activity that would be considered Insider threat. As organizations adopt agentic AI and integrate these across the enterprise, the models are assisting and being trained on emails, personally identifiable information (PII), sensitive commercial documents, etc.

These AI agents are authorized access to sensitive systems, and more importantly, make decisions. Most organizations treat these AI agents as a static part of the infrastructure.

These agents really operate as active users. This creates a blind spot in Insider risk management that arise if humans are not given sufficient time or resources to evaluate agentic AI [active users/ employees] prior to deployment.

Using GenAI in a corporate environment
Regulators are starting to enforce stricter controls within sectors for whom AI presents systemic risks. The applicability of the European Union's Digital Operational and Resilience Act (DORA) enacted Jan 2025 was meant to cover financial entities and their suppliers. However, DORA also sets a bar for cybersecurity preparedness for all companies with proximity to the EU.[5]

A practical example of how DORA's oversight regime can extend to cover non-financial sector enterprises and suppliers is the realms of social engineering. During 2025, the retail price of desktop supercomputers featuring GPUs capable of delivering one petaFLOP of AI performance fell to below US$3,000. These devices have made it substantially easier for threat actors to run LLMs rivalling frontier model performance standards outside the constraints of a datacenter. As a result, threat actors can enhance, deploy and very sophisticated deepfakes, voice manipulation, realistic fake identities and sophisticated phishing email campaigns.

As organizations integrate agentic AI across the enterprise, they are authorizing systems that access sensitive data — and make decisions

Covering AI-specific Insider events

While implementing internal controls to mitigate the risks of Insider threats, organizations will seek to insure themselves against the associated risks. While current insurance products generally provide the appropriate coverage for Insider events, there are significant gaps for AI-specific Insider events and cross-jurisdictional regulatory exposures. Most insurers have yet to conclusively redefine coverage parameters to address AI-specific risks, and the wide variety of losses which can occur due to AI systems.

A key component is around the determination of liability between AI systems developers (the model itself) and the organizations that deploy them (the use of model). In a fast-evolving landscape, policies will soon have to adapt to cover costs associated for complying with AI regulations. Underwriting such policies will generally need to include AI-specific risk assessments and reporting requirements.

Key areas for organizations to look out for when considering coverage for Insider events include:

Current insurance covers most Insider events, but gaps remain for AI-specific risks and cross-jurisdictional exposures

1. **Regulatory coverage** to provide protection for legal defence costs associated with regulatory investigations and coverage for regulatory fines and penalties where legally insurable. This coverage is increasingly important under stricter regulatory landscapes, particularly in jurisdictions with significant penalty regimes.

2. **Extortion coverage** to address ransom demands and malicious threats, providing coverage for costs related to restoring affected systems. This coverage is relevant for insider threat scenarios involving data theft or system manipulation for extortion purposes.

3. **Liability coverage** addressing third-party claims and associated defence costs arising from data breaches. This coverage is particularly relevant for M&A scenarios where acquired company breaches may affect the acquiring organization's liability exposure.

4. **Business interruption coverage** addresses income loss resulting from IT system downtime and aids in restoring data, networks, and IT systems. This coverage is critical for integration scenarios where system disruptions can have significant financial impact.

5. **Directors & Officers (D&O) indemnification and coverage** is a particularly crucial area. Of note, Chief Information Security Officers (CISOs) are increasingly expected to be skilled across risk domains with responsibilities and decision-making authority yet might not hold C-Suite or board positions that would traditionally have the appropriate benefits and safeguards for personal liability.

6. **Representations & warranties** insurance also known as Warranty and Indemnity (W&I) coverage, has coverage specifically addressing unknown risks and potential losses arising from breaches or inaccuracies of representations, indemnities and/or warranties. In effect, it applies to unknowns i.e. undisclosed insider threats and vulnerabilities that may not be discovered during due diligence processes or even with a comprehensive insider program.

However, when it comes to current insurance products, it is unlikely that standard representations and warranties adequately cover AI model integrity, the authenticity of training data, or the long-term implications of AI system compromises. Premiums for insurance products are based upon historical data and risk assessments. Academic research into Insider threats, and weaknesses posed by LLM training data mean that underwriters struggle to agree how much coverage to underwrite for AI-specific risks.

Multi-national companies regulated by more than one jurisdictional regulator must assess whether to take advantage of regulatory arbitrage, i.e. shifting or outsourcing higher-risk activities into jurisdictions with lower regulatory compliance burden. Alternatively, the most pragmatic method of ensuring compliance is adopting a universal compliance programme to meet the most stringent compliance burden set by a regulator.

Standard insurance products were not designed to cover AI model integrity, training data authenticity, or the long-term consequences of system compromise

Conclusion

In conclusion, managing Insider risks in today's complex regulatory landscape and interconnected business environment requires a multifaceted approach that goes beyond traditional system-based strategies. Organizations must embrace a behavior-centric mindset, focusing on the human element to effectively identify and mitigate Insider threats. By understanding the evolving definitions of Insiders and recognizing the diverse range of individuals who may pose risks, businesses can develop robust Insider programs. As the region continues to evolve with advancements in technology, particularly AI, it is crucial for organizations to stay informed and agile, ensuring they are equipped to navigate the challenges posed by Insider risks and be prepared for Insider events which require the right forensic and legal expertise.

Endnotes

[1] Integrated Review Refresh 2023: Responding to a more contested and volatile world - GOV.UK

[2] National Protective Security Authority | NPSA

[3] Centre for the Protection of National Infrastructure - GOV.UK

[4] NPSA Changes Insider Risk Definitions

[5] Explanatory note (20) of DORA sets out... "the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal framework establishing a digital oversight authority" (Source: https://eur-lex.europa.eu/eli/reg/2022/2554/oj).

Deloitte authors:

Simon Cuerden
Partner | Forensic & Financial Crime Leader
Deloitte Middle East

Christopher Clements
Partner | Forensic & Financial Crime
Deloitte Middle East

Karthik Prabhakar
Partner | Forensic & Financial Crime
Deloitte Middle East

Pravin Arvyta
Director | Forensic & Financial Crime
Deloitte Middle East

KLME authors:

Carolina Gerding
Partner | Technology & Telecommunication | KLME

Khaled Shivji
Partner | AI & Technology | KLME

Deloitte.