McGrathNicol

Risk and Security Report 2025 —

CONTENTS

Building resilience against interconnected threats

The intensifying risk and security threat landscape demands a fundamental shift from siloed approaches to integrated risk management.

Australian business leaders face a critical gap between security risk awareness and organisational capability. The fragmenting geopolitical landscape amplifies security challenges. Threats are transcending traditional boundaries and spreading across organisational networks. As threat actors adopt more advanced, AI enabled tactics, organisations must address the interconnected nature of security risks.

In partnership with YouGov, McGrathNicol's third annual Risk and Security survey shows that cyber threats continue to dominate executive concerns. Over two thirds of respondents (67%) rank cyber risks among their top five business challenges and almost half (49%) expect cyber risks to increase in severity over the next 12 months. Organisations are up against sophisticated AI-powered attacks and "living-off-the-land" techniques that bypass traditional defences.

For the first time, geopolitical risks have emerged as a top five concern for executives, with 80% of organisations anticipating that geopolitics could pose a risk to their operations. Meanwhile, traditional financial risks are also increasing, including supply side costs, price volatility and resource scarcity.

Despite overall confidence in their ability to navigate supply chain issues (91%), critical vulnerabilities are still being overlooked. Findings show that most organisations (82%) are not conducting risk assessments beyond their first-tier suppliers.

How to respond

Organisations must transition to more proactive and integrated risk management beyond simple compliance.

Supplier criticality matrices, now a requirement for organisations in the financial services sector under APRA CPS 230, can extend due diligence beyond first-tier relationships and strengthen both cyber resilience and insider risk management through advanced threat detection.

Domestic and global regulations are also mandating increased security, supply chain due diligence, and risk obligations.

Genuine resilience requires comprehensive programs that identify and address the interconnected nature of geopolitical risks, cyber threats, the operational environment, supply chains, and counterparty relationships.

This study was conducted online between 30 March and 4 April 2025 by YouGov. The study targeted C-Suites and Board-level Directors and Managers in Australian businesses with 50+ employees across all industries including financial services, technology, manufacturing, health care and pharmaceuticals, and transport and logistics. The sample is comprised of 335 respondents. The findings have been weighted by industry and location, and the sample is representative of the approximately 86,000 Australian organisations with 50+ employees.

Matt Fehon AM
Head of Advisory, McGrathNicol

AT A GLANCE

Balancing innovation and risk

Increased regulatory efforts are having the desired effect

A comprehensive risk management program includes identification of potential risks, actions taken to mitigate such risks, and crisis planning for scenarios likely to undermine an organisation's ability to respond and recover. Encouragingly, 82% of respondents say they have a holistic security risk management plan, due in part to regulatory changes.

- Most Australian organisations (90%) have established a single accountable authority to oversee security risk management
- Greater executive visibility and support is being achieved, with 57% of security leaders reporting to the CEO.

Warning signs persist, pointing to a lack of connected thinking

Business leaders remain focused on enhancing their cyber detection and response capabilities. However, in doing so, they are neglecting other areas vulnerable to cyber risk, such as supply chain and counterparty security.

- Critical vulnerabilities are being overlooked, with 70% of organisations failing to conduct due diligence on key suppliers.
- When it comes to performance and supplier evaluations, 71% of organisations are not considering their suppliers' own security as a key metric.

