

WHO HAS THE CAPABILITY TO MATERIALLY IMPACT YOUR ORGANISATION?

Why Significant
Insider Exposure Can
Extend Far Beyond
the Executive Suite.



TABLE OF CONTENTS

▶	03	<u>Looking Beyond The Organisation Chart</u>
▶	05	<u>We Misunderstand Where Power Sits</u>
▶	07	<u>What Actually Creates Capability</u>
▶	10	<u>The People We Don't Think About</u>
▶	13	<u>Why Organisations Don't See It</u>
▶	16	<u>When Capability Becomes Consequence</u>
▶	19	<u>Conclusion - Looking Beyond Position</u>
▶	21	<u>About The Author</u>

LOOKING BEYOND THE ORGANISATION CHART

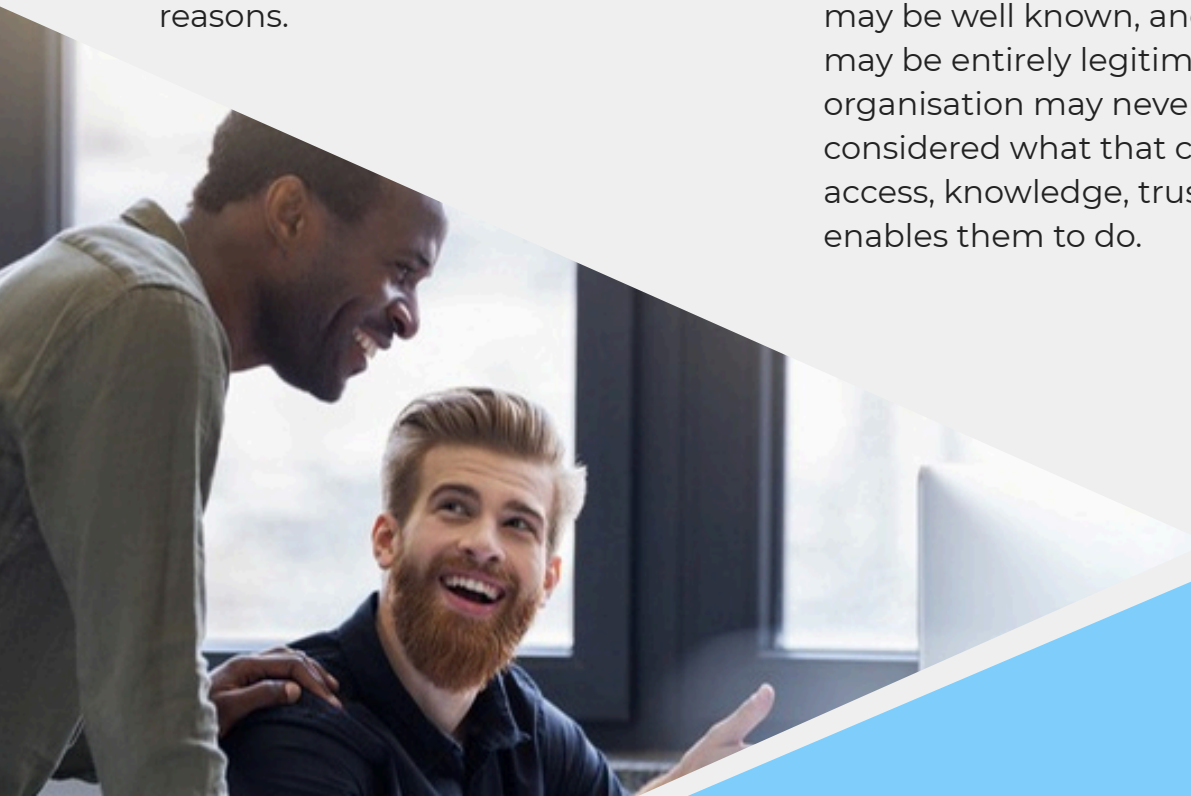
Every organisation has a formal structure. We know who leads, who reports to whom, who owns decisions and who holds formal accountability.

But that doesn't necessarily tell us who has the capability to materially affect an organisation.

Senior executives are an obvious example. Their authority, influence and decision-making responsibilities give them significant capability to affect organisational outcomes. But that capacity can also exist much further down the organisational structure, and for very different reasons.

As an investigator and intelligence practitioner, I have learned to look beyond the organisational chart. People in less senior or less visible roles can sometimes have significant capability because of their access, the information they see, the relationships they have built, or their understanding of how the organisation actually works.

