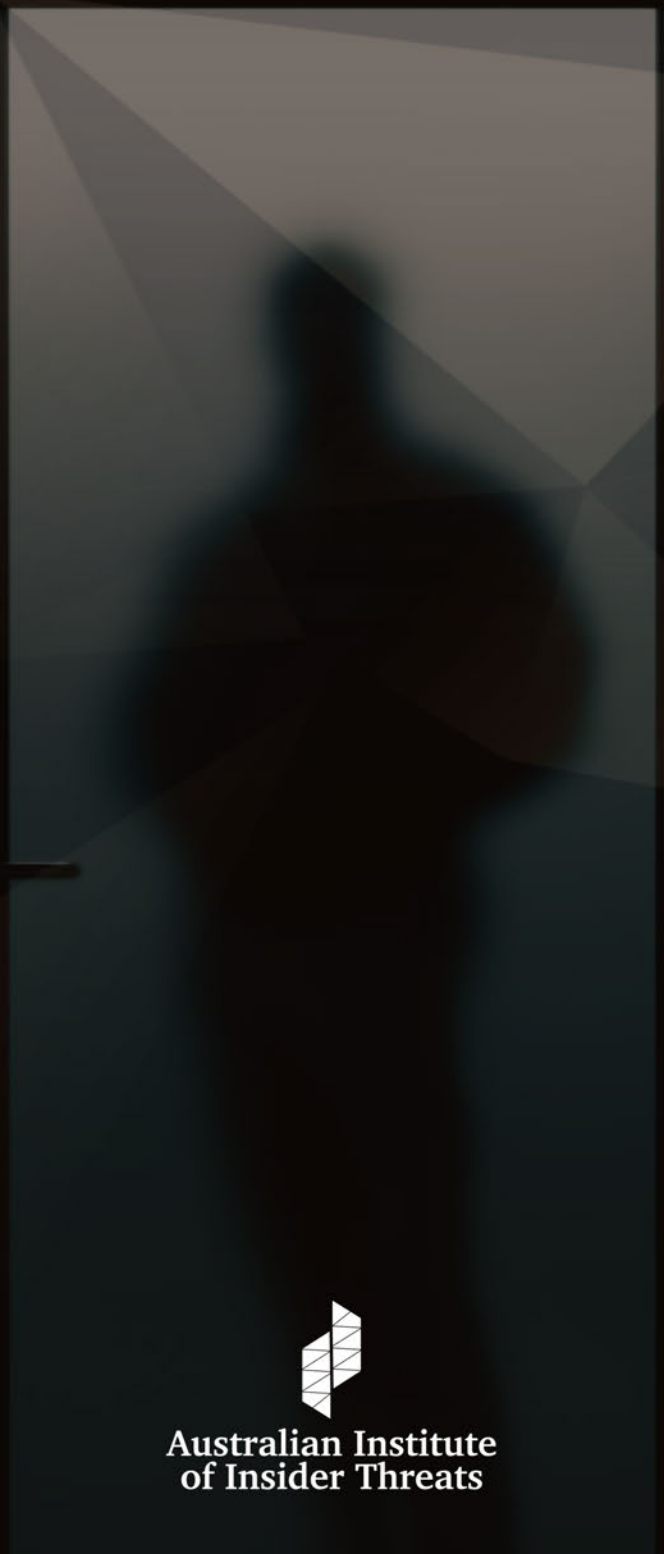
INSIDER THREATS VS INSIDER RISK

Why Industry Keeps Getting It Wrong



Australian Institute of Insider Threats

Table of Contents

INTRODUCTION

> *The greatest danger in times of turbulence is not the turbulence, it is to act with yesterday's logic.*
>
> — Peter Drucker

Does the industry continue to misunderstand the difference between insider threat and insider risk?

In many instances, the answer is yes, and the reason lies not only in the definition but also in how the problem is framed.

Across organisations and industries, the terms "insider threat" and "insider risk" are often used interchangeably. This is commonly thought to be a language issue. In reality, it reveals a deeper conceptual confusion.

The two terms are viewed as if they describe the same problem, when in fact they refer to different aspects of how harm happens within an organisation.

This confusion has been reinforced by a shift in terminology.

- Insider threat is seen as "malicious" and confronting. It implies intent, disloyalty, and the possibility of harm caused by trusted individuals.
- Insider risk, by contrast, is more "neutral". It aligns more easily with enterprise risk language and is less likely to create discomfort.

As a result, organisations and industry have increasingly adopted the term "risk" in place of "threat."

However, this shift has not led to greater clarity.

In practice, insider risk is neither treated as a threat nor fully integrated as a form of organisational risk.

It is often positioned at the margins. It may be recognised but not prioritised. It might be discussed, but not entirely accepted.

In many cases, it is missing from formal risk registers or is tucked into operational risk without distinction.

This reflects both structural and behavioural factors.

Structurally, insider risk does not fit neatly within existing risk categories. Behaviourally, it requires organisations to confront the possibility that trusted individuals may act in ways that cause harm, whether intentionally or unintentionally. This is often uncomfortable, and as a result, the issue may be deprioritised or avoided.