Elevating resilience must be a board and executive priority

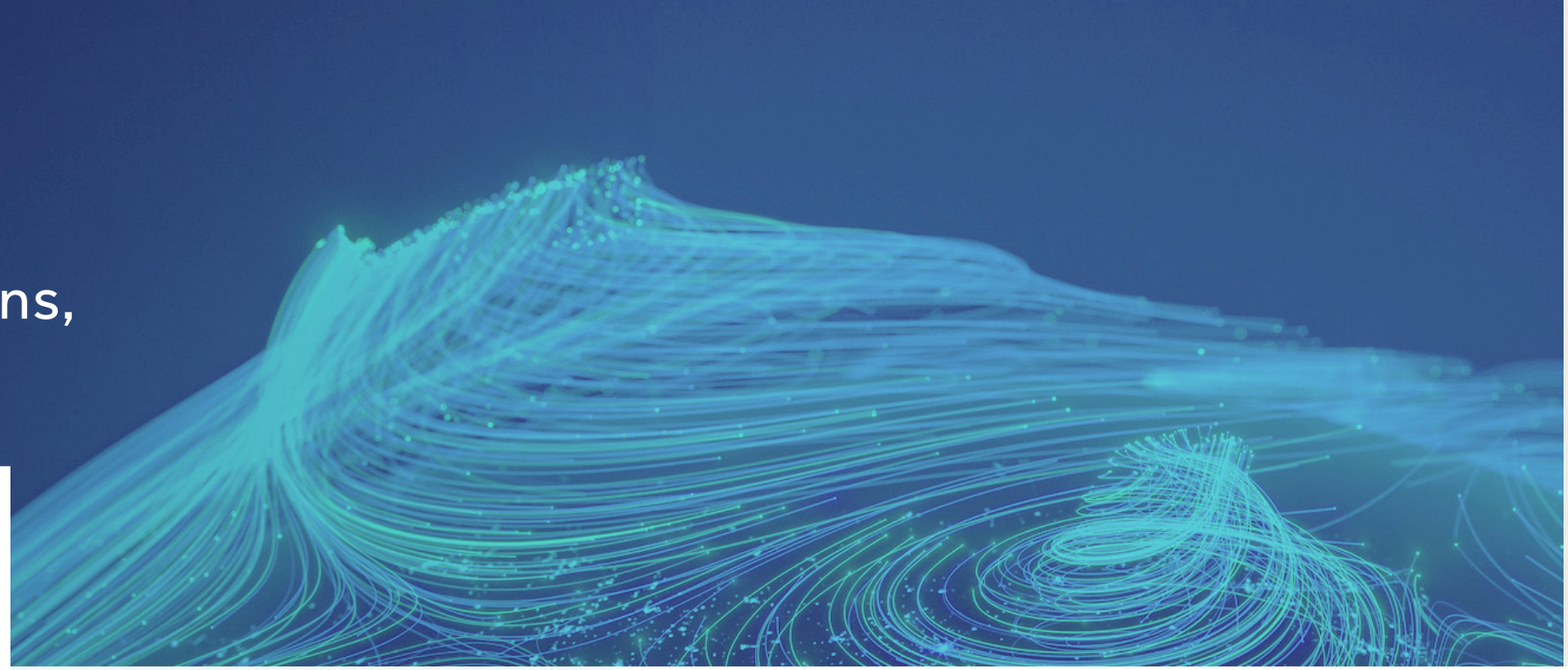
There is a continuing need to enhance and improve preparedness through integrated security and risk management. Business leaders can look to industries such as Financial Services and consider implementing similar best practice frameworks as those under APRA CPS 230 and the risk management recommendations under the Security of Critical Infrastructure (SOCI) Act.

- Business Continuity Plans must be continually updated and tested, with 30% of respondents saying their key executives are too busy or do not see the need to address this.

AI – a dual challenge and opportunity

Respondents recognise that AI adoption will drive business benefits but many commented on the potential for new security, governance, regulatory, ethical, and data privacy challenges.

- Forward-looking organisations are exploring AI-enabled cyber defences to strengthen their cyber capabilities, automated incident response and continuous security monitoring.
- Organisations must balance innovation with strengthening enterprise-wide risk frameworks including establishing ethical AI use guidelines, training staff in responsible AI use and taking a holistic view when reviewing security investments.