This is important because organisations can spend considerable effort managing the risks they readily recognise, while overlooking capabilities that have developed elsewhere. The individual may be well known, and their access may be entirely legitimate. But the organisation may never have considered what that combination of access, knowledge, trust and position enables them to do.





And that raises an
important insider
threat question:

**How well does your
organisation
understand where the
capability to cause
significant harm exists?**

This article explores why that capability can be difficult to recognise, where it can develop, and why understanding it is an important part of assessing your organisation's insider exposure.

01 WE MISUNDERSTAND WHERE POWER SITS

Most organisations continue to rely, consciously or not, on hierarchy as a proxy for control.

Risk frameworks are often aligned with seniority. Oversight mechanisms focus upwards. High-impact decisions are assumed to flow from the top.

When organisations ask where risk lies, the answer is often shaped by who holds formal authority.

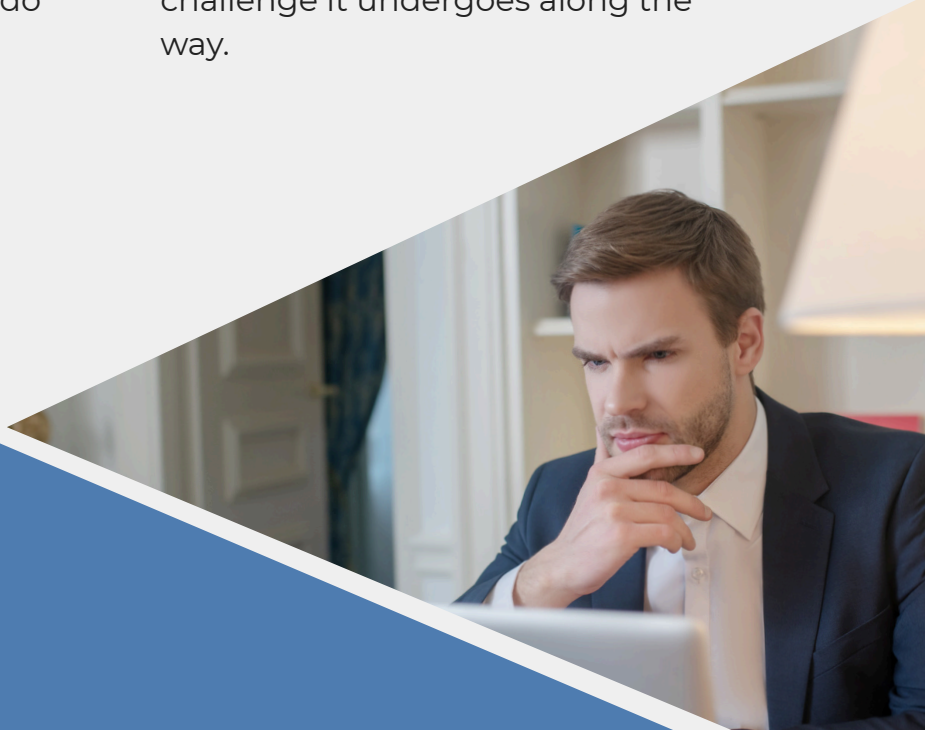
But hierarchy is a representation of control, not a guarantee of control.

In practice, the ability to influence outcomes, shape decisions, or make an impact often depends less on what someone is authorised to do and more on what they can do.

And those two things are no longer the same.

Take, for example, an intelligence or insights team tasked with providing options to senior decision-makers. We often assume that those at the top of a hierarchy make decisions largely on their own judgement and experience. In reality, those decisions are also shaped by the information, analysis and recommendations from people further down the organisation.

The quality of the decision is therefore intrinsically linked to the quality and accuracy of the information that reaches the decision-maker, and to the level of challenge it undergoes along the way.



From an intelligence perspective, this is an important distinction. The person making the final decision clearly holds significant authority, but those who collect, interpret, filter and present the information can also exert considerable influence over the outcome.

Their position in the hierarchy may be very different. Their ability to materially affect what happens may not be.

Low Profile, High Impact

There is a persistent assumption across many organisations that impact correlates with visibility. Those who can cause the most disruption are often assumed to be the most visible: Senior leaders, decision-makers and individuals with formal authority.

But significant capability can also reside with people who attract little attention. They may have limited authority and little influence over organisational decisions, yet their access, knowledge, relationships or position within a critical process can enable them to materially affect an outcome.

Understanding where that capability comes from requires looking beyond hierarchy and asking what actually enables someone to be consequential.

02 WHAT ACTUALLY CREATES CAPABILITY

Within any organisation, there are individuals who sit at critical junctions of access.