Insider risk is often interpreted as either a people problem or a system problem. In practice, it is neither in isolation.

It is created through the interaction between human behaviour, access, and organisational conditions.

- Threat reflects the capability of a trusted entity.
- Vulnerability reflects weaknesses across systems, policies, processes, culture, people and oversight.
- Access determines the ability to act, and
- Assets define what is at stake.

Risk emerges only when these elements interact. This distinction is important because it shapes where attention is directed.

When insider risk is viewed primarily as a people problem, organisations focus on identifying malicious intent or screening individuals. When it is viewed as a systems problem, attention is placed on controls, monitoring, and technology. In both cases, the interaction between elements is overlooked.

At the same time, the industry has increasingly approached insider risk from a solution perspective. Technology platforms, monitoring tools, behavioural analytics, and screening processes are often presented as mechanisms for managing insider risk.

While these capabilities provide value in specific areas, they address only part of the solution. They focus primarily on detecting activity or identifying individuals, rather than understanding how risk is
created.

This creates a further layer of confusion.

Organisations may believe they are managing insider risk because they have implemented specific controls or technologies.

In reality, they are addressing isolated elements, often associated with threat detection, while the broader conditions that give rise to risk remain insufficiently understood.

The distinction between insider threat and insider risk is therefore critical.

An insider threat refers to a trusted entity with the capability, and in some cases, the intent, to cause harm.

Insider risk, by contrast, reflects the potential for harm arising from the interaction between threat, vulnerability, access, and assets, with impact determining its significance.

The difference is not semantic. It is structural.

When these concepts are mixed, organisations tend to focus on identifying threats rather than understanding the vulnerabilities, access conditions, and organisational factors that enable harm.

The consequence is a persistent gap between perceived control and actual exposure. Organisations may improve their ability to detect activity or assess individuals, yet remain vulnerable due to unaddressed weaknesses in access, governance, culture, and organisational design.

In such cases, the presence of solutions can create confidence, while the underlying conditions that give rise to risk remain.

This paper addresses that gap. It clarifies the distinction between insider threat and insider risk, examines why the two are frequently confused, and explains how insider risk is created within organisational environments.

It also introduces a structured model for understanding insider risk as a system formed through the interaction of its components.

The objective is not to propose another solution. It is to correct how the problem is understood.

1

The Industry Has a Language Problem

The use of the term risk is reinforced by its widespread adoption within organisations.

Across enterprise environments, risk is a familiar concept, integrated into governance structures like risk registers, enterprise risk frameworks, and operational, financial, and legal reporting. In these environments, risk is seen as something that can be identified, evaluated, recorded, and tracked over time.

This familiarity influences how the term insider risk is understood. When it is first introduced, it is often seen in the same way as other risk categories, leading management to believe it can be handled similarly.

It is therefore regarded as something that can be measured, recorded, and managed within existing structures and reporting mechanisms.

At the same time, the term threat has gradually been avoided. It is often perceived as negative, suggesting intent, suspicion, or wrongdoing.

In organisational contexts, especially in human resources and workplace culture, this language can come across as confrontational or too accusatory.

The shift toward the term risk has therefore been, in part, an attempt to adopt language that is more neutral and more acceptable across the organisation.

This shift is understandable. However, it has introduced a conceptual gap.

By moving away from the term threat, the focus on the source of harm is reduced. Risk is then considered in isolation, as something that can be observed and managed, rather than something that emerges from the interaction between an actor and the organisation.

Insider risk does not exist independently. It arises when a threat, whether intentional or unintentional, interacts with vulnerabilities within organisational assets.

Without recognising the role of the threat, risk is treated as an abstract condition rather than a consequence of human or system behaviour.

As a result, applying conventional risk management approaches to insider-related harm can create a false sense of structure and control.

While the language aligns with established governance practices, it can obscure the relationship between threat, vulnerability, and risk.

Restoring this relationship is essential.

> *Risk cannot be fully understood without first understanding the threat that gives rise to it.*

KEY **Insights**

The shift from “insider threat” to “insider risk” has made the problem easier to describe, but harder to understand. By removing the concept of threat, organisations risk focusing on observable symptoms rather than the underlying causes of harm.

Implications for Organisations

When insider-related harm is framed primarily as a risk, organisations are more likely to rely on measurement and monitoring mechanisms.
This can lead to an overemphasis on detection, while the underlying drivers of risk - human behaviour, organisational vulnerability, and organisational conditions, remain insufficiently addressed.

2

The Illusion of “Managing Insider Risk”

The shift in language from insider threat to insider risk has influenced more than terminology. It has shaped how organisations believe the problem can be addressed.

When insider-related harm is framed as risk, it is often assumed that it can be managed in the same way as other enterprise risks, through measurement, monitoring, and control mechanisms. This assumption has contributed to the widespread belief that implementing specialised technology platforms is sufficient to manage the problem.

This belief is reinforced by how these platforms are positioned.

Many solutions describe themselves as managing insider risk. In doing so, they create the impression that the organisation has gained control over the problem.