GEOPOLITICAL RISK

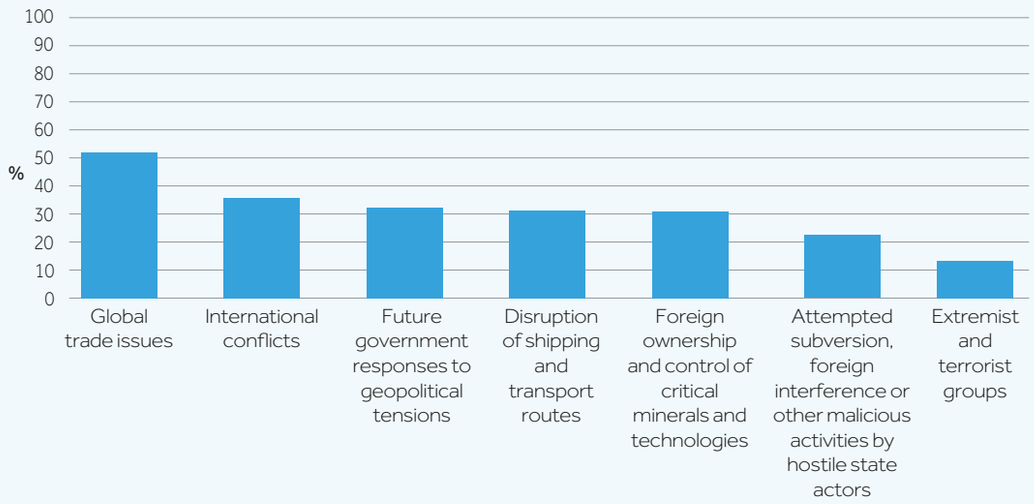
Global tensions, local impact

CRITICAL TREND

80% of business leaders

believe geopolitical issues will pose a challenge to their organisation and supply chain over the next 12 months.

Which of the following will pose a challenge to your organisation and supply chain over the next 12 months?



Australian organisations are aware of the complex realities of geopolitical risk, but significant gaps remain between awareness and preparedness. The changing global ecosystem is requiring businesses to have a more sophisticated understanding of how international tensions can quickly translate into domestic issues.

While 80% of organisations expect geopolitical issues to pose challenges to their operations and supply chains over the next twelve months—up from 66% in 2024—this awareness is unevenly distributed. Financial services organisations are showing heightened vigilance, with 40% expecting geopolitical risks to increase in severity over the next 12 months. In contrast, healthcare executives appear less concerned, with only 11% anticipating an increase in severity. It is important to note the Australian healthcare sector is particularly vulnerable to nation-state cyber threats targeting valuable personal information like patient data, research and intellectual property.

Surprisingly, concerns about foreign interference have only risen from 19% to 22% year-over-year. The modest increase suggests that many organisations view foreign interference as primarily a government concern rather than a commercial risk. This is despite ASIO's warning that foreign interference will escalate beyond its current "extreme" rating in 2025.

The Federal Government faces a delicate balancing act between upholding our critical security relationships with the United States and United Kingdom, as well as economic ties with China. A third of executives (33%)—up from 20% in 2024—indicate that responses from Federal and State Governments to geopolitical tensions may create challenges for their organisation in the future.

How to respond

The secondary impacts of geopolitical tensions can often prove more disruptive than the primary effects, and preparation requires sound risk modelling and scenario planning.

Organisations must move beyond reactive monitoring to proactive risk management, integrating geopolitical considerations into strategic plans, supplier evaluations, and operational resilience frameworks.