They may not hold senior titles or appear on risk registers. They are often operational, embedded in the day-to-day functioning of the business. However, through a combination of permissions, knowledge and proximity, they can become uniquely positioned.

They may see across systems in ways others cannot. They can move information between environments, influence how processes are applied in practice, or interpret and filter information before it reaches decision-makers.

But access alone doesn't explain capability.

From an investigation and intelligence perspective, access can be obtained and capability can be developed. Someone's organisational knowledge, trusted relationships, understanding of processes and workarounds, credibility with colleagues, or ability to influence others may be just as important as the permissions they currently hold.



This raises a different insider risk question. Rather than looking only at who currently holds privileged access, organisations also need to consider who could legitimately accumulate greater capability over time.

A person may move between roles, gain additional permissions, build relationships, acquire knowledge, and become increasingly trusted. None of these developments is necessarily unusual or concerning. In many cases, they are simply part of someone's career and their value to the organisation.

But collectively, they can significantly change what that person is capable of.

“ Access can be acquired. Capability can be developed. The person who appears unlikely to attract attention today may, under different circumstances, become highly significant tomorrow. ”

Steve W.

This doesn't mean organisations should treat people as potential threats simply because they are knowledgeable, trusted or well connected. It means insider risk cannot be understood by looking at a snapshot of who has access today.

Motivation also needs to be considered. People's circumstances, relationships and intentions can change, as can their access and capability. The challenge is understanding how those factors can come together and whether the organisation would recognise a meaningful change before harm occurs.

| Consider your own organisation:

Are you assessing only who has significant access today, or do you understand how capability is accumulating over time?

Takeaway: Access tells you what someone can reach today. Understanding capability requires a much broader view of what they know, who they know, how they operate and what they may be able to do tomorrow.

03 THE PEOPLE WE DON'T THINK ABOUT

Between strategic leadership and front-line execution lies what might be described as the operational middle.

This is where processes are enacted, systems are navigated, and organisational intent is translated into action. It is also where access, knowledge and trust accumulate over time.

Individuals in these roles may develop broad system permissions, deep process knowledge, an understanding of workarounds and exceptions, trusted relationships across the organisation, and considerable autonomy gained through experience.

None of this is inherently problematic. In many cases, it is essential for organisations to operate efficiently.

But it can create significant capability that isn't always matched by corresponding visibility or protection.

I encountered this directly while debriefing an Executive Assistant to a CEO. The EA had access to much of the same information and systems as the CEO, yet had little appreciation that this could make them a potential target.

The contrast was striking. The CEO had a range of protective measures in place - a secure property, a safe room, CCTV and other physical security arrangements. The person with comparable access to much of their information had none of those protections.





That raises an
uncomfortable
question:

If an adversary cannot easily reach the principal, why wouldn't they look for the person who can provide almost everything they need without ever having to approach the principal?

The point is not that an Executive Assistant poses an insider threat. It is that organisations can protect people according to their status, rather than recognising the capability that may exist around them.

An EA may have no decision-making authority, yet possess the access, knowledge, relationships and proximity necessary to materially affect an organisation's security or that of its leadership.

This extends well beyond Executive Assistants. Low-profile roles embedded within systems and processes can have disproportionate impact precisely because they operate below the threshold of attention. Their access may have accumulated over time, their knowledge may extend well beyond their formal responsibilities, and the trust they have earned may mean their activities are rarely questioned.

| Consider your own organisation:

Who are you protecting because of their position, and who might you be overlooking because their position seems unimportant?

Takeaway: We tend to protect the people we know are important. The greater blind spot may be the people who have become important because of what they know, what they can access, and whom they are trusted by.

04 WHY ORGANISATIONS DON'T SEE IT

Organisations invest heavily in visibility.

Dashboards, reporting, analytics and audit trails are designed to provide insight into what is happening within the business. These tools create a sense of control, a belief that activity is observable, measurable and therefore manageable.

But visibility is only as effective as the assumptions that underpin it. If those assumptions prioritise formal authority, known access and how processes are supposed to operate, organisations may still overlook how capability has developed in practice.

Most organisations design their controls around how processes are meant to work. Real-world operations rarely follow that design perfectly.

Over time, exceptions emerge. Workarounds develop. Access is granted to solve immediate problems and isn't always reviewed. Responsibilities shift. Informal relationships develop. People become relied upon for tasks that may extend well beyond their formal role.

What emerges is a gap between design and reality.