The presence of dashboards, alerts, and analytics provides a visible and structured representation of activity, which can be interpreted as evidence that risk is being

actively managed.

This creates a sense of assurance. However, this assurance is often misplaced.

The capabilities of these platforms are, in most cases, well-defined. They are designed to detect anomalies, monitor behaviour, and support investigation through the collection of evidence. These functions are valuable and, in many cases, necessary.

But they represent only one part of the broader solution to managing insider risk.

They do not address the conditions that give rise to risk.

They do not influence how individuals make decisions, how teams operate, or how organisations establish and enforce expectations.

They do not address weaknesses in governance, close policy gaps, or improve the effectiveness of processes.

Most importantly, they do not reduce vulnerability.

The distinction is critical.

- Detection provides visibility.
  It does not provide control.
- Monitoring identifies activity.
  It does not prevent behaviour.
- Evidence supports investigation.
  It does not address the cause.

When organisations equate the implementation of technology with the management of insider risk, the focus narrows. Effort is directed toward observing what has already occurred or is in progress, rather than understanding and addressing why it occurs.

As a result, risk is managed reactively.

The organisational conditions that shape insider risk: Culture, behaviour, governance, and vulnerability are not directly addressed.

This creates an illusion of control.

- The organisation can see more.
- It can measure more.
- It can report more.

But seeing is not the same as building risk resilience.

The consequence is not that technology is ineffective. It is that it is often overextended beyond its intended role.

Technology is a component of insider threat management. It enables detection and supports response. It provides important signals that can inform decision-making.

However, it is only a single pillar of risk resiliency.

To build insider risk resiliency effectively, organisations must move beyond detection.

They must address the vulnerabilities that let threats access organisational assets. This demands a broader capability, encompassing governance, culture, policy, process, and behavioural understanding, supported by technology rather than driven by it.

KEY **Insights**

Technology platforms positioned as managing insider risk mainly offer detection and investigation capabilities. This creates a perception of control but does not tackle the root causes of the risk.

Implications for Organisations

Organisations that rely on technology as the primary mechanism for managing insider risk are likely to operate reactively. Without addressing organisational vulnerability, governance, and behavioural factors, risk remains present despite increased visibility.

3

What An Insider Threat Actually Is

The term insider threat is often misunderstood.

It is often linked to malicious individuals who intentionally aim to harm the organisation for personal, financial, ideological, or other motives.

While such cases are important, they represent only one part of a broader and more complex reality.

An insider threat is not defined solely by malicious intent.

An insider threat arises from the presence of a trusted entity with the capability to cause harm through authorised access. This includes employees, former employees, contractors, business partners, third parties, and systems that are granted legitimate access to organisational assets, whether operating internally or through connected external relationships.

These entities may act intentionally, negligently, unknowingly, or under external influence. In each case, the capability to cause harm exists, regardless of whether

intent is present.

This distinction is critical.

A narrow focus on malicious intent limits the understanding of insider-related harm. Many significant incidents arise not from deliberate action, but from human error, poor judgment, lack of awareness, or failures in process and oversight. The absence of intent does not reduce the potential for impact.

The nature of trusted access has also evolved.

Organisations now operate across distributed environments, with remote and globally dispersed workforces accessing systems and data from a wide range of locations. Access is no longer confined to controlled office settings, and organisational boundaries are increasingly fluid.

At the same time, the traditional concept of a defined network perimeter has diminished. Applications and information are commonly delivered through cloud-based platforms, enabling access from virtually any location. The distinction between internal and external environments is no longer clearly defined.

In this context, access, not location, has become the primary control point.

> *What defines an insider is not where they are, but the level of access they hold and how that access is governed.*

The scope of insider threat must also extend beyond people.

Organisations are increasingly authorising artificial intelligence, automated systems, and digital agents to access applications, data, workflows, and decision-making processes.

In many settings, these systems are integrated within organisations and given trusted access to perform tasks that were previously done by humans.

These systems may retrieve information, move data between platforms, generate outputs, trigger actions, or interact directly with business processes at scale.

They do not have intent in the traditional human sense. However, they do have the capability, and when that capability is combined with trusted access, the potential for harm becomes real.

This is particularly important because synthetic insiders can operate with speed, scale, and persistence well beyond human capacity. Where access is excessive, controls are weak, or oversight is limited, their actions can amplify error, misuse, exposure, or disruption across the organisation.

Taken together, insider threat can be understood as encompassing human insiders, such as employees, contractors, and partners, as well as human-directed insiders, like those who are coerced, manipulated, or compromised, and synthetic insiders, such as authorised AI systems, automated processes, and digital agents with trusted access.

Each operates within a position of trust. Each has the capability to cause harm.

This reframing restores clarity.

> *An insider threat is not just a label applied to individuals. It is a situation that arises when trusted access is present along with the ability to do harm.*

From this perspective, threat is not inherently negative. It is a recognition of potential within a trusted environment.

Understanding insider threat in this way provides a more complete foundation for managing risk. It shifts the focus from identifying malicious actors to understanding how access, capability, and organisational conditions interact.