CYBER RISK

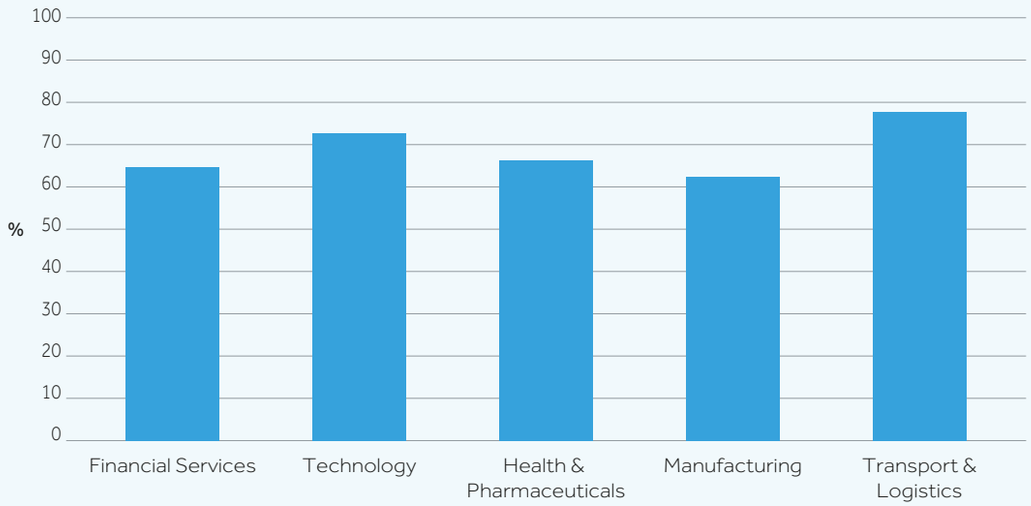
Beyond your organisation's perimeter

CRITICAL TREND

67% of business leaders

now rank cyber risk among their top five business challenges, with 24% identifying cyber as their most pressing concern.

Which industry sector identifies cyber security as the greatest current risk to their organisation and supply chain?



For the third consecutive year, cyber risk dominates executive concerns—67% rank it among their top five challenges and 24% identify it as their most pressing concern. Further, 49% expect increased cyber security challenges in the year ahead—up from just 16% in 2023. This sharp rise reflects not only the persistence of cyber threats but also a broader understanding of their impacts across operations and supply chains.

As cyber defences evolve, so too do the tactics deployed by criminals. Attackers are using increasingly sophisticated techniques that bypass traditional security measures. The emergence of "living-off-the-land" techniques, where attackers use legitimate tools already present within systems, represents a fundamental shift in attack methodology.

Supply chain compromises have become a particular area of concern, as cyber criminals realise the benefits of targeting one supplier to simultaneously gain access to multiple organisations. This "one-to-many" attack strategy is highly effective and has prompted organisations to reconsider their approach to third-party supplier security assessments.

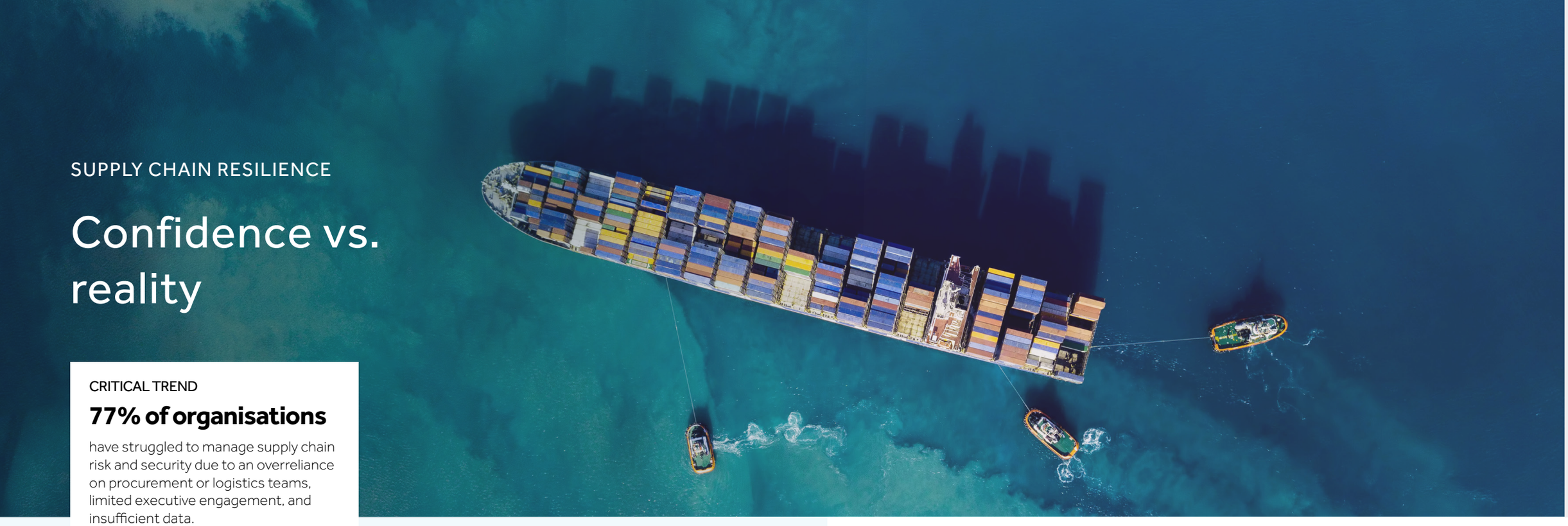
Artificial Intelligence is also being integrated in both attack and defence strategies. While AI offers powerful capabilities for enhancing security operations, it also allows cyber criminals to cross language barriers more effectively and carry out sophisticated, targeted attacks.