What Investigations Reveal

What tends to become apparent during an investigation is how different an organisation's formal understanding of itself can be from how it actually operates.



Investigations often reveal relationships, dependencies and informal pathways that don't appear on an organisational chart or risk register. Someone may have access because it was granted years ago to solve a problem, while another person has become the unofficial conduit through which information or decisions flow.

Perhaps most importantly, investigations reveal how much organisational knowledge resides in people's heads rather than in formal systems. The person everyone relies on to make things happen may appear insignificant from a risk perspective, yet possess a combination of access, knowledge and relationships that makes them highly consequential. What initially appears to be a series of unrelated, low-level activities can present a very different picture when viewed together.

“**The investigation doesn't always uncover something deliberately hidden. Sometimes it uncovers something the organisation simply never understood about itself.**”

Steve W.

| That should raise a difficult question for organisations:

What would an investigation reveal about how your organisation *actually operates* that your current controls, reporting and risk assessments don't show you today?

Takeaway: Visibility isn't simply about how much information an organisation collects. It is also about whether that information enables the organisation to understand how access, relationships, knowledge and capability come together in practice.

05 WHEN CAPABILITY BECOMES CONSEQUENCE

Consider a recent case from the United States involving multiple elite law firms.

At the centre was not a senior partner or executive, but an individual working within the professional services layer, with access to sensitive merger and acquisition information.

Over time, this access allowed the individual to view confidential deal information ahead of market announcements. The access itself was considered routine for the role. It fell within expected permissions and attracted little scrutiny.

It was later uncovered that the individual had been exploiting that access to share information externally as part of a wider insider trading scheme spanning several organisations.

What makes the case particularly relevant is that the individual was not inherently high-risk because of their position. They became significant because of the combination of access, knowledge, trust and low visibility.



“The important distinction is between where someone sits within an organisation and what they are capable of doing from where they sit.”

Steve W.

The issue wasn't simply that the individual had access. That access was accompanied by knowledge of what was valuable, an understanding of how the organisation's systems worked, and the ability to operate within legitimate processes without attracting attention.

Viewed individually, the activity could appear entirely normal. Viewed collectively, it presented a very different picture.

For insider threat practitioners, there is a broader lesson here. We should not only ask who has privileged access. We should also ask who has consequential capability.

Access is one component. Capability can emerge from the combination of access, knowledge, relationships, motivation and the ability to operate undetected. Many of those characteristics will never be obvious from a job title, organisational chart or conventional risk assessment.

Consider your
own organisation:

**Who could materially affect it
while appearing to be doing
no more than their job?**

Takeaway: The people capable of causing significant harm may not appear powerful or high-risk. Sometimes the capability lies quietly within legitimate access, trusted relationships and everyday activity.



CONCLUSION

LOOKING BEYOND POSITION

This is not an argument that organisations are inherently vulnerable or that individuals should be viewed with suspicion.

Hierarchy and authority still matter. Senior leaders, privileged users and others in positions of significant responsibility can have considerable influence over an organisation.

But they are only part of the picture.

Having worked in investigations and intelligence, the one thing I would like leaders and insider threat practitioners to rethink is where they look for risk.

We naturally look to senior people, privileged roles and those who appear influential. But investigations repeatedly show that consequences do not always follow hierarchy. They can rest with the person who has the right access, knowledge, relationships and opportunity, often without the organisation or even the individual themselves fully appreciating how consequential their position has become.

So rather than looking only at someone's title, position or current level of access, there is a much simpler question organisations should ask:

**What could this
person actually do
from where they sit?**

About The Author



Steve Wright is an intelligence and organisational risk practitioner with more than 20 years' experience across defence, national security, financial crime and operational leadership. A former Royal Navy Healthcare and Intelligence professional, Steve has worked in counterintelligence, human intelligence, geospatial intelligence and insider threat environments, including roles focused on identifying and assessing individuals' access, capability and intent.

His experience spans both government and private-sector environments, giving him a practical perspective on how organisational risk manifests beyond formal structures, policies and reporting lines. He is particularly interested in the intersection of access, capability, influence and human behaviour, and in challenging assumptions about where meaningful organisational power and risk actually reside.

Steve currently works in a healthcare leadership role and has previously led financial crime teams in the banking sector financial having previously held senior operational and intelligence roles within UK Defence. His work focuses on translating intelligence and risk principles into practical approaches that organisations can use to better understand their exposure to people who may possess the capability to materially influence outcomes - whether intentionally or otherwise.

Contact Us

 www.insiderthreats.au

 hello@insiderthreats.com.au

 +61 2 6198 3381