Without this understanding, the concept of insider risk remains incomplete.

KEY **Insights**

An insider threat is defined by trusted access and capability, not solely by malicious intent. It includes employees, third parties, and authorised systems operating within the organisation, whether acting deliberately or unintentionally.

Implications for Organisations

Organisations that define insider threat too narrowly, focusing only on malicious individuals or internal staff, risk overlooking a wide range of scenarios that can lead to harm. A broader understanding of trusted access is required to effectively identify and build insider risk resilience.

4

What Insider Risk Actually Means

> *Insider risk is not fundamentally a problem of detection. It is a problem of organisational blindness.*

It reflects what leaders do not see, do not want to see, or are not structured to see.

These conditions arise in different ways.

- Some risks are not recognised due to limited awareness or understanding. Changes in behaviour, pressure indicators, or shifts in conduct may not be identified early.
- Other risks are visible but not addressed. Concerns may be dismissed, minimised, delayed, or avoided due to competing priorities or organisational culture.
- In some cases, the organisation is not structured to see risk at all. Information is fragmented, responsibilities are

unclear, and systems do not provide a consistent view of behaviour, access, and organisational conditions.

Insider risk is not a singular condition. It is defined by the interaction of three components: Threat, Vulnerability, and Impact.

- Threat refers to the capability, and in some cases intent, of a trusted entity to cause harm.
- Vulnerability refers to weaknesses within organisational controls, culture, processes, access, or oversight.
- Impact refers to the consequence arising from the realisation of harm to organisational assets.

Risk exists only where these components intersect.

These components are inherently variable. Threat is subject to change as individuals respond to internal and external influences, including pressure, motivation, and opportunity.

Vulnerability is shaped by organisational design, control effectiveness, governance, and cultural conditions, all of which evolve over time.

Impact is contingent upon the value, sensitivity, and exposure of organisational assets, which may also change.

Accordingly, insider risk is neither fixed nor stable…Insider risk is dynamic and adaptive.

It changes as the components that define it change. It cannot be reduced to a static level of exposure, nor can it be reliably inferred from historical observations alone.

Any assessment of insider risk must therefore consider the changing relationship between threat, vulnerability, and impact.

A common limitation in practice is the disproportionate focus on threat.

Organisations often evaluate insider risk by looking for signs of malicious activity or behavioural anomalies. This method assumes that the existence of a threat is the main factor determining risk. However, this assumption is incomplete.

Risk may be elevated in the absence of an observable threat where vulnerabilities are significant, and the potential impact is high. Conversely, the presence of a capable insider does not necessarily result in harm where vulnerabilities are effectively controlled.

> *The absence of a detected threat does not constitute evidence of low risk.*

It may instead indicate limitations in visibility, interpretation, or organisational awareness.

Organisational blindness arises when the interaction between threat, vulnerability, and impact is not fully understood or observed.

This may result from fragmented information, insufficient integration of data sources, unclear accountability, or structural limitations that prevent a comprehensive view of risk.

In such conditions, risk is considered in isolation rather than as a function of interacting components.

The consequence of this blindness extends beyond missed malicious activity.

It includes the inability to identify individuals under pressure before harm occurs.

An organisation that cannot see vulnerability cannot intervene early. It can only respond after impact has materialised.

Effective resilience of insider risk requires a systemic perspective.

It requires visibility of the components that define risk and an understanding of how they interact within the organisational environment.

This includes:

- The capability and access of trusted entities
- The vulnerabilities present within the organisation
- The potential impact on critical assets

Without this integrated view, risk cannot be fully understood.

KEY **Insights**

Insider risk is defined by the interaction of threat, vulnerability, and impact. It is inherently dynamic and cannot be understood through isolated indicators or static measures.

Implications for Organisations

Organisations that mainly focus on threat detection tend to underestimate risk. An effective resilience approach involves a comprehensive understanding of vulnerability and impact, supported by visibility across all components.

5

The Implications of Organisational Blindness

Organisational blindness is not a theoretical limitation. It has direct and observable consequences for how insider risk is understood and managed.

> *When the interaction between threat, vulnerability, and impact is not apparent, risk is misunderstood.*

This misinterpretation influences how resources are allocated, decisions are made, and how effectively the organisation can respond to emerging conditions.

One consequence is the misallocation of effort.

Organisations frequently invest in capabilities designed to detect indicators of threat, including behavioural anomalies and suspicious activity.

While such capabilities are necessary, they address only one component of insider risk.

Where vulnerability remains insufficiently examined, and impact is not clearly understood, organisational effort becomes focused on observation rather than on reducing exposure. In these circumstances, the organisation may improve its ability to spot activity without enhancing its capacity to manage risk.

A second consequence is delayed intervention.

Where vulnerability is not visible, early indicators of pressure, behavioural change, or organisational stress may not be recognised.

Individuals who may be at risk of making harmful decisions are not identified in time, and opportunities for early intervention are missed.

As a result, the organisational response is triggered only after harm has materialised, rather than at the point at which it could have been prevented.

A third consequence is the failure to escalate and act on known signals.