How to respond

Forward-looking organisations should begin laying the groundwork, updating governance frameworks, training staff on responsible AI use, and exploring AI-enabled cyber defence strategies.

The regulatory environment impacting cyber security continues to evolve, with new standards such as CPS 230 establishing more stringent requirements for operational risk management in financial services. These regulations emphasise the need for organisations to extend their risk management practices to include cyber risk that encompasses third party suppliers and service providers in other jurisdictions.

Organisations must urgently develop comprehensive incident response capabilities and business continuity plans that address the full spectrum of cyber threats.



SUPPLY CHAIN RESILIENCE

Confidence vs. reality

CRITICAL TREND

77% of organisations

have struggled to manage supply chain risk and security due to an overreliance on procurement or logistics teams, limited executive engagement, and insufficient data.

Organisations continue to rely too heavily on suppliers to manage risk, and are failing to implement good practice due diligence measures.

70% OF ORGANISATIONS

do not conduct operational or cybersecurity due diligence on key suppliers.

82% OF ORGANISATIONS

do not extend risk assessments to 2nd, 3rd or 4th-tier suppliers.

63% OF ORGANISATIONS

do not use a criticality matrix to prioritise their key suppliers.

71% OF ORGANISATIONS

do not consider supply chain security alongside cost and performance in supplier evaluations.

Despite overall confidence in their ability to navigate future supply chain issues (91%), only 37% of business leaders report being "very confident"—down from 53% in 2023. Meanwhile, those now answering "somewhat confident" has steadily increased in the same period, from 44% to 54%. Some of the reasons for this diminishing confidence include:

- Geopolitical risk responses identify disruption fears linked to shipping and transport (more than doubled from 14% in 2023 to 32% in 2025) alongside a rise in global trade concerns (up from 30% to 53%).
- Continued over-reliance on suppliers to manage risk, with critical assurance and due diligence measures often missing. A lack of visibility beyond first-tier suppliers presents another critical vulnerability, with 82% of organisations failing to extend risk assessments to second, third, or fourth-tier critical suppliers.
- 77% of organisations have faced recent challenges managing supply chain risk and security. This has been mostly due to misplaced confidence in procurement or logistics teams, executive disengagement, and a lack of data to quantify the financial impact.

Counterparties may not provide goods or services but often play strategic roles as investors, finance providers, trusted advisers, joint venture partners, international distributors, or research collaborators. Increased recognition of broader supply chain partner roles in risk management and data protection has seen 32% of respondents ranking counterparty risk among their top five concerns.