In some cases, indicators of risk are visible to individuals or systems. These may include behavioural changes, access anomalies, or contextual clues that indicate increased exposure. However, such signals are often not escalated or acted upon. This can happen when responsibility is unclear, accountability is spread out, or individuals hesitate to act due to fears of making wrong decisions or causing unintended consequences. In addition, organisational culture might discourage escalation, especially when raising concerns is seen as disruptive or unwelcome. In these situations, risk is present; it is recognised but not addressed.

A fourth consequence is the creation of false assurance.

The existence of policies, controls, and monitoring systems can give the impression of control. Metrics are reported, dashboards are examined, and activity is monitored.

However, these indicators show what can be observed rather than the underlying factors that cause risk.

As a result, the organisation may appear secure while exposure remains.

A fifth consequence is fragmented accountability.

Responsibility for threat, vulnerability, and impact is often divided among different organisational functions. Security teams may concentrate on detection, risk, and compliance, while governance and business units focus on operational delivery. Without integration, no single function has a full view of how risk is created or how it evolves.

Risk is therefore not managed as an interconnected system, but as a set of separate concerns.

A sixth consequence is the normalisation of risk over time.

When visibility is limited, behaviours and conditions that should be seen as warning signs may become accepted as normal parts of operations. Excessive access, policy breaches, and cultural pressures might no longer be recognised as risk factors. Instead, they become ingrained in daily practice, further heightening exposure.

These consequences are cumulative. They do not occur independently but reinforce one another, creating an environment in which risk is both present and insufficiently understood.

Detection capability may increase, but underlying exposure remains unchanged.

Organisational blindness does not prevent risk from existing. It prevents risk from being recognised and addressed. The issue is not the absence of controls, but the absence of visibility into how those controls operate in practice, how behaviour is changing, and how vulnerability is evolving.

The central implication is clear. Insider risk is not unmanaged because it is inherently complex. It is unmanaged because it is not seen clearly, or because it is not acted upon when it is seen.

KEY **Insights**

Organisational blindness results in misallocation of effort, delayed intervention, failure to act on visible signals, false assurance, fragmented accountability, and the normalisation of risk.

Implications for Organisations

Where risk is not visible across threat, vulnerability, and impact, or where visible indicators are not acted upon, organisations are likely to focus on detection while underlying exposure remains unaddressed.

6

The Model The Industry Is Missing

The previous chapters have shown that confusion in the field comes from failing to clearly distinguish between threat and risk, and from treating insider risk as something that can be detected rather than understood.

To address this, a structured model is required.

This model must distinguish between the components that give rise to risk and explain how they interact.

A Structured View of Insider Risk

Insider risk is best understood as the interaction between five elements:

- Threat
- Asset
- Vulnerability
- Access
- Impact

Each element represents a distinct aspect of the system. Risk does not reside in any single element. It emerges from their interaction.

Threat

Threat refers to a trusted entity with the capability, and in some cases intent, to cause harm.

This includes employees, contractors, third parties, and systems operating with authorised access. Threats are not limited to malicious actors. They also encompass negligent, compromised, or unaware individuals, as well as automated systems acting under delegated authority.

> *Threat defines who or what has the potential to act.*

Asset

Asset refers to what the organisation seeks to protect.

This includes information, systems, processes, intellectual property, operational capability, and, importantly, people.

Individuals within an organisation can be viewed as assets because their well-being, knowledge, and abilities are vital to organisational performance. Harm to individuals, whether through coercion, pressure, or exploitation, can directly affect the organisation.

At the same time, individuals may also serve as threat actors, depending on their access, capability, and behaviour.

This dual role is a defining characteristic of insider risk and distinguishes it from many other forms of risk.

Asset therefore, defines what is at stake, including both organisational resources and the people who operate within them.

> *Asset defines what is at stake.*

Vulnerability

Vulnerability refers to weaknesses (vulnerabilities) within the organisation that may enable harm to occur.

These weaknesses are not confined to technical systems. They arise across multiple domains and must be understood in a structured manner.

A comprehensive view of insider risk requires recognising the different forms that vulnerability may take.

- ***Human Vulnerabilities*** - Arise from individual circumstances, behaviours, and limitations that may increase exposure to risk. These may include stress, dissatisfaction, lack of awareness, coercion, or changes in personal circumstances. Such conditions may influence decision-making, increase susceptibility to exploitation, or lead to actions that cause harm.

- ***Technological Vulnerabilities*** - Arise from weaknesses in systems, infrastructure, and access control mechanisms. These may include inadequate access controls, outdated systems, unpatched software, or poorly configured environments. Such weaknesses may create opportunities for misuse, unauthorised access, or unintended exposure of information.

- ***Physical Vulnerabilities*** – Arise from weaknesses in the security of facilities, environments, and physical assets. These may include inadequate building access controls, unsecured workspaces, poor asset protection, or insufficient monitoring of physical entry and movement. Such conditions may enable unauthorised access to systems, information, or equipment.