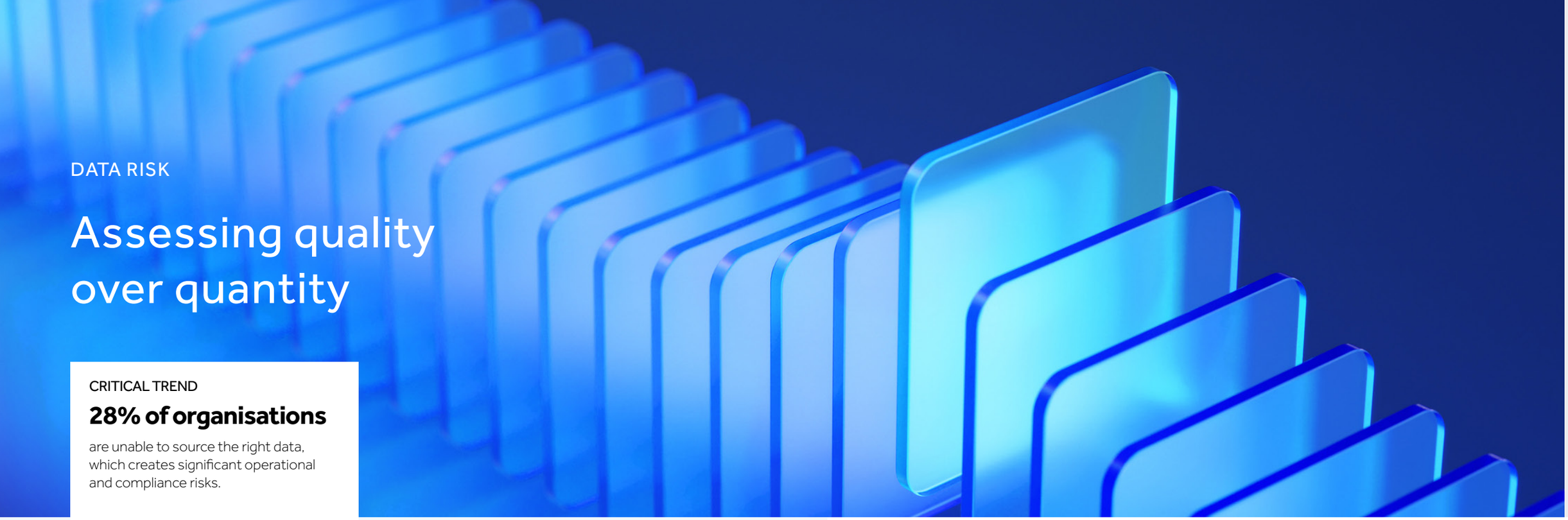
Despite the potential for significant strategic, financial, and reputational risks, the level of due diligence on counterparties is not typically covered under traditional qualification processes used for suppliers and service providers.

How to respond

Enhanced due diligence should provide greater transparency on ownership, affiliations, jurisdictional exposure to sanctions, or legal compliance.

By default, counterparty access to critical or sensitive assets necessitates the requirement to embed counterparties into enterprise risk management frameworks and associated controls.

The strength of a supply chain is dependent on its weakest link – one that may lack visibility and appropriate oversight.



DATA RISK

Assessing quality over quantity

CRITICAL TREND

28% of organisations

are unable to source the right data, which creates significant operational and compliance risks.

> "Data is a critical asset to our organisation. Protecting and safeguarding it is our top priority. It allows us to stay informed and agile, helping to maintain our position as a leader in the industry. By addressing the root of the problem, we strengthen our overall security posture."

Respondent Quote

The McGrathNicol survey reveals that cyber is the number one risk identified by executives. This risk is commonly associated with data being stolen, compromised or misused by threat actors. The survey also revealed many organisations struggle with fundamental questions about what data they possess, the quality of that information, as well as its ability to support risk discussion and business operations. There is often little connection between the volume of data being maintained and its actual strategic value. This disconnect between quality and incompleteness of data can create significant operational, regulatory and compliance risks.

For the third consecutive year, over 25% of organisations are unable to source the right data, meaning limited transparency of supply chain operations and an inability to quantify risks, such as data security.

As organisations enhance their cybersecurity and explore artificial intelligence capabilities, the requirement for high-quality, secure data becomes even more critical. AI systems are only as effective as the data they process, making data quality a fundamental prerequisite for successful AI adoption.

The ability to respond to regulatory requirements also depends on access to the right information in the appropriate format. Organisations that can facilitate accurate information exchange with regulators foster positive regulatory relationships and reduce compliance costs. Conversely, the time and expense required to compile data from disparate, or incomplete, sources can pose a significant operational burden.

How to respond

Organisations should assess data quality issues by examining how long it takes to meet data requests within their business and how many people must be consulted along the way. Extended timeframes and the involvement of too many stakeholders can point to underlying quality and accessibility problems.

INSIDER RISK

Security from the inside

CRITICAL TREND

70% of organisations

do not have a nominated executive or accountable authority responsible for managing insider risk.

"With over 60% of organisations still lacking fundamental controls, executives are urged to implement a robust insider risk framework to identify and mitigate potential threats."