- ***Organisational Vulnerabilities*** - Arise from structural and governance-related weaknesses. These may include fragmented responsibilities, a lack of coordination between functions, unclear ownership, or insufficient information sharing. In such cases, risk indicators may not be linked, and the relationship between threat, vulnerability, and impact may not be fully evident.

- ***Cultural Vulnerabilities*** – Arise from the norms, behaviours, and expectations present within the organisation. These may include low levels of trust, poor communication, disengagement, or environments where concerns are not raised or acted upon. Cultural conditions influence how people behave and whether signs of risk are recognised or ignored.

- ***Policy Vulnerabilities*** – Arise from weaknesses in the design, clarity, or enforcement of organisational policies. These may include incomplete policies, ambiguous requirements, a lack of alignment between policy and practice, or policies that are not consistently applied. Such weaknesses can create uncertainty, reduce accountability, and enable behaviours that increase risk exposure.

- ***Procedural Vulnerabilities*** - Arise from weaknesses in processes and operational practices. These may include inconsistent or outdated procedures, ineffective access management, or gaps in processes such as onboarding, offboarding, or incident response. Such weaknesses may result in exposure where controls are not applied consistently.

Access

Access means a trusted entity's ability to interact with organisational assets.

This covers system permissions, physical entry, and indirect access via integrated systems or delegated authority. In contemporary settings, access is frequently distributed, flexible, and not always immediately apparent.

> *Access defines how interaction is possible.*

Impact

Impact refers to the consequence if harm occurs.

This may involve financial loss, operational disruption, reputational damage, regulatory consequences, or loss of trust. Impact is not part of risk itself, but it determines the significance of risk when realised.

> *Impact defines why the risk matters.*

These domains do not operate independently.

Vulnerabilities can exist across multiple domains at the same time,
and their significance depends on how they connect to threats,
access, and the asset's value.

> *Vulnerability defines where the organisation is exposed.*

Understanding the Interaction

Insider risk emerges from the interaction between its constituent elements. It does not reside within any single component but is realised through their combined effect.

A threat without access lacks the means to act. Access provides capability, and vulnerability creates the opportunity for harm.

However, these conditions alone do not result in harm. Harm occurs only when they are acted upon, whether intentionally or unintentionally.

The presence of intent may increase the likelihood of harm, but it is not required for harm to occur. Negligence, error, lack of awareness, or external influence may also activate existing vulnerabilities.

The significance of harm is determined by the asset's value and exposure. When critical assets are exposed, even low levels of threat or unintentional behaviour may have significant consequences.

Insider risk, therefore, becomes meaningful only when these elements interact. It reflects not a single condition, but the alignment of capability, opportunity, behaviour, and impact within the organisational environment.

A System, Not a Signal

This model establishes a critical distinction between isolated indicators and systemic understanding.

Insider risk cannot be reduced to a signal to be detected. It must be understood as a

system formed by the interaction of multiple elements.

Although individual components may be seen separately, risk cannot be fully understood without understanding the connections between them. A fragmented view of threat, vulnerability, or impact does not give a complete picture of risk.

A comprehensive understanding, therefore, requires an integrated perspective that considers how these elements interact within the organisational environment.

Resolving the Industry Confusion

This model provides a clear distinction between insider threat and insider risk.

- **Insider threat** refers to the presence of a trusted entity with the capability, and in some cases, intent, to cause harm.
- **Insider risk** refers to the potential for harm arising from the interaction between threat, vulnerability, access, and assets, where harm may be realised through behaviour, whether intentional or unintentional, and with impact determining its significance.

Implications of the Model

The significance of this model lies not in prescribing specific actions but in providing a consistent and structured basis for understanding insider risk.

It establishes a clear distinction between the components that define risk, enables risk to be interpreted as a system rather than a set of isolated indicators, and supports the integration of perspectives across organisational functions.

In the absence of such a model, organisations are likely to continue focusing on individual elements, particularly threat, while overlooking the interaction of conditions that give rise to risk.

KEY **Insights**

Insider risk does not reside in threat, vulnerability, or impact alone.

It emerges from the interaction between threat, asset, vulnerability, access, and impact.

Implications for Organisations

Where these elements are not understood as an integrated system, insider risk is likely to be misinterpreted, leading to fragmented visibility and incomplete understanding.

7

Where Risk Is Actually Created

Insider risk is not created by a single event, system, or individual.

It emerges from the interaction between people, access, and organisational conditions, and develops gradually rather than at a single point.

By the time an action is detected or an incident occurs, the conditions that led to that outcome have already been established.

These conditions rarely result from a single decision or failure.

Instead, they gradually develop through a combination of access choices, behavioural changes, and organisational factors that evolve over time.

> *Risk is therefore not generated at the point of detection. Detection shows activity, not the source of risk itself.*

The origin lies in how access is granted and maintained, how vulnerabilities are introduced or left unaddressed, and how individuals behave within the environment in which they operate.

Access often expands over time as roles change, systems are integrated, and permissions are accumulated without consistent review.

At the same time, vulnerabilities can arise across technical, procedural, cultural, and governance domains. These might include control gaps, unclear processes, fragmented oversight, or situations that hinder accountability and transparency.