Sara Deady, Partner
McGrathNicol

Organisations are struggling with the implementation and maintenance of an effective insider risk management program. In 2025, only 53% of respondents report having well-understood, comprehensive insider risk management programs in place—down from 71% in 2024. The complexity of insider risk, which encompasses both malicious and inadvertent actions by employees, contractors, and other trusted individuals, requires a coordinated approach.

The threat is complex and evolving, as it can directly increase your cyber risk. Organisations are facing significant technology and data challenges. At the same time, employees working in hybrid and remote roles, or those under significant cost of living pressure, have contributed to a marked rise in external threat actors leveraging insiders to exploit security weaknesses.

These issues have added new dimensions to insider risk management, creating challenges and opportunities around endpoint security, data access controls, and behavioural monitoring. There is a complex trade-off for organisations between productivity and profitability while still ensuring insider threats are detected, monitored and mitigated against.

The survey highlights several key vulnerabilities, including inadequate access controls and limited monitoring of privileged user activities.

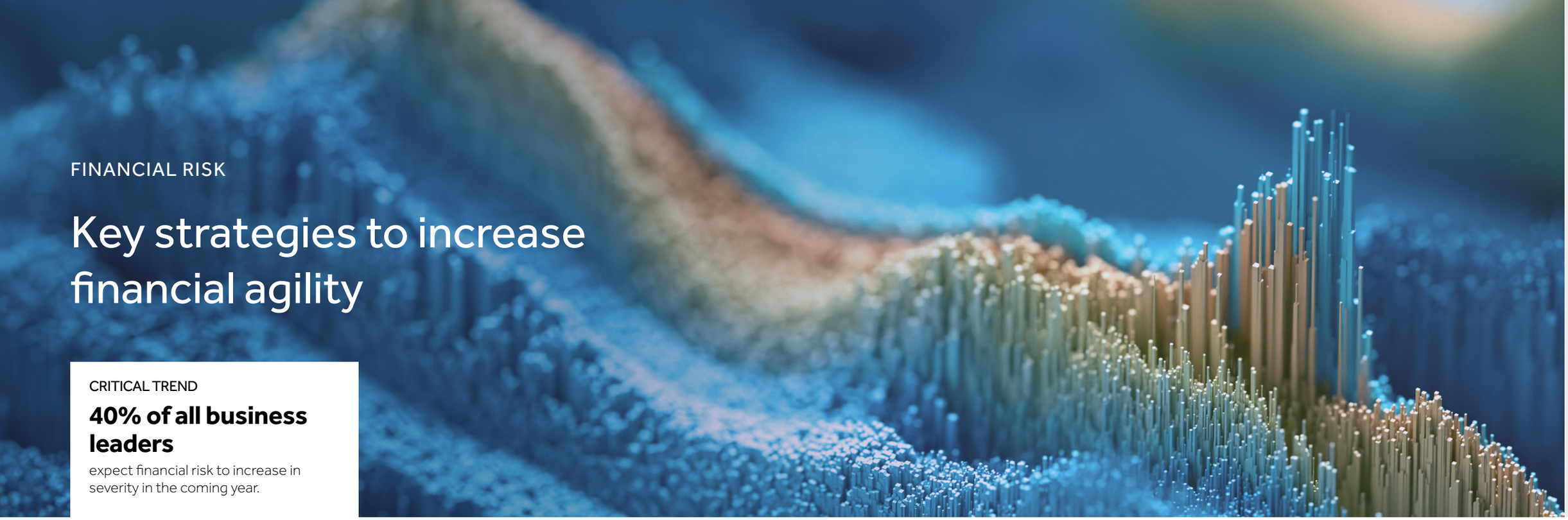
Insufficient education for employees also undermines work to recognise and respond to insider risks such as fraud, corruption, scams, foreign interference and cyber-attacks. Weak onboarding and offboarding processes for employees with access to critical information and systems further introduces vulnerabilities to be exploited.

Positively, the research finds that 89% of organisations are planning to implement practices to better understand and mitigate insider risks, with education and technology investment key elements of their new programs.

How to respond

A best practice insider risk management program should include:

- An assessment program to identify risks and vulnerabilities, and robust identity and access management systems to align user access with critical roles and risk tolerances.
- A comprehensive security awareness program to educate and empower employees to understand threats and their own role in protecting the business.
- Establishing clear incident response protocols is also essential to detect and respond to insider threats.