Human behaviour adds a further dimension.

Individuals do not operate in a static state. Their decisions and actions are influenced by pressure, motivation, personal circumstances, and opportunity.

These influences may evolve slowly and are not always detectable through formal controls or monitoring systems. As behaviour shifts, insiders interact with existing access points and vulnerabilities in ways that can either increase or decrease exposure.

This interaction is not linear and cannot be understood through isolated indicators.

Risk is created when these elements converge.

Access provides capability, vulnerability provides opportunity, and behaviour determines how that capability and opportunity are used. Where these elements align in the presence of valuable assets, the conditions for potential harm are established.

In this sense, risk is not introduced at the point of action. It is embedded in the environment that enables action.

This interaction is shaped by the organisational environment.

Decisions about access control, policy enforcement, governance structures, and cultural expectations influence how risk develops.

- Where access is not well governed, vulnerabilities are more likely to persist.
- Where culture discourages escalation or limits visibility, early indicators of risk may not be recognised or acted upon.
- Where policies are inconsistently applied or not enforced in practice, gaps emerge between formal controls and actual behaviour.
- Where oversight mechanisms are weak or not regularly exercised, deviations from expected behaviour may remain undetected.
- Where responsibilities are fragmented, no single view of risk exists.
- Where critical assets are not clearly identified or prioritised, exposure may exist without being recognised.
- Where individuals operate under pressure, stress, or changing circumstances, behavioural shifts that influence risk may not be recognised.

These conditions do not create risk independently, but they influence how the components of risk interact.

> *It is therefore possible for risk to exist without any observable signal.*

The necessary conditions may already be in place, even where no malicious or negligent behaviour has been detected. In such cases, the absence of activity does not indicate the absence of risk. It indicates that the conditions have not yet resulted in observable outcomes, or that those outcomes have not yet been recognised.

This highlights a key idea. Insider risk is not created when harm occurs. Instead, it is built on the conditions and environment that allow harm to happen.

Understanding where risk originates requires paying attention to how threat, vulnerability, access, and assets interact within the organisation, and how these interactions evolve over time.

Without this understanding, organisations are likely to identify risk only after it has materialised, rather than recognising it in the conditions that come before it.

KEY **Insights**

Insider risk arises from the combination of behaviour, access, vulnerability, and organisational factors that exist before any visible activity or incident takes place.

Implications for Organisations

When the focus is on detecting activity rather than understanding how risk develops, organisations are likely to react only after harm has occurred.

8

You Cannot Buy Your Way Out Of Insider Risk

Insider risk cannot be resolved through the acquisition of technology alone.

This is not a limitation of technology itself, but a result of how insider risk develops.

As established, risk arises from the interaction of threat, vulnerability, access, and assets, influenced by human behaviour and organisational factors. Technology functions within this framework but does not define or control it.

In practice, many organisations approach insider risk as a capability challenge. The assumption is that with sufficient monitoring, analytics, and detection tools, risk can be identified and managed successfully. This leads to significant investment in platforms that are built to detect anomalies, monitor behaviour, and raise alerts.

While these capabilities are valuable, they address only a portion of the problem.

Technology is effective at identifying signals. It can detect unusual access patterns, behavioural deviations, or

indicators of potential misuse. It can provide visibility into activity and support investigation after an event has occurred.

However, these capabilities function only at the point where activity becomes observable. They do not address the conditions that allow that activity to happen.

Risk is not caused by the lack of monitoring. Instead, it arises from vulnerability, the distribution of access, and organisational and behavioural factors.

Technology does not determine how access is granted, how culture influences behaviour, or how vulnerabilities emerge and persist. These are shaped by organisational decisions, governance structures, and leadership priorities.

As a result, organisations may increase their ability to detect activity without reducing the level of risk that exists within the environment. Detection capability improves, but the underlying conditions remain unchanged. This creates a situation in which organisations become more effective at identifying incidents, but not necessarily at preventing them.

This distinction is critical.

> *Detection provides visibility after conditions have aligned. It does not prevent those conditions from forming.*

Where vulnerability is present, access is excessive, and critical assets are exposed, the potential for harm exists regardless of the presence of monitoring tools. Technology may identify the activity when it occurs, but it does not eliminate the opportunity for it to take place.

This highlights that insider risk is a system rather than a product. Risk cannot be simply bought or achieved. It arises from the interactions of various elements that go beyond technology.

Technology remains a vital pillar of insider risk governance. It enhances visibility, supports investigations, and helps organisations identify warning signs. However, it functions within the broader risk framework and cannot replace the need to understand and address the root causes of those risks.

Insider risk is therefore not something that can be purchased and resolved. It must be understood in terms of how it is created, how it evolves, and how the organisation influences interactions among its components.

KEY **Insights**

Technology can identify signals of insider activity, but it cannot change the conditions that create insider risk.

Implications for Organisations

Organisations that rely primarily on technological solutions are likely to improve detection capability without reducing underlying exposure to risk.

From Understanding To Action

The purpose of this paper is not to provide a checklist or prescribe a solution. It is to establish clarity.