FINANCIAL RISK

Key strategies to increase financial agility

CRITICAL TREND

40% of all business leaders

expect financial risk to increase in severity in the coming year.

In the year ahead, the following respondents expect financial risk to increase in severity:

51% OF ORGANISATIONS

in the Financial Services industry

34% OF ORGANISATIONS

in the Transport/Logistics industry

42% OF ORGANISATIONS

in the Manufacturing industry

35% OF ORGANISATIONS

in the Technology industry

30% OF ORGANISATIONS

in the Health/Pharmaceutical industry

As financial risks intensify, Chief Financial Officers face unprecedented challenges. With 60% of organisations ranking financial risk among their top five concerns and 40% expecting greater financial risks in the coming year, CFOs must adopt proactive strategies to address both traditional financial pressures and emerging security-related threats.

Current financial uncertainty stems from a complex range of domestic and international factors including market and price volatility, trade and tariff concerns, inflation, cost of living pressures, and resources scarcity. Traditional financial risks are being compounded by broader security concerns, including international conflicts that can quickly result in operational and financial challenges.

Market dynamics are evolving at pace. This makes it increasingly difficult for organisations to adapt operations quickly, while maintaining an appropriate risk profile, adhering to expanding regulatory requirements and strengthening their financial position. External factors beyond organisational control are disrupting market stability and supplier reliability, meaning that more agile financial strategies are required.

Evolving regulatory requirements, including ESG reporting, data privacy laws, and security legislation, increase compliance costs and require proactive resource allocation. Cyber security is a particular concern for CFOs and finance managers, with the potential for widespread consequences driving increased investment in protecting their most important assets.

How to respond

CFOs must strategically manage risks and improve efficiency to build financial resilience. Across people, processes, and technology, cost control can be achieved through transformation and automation.

Effective financial risk management requires clear communication between boards, executives, and stakeholders to support both organisational transformation and protection objectives.

Business cases including those required for advanced threat mitigation and cyber resilience in the face of more AI-enabled attacks must always be underpinned by sound risk analysis and supporting financial evidence.

How we help

McGrathNicol helps companies improve performance by mitigating risk, managing change and achieving growth.

Having operated within and alongside the highest levels of Government and Industry, our independent experts deploy a unique mix of capabilities to address the broad existing and emerging threats and security risks governments and organisations face.

Our team provides the expertise and strategic guidance necessary to help your organisation bridge the risk and security awareness-action gap. We work with you to identify and manage enterprise security risks and potential areas of threats. We assess and connect your security and risk frameworks, identify vulnerabilities, isolate areas to uplift risk management and defences, and pinpoint duplication and redundancy.

We specialise in developing robust frameworks, policies, systems and controls tailored to your organisation's needs, meet legislative and policy responsibilities and align with better practice including the Australian Risk Management Standards, ISO 27001, and NIST frameworks. Well-designed roadmaps and strategies can boost your security, mitigate risks, and ensure compliance with the Security of Critical Infrastructure Act 2018 (SOCI Act) legislation and evolving regulatory standards such as APRA CPS 230.

We provide you with the information, training and frameworks to make informed security decisions and manage, investigate and respond to risks against your business, people, data, reputation and interests.

Contacts

Matt Fehon AM
Partner
Head of Advisory
M +61 402 130 769
E mfehon

Sam Boarder
Partner
National Security
M +61 439 447 187
E sboarder

Emma Boucher
Partner
Performance
M +61 458 770 076
E eboucher

Sara Deady
Partner
Forensic
M +61 420 941 295
E sdeady

Matt Grant
Partner
Forensic
M +61 439 205 873
E mgrant

Alex Morkos
Partner
Cyber
M +61 400 090 074
E amorkos

Rhyan Stephens
Partner
Supply Chain
M +61 411 048 391
E rstephens

Janine Thompson
Partner
Forensic
M +61 407 555 852
E jthompson

Mark Wroniak
Partner
Cyber
M +61 448 098 204
E mwroniak