However, clarity introduces responsibility.

For leaders and boards, the question is no longer whether insider risk exists, but whether it is understood in the context of how it is created, how it evolves, and how visible it is within the organisation.

Where this understanding is incomplete, further discussion is required.

The Boardroom Executive Briefing

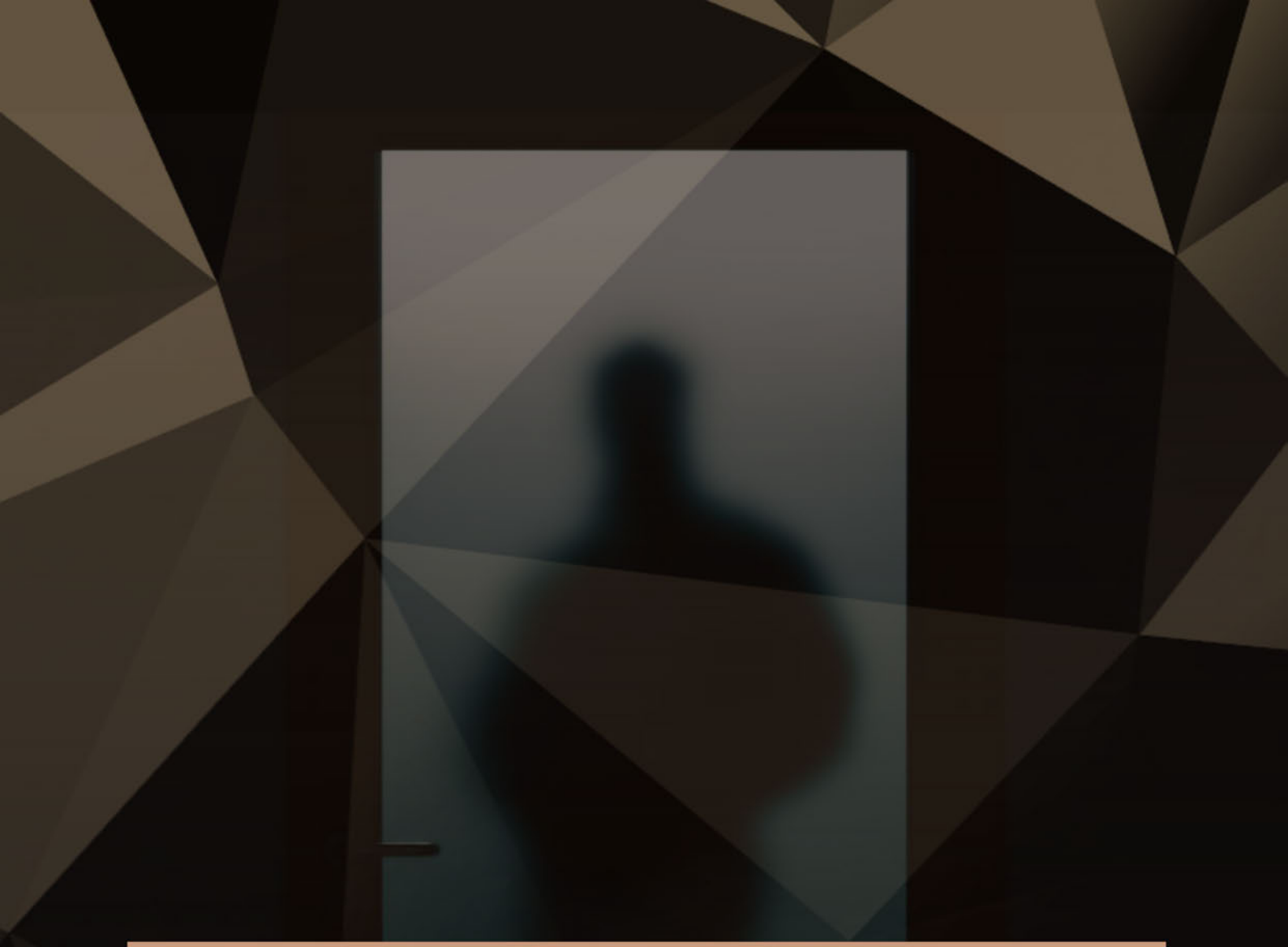
has been created to support this discussion. It offers a structured overview of insider risk from a leadership viewpoint, emphasising visibility, accountability, and decision-making.

The briefing explores how risk develops within organisational settings, how it can stay hidden, and how leaders can understand risk beyond technical signs and scattered reports.

It is tailored for executive and board-level engagement and is intended to provide clarity rather than technical depth. The format is concise and focused, enabling leaders to understand the implications of insider risk within their own organisational context.

An initial discussion can be used to explore whether the briefing is appropriate and aligned with organisational priorities. This includes an overview of the format, topics covered, and expected outcomes.

If this paper has raised questions about how insider risk is understood within your organisation, a discussion may provide a useful next step.



Australian Institute
of Insider Threats

www.insiderthreats.com.au
hello@insiderthreats.com.au
+61 2 6198 3381