McGrathNicol

The Changing Landscape of Business Risk —

Risk and Security Report

Awareness is growing, but many businesses are unprepared for future geopolitical, insider, cyber, supply chain, regulatory, and financial threats.

Contents

The Changing Landscape of Business Risk

89 percent of surveyed executives believe risk and security issues will worsen in severity over the next 12 months up from 58 percent in 2023. Cyber security ranks as the number one current concern for businesses, followed by financial, legal and regulatory risks.

As we review the findings of our annual Risk and Security Survey, a few lessons for executives stand out. Executives face challenges in the 'changing landscape of business risk' such as geopolitical events, insider threats and cyber security issues in the supply chain. There is general awareness of these risks and yet, many are struggling to address and mitigate them.

These various risks are interlinked. Following a data breach, a cyber incident can rapidly escalate throughout the supply chain to your customers and employees, and become a regulatory data and privacy issue with financial and reputational consequences. Surprisingly, almost three quarters (72 percent) of surveyed business leaders have no intention to revisit their business continuity plans, despite the frequency and success of these cyber attacks.

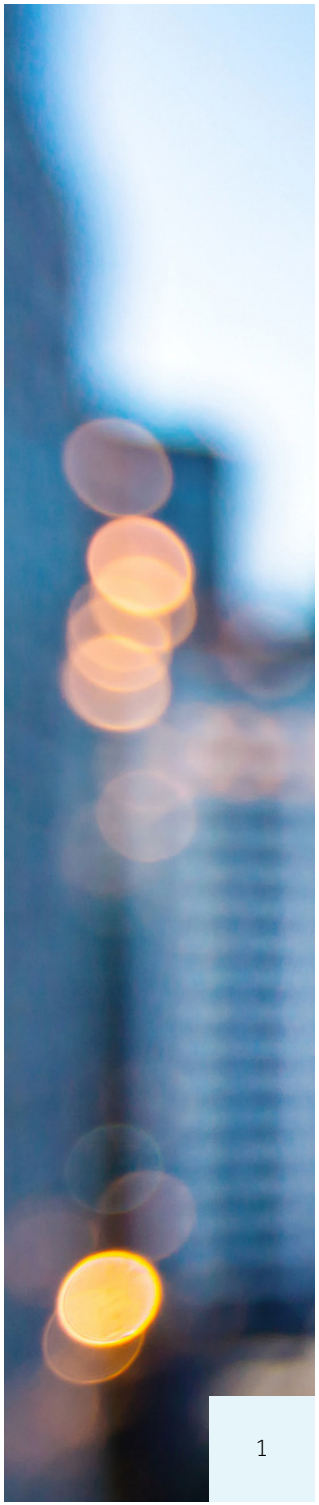
Business leaders understand the threat environment is driving these emerging risks but they struggle to comprehend and connect the dots between these complex risks. In understanding and addressing the changing landscape of business risk, executives should consider the possible 'flow-on' effects posed by geopolitical events. For example, how a regional conflict could disrupt their supply chain or the next US President could affect international trade patterns, and then map out where in their business such risk events are most likely to impact.

Despite awareness of these emerging risks, executives say they find it difficult to choose appropriate risk frameworks and ensure that these are fully integrated across their business. We repeatedly see incomplete data governance and risk management, as well as insufficient implementation of the right controls all driven by a lack of in-house risk expertise. This leaves organisations exposed and vulnerable.

These risk survey findings should serve as a wake-up call for CFOs and executives. Failure to address and prevent these risks could potentially lead to operational disruptions, financial losses, as well as new legal and regulatory penalties. To counter this, CFOs must be brought into risk conversations early on and work with their risk colleagues to assess the effectiveness and return on risk investments to date. Organisations often react once the risk occurs. This is costly and we prefer that our clients are prepared with the tools to confidently face the changing landscape of business risk head on.

Matt Fehon AM
Head of Advisory, McGrathNicol

This study was conducted online between 16 April and 1 May 2024 by YouGov. The study targeted C-Suites and Board-level Directors and Managers in Australian businesses with 50+ employees across all industries. The sample is comprised of 318 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.



Key survey findings

01. Businesses underestimating the secondary impacts of geopolitics

Despite months of chaos in the Middle East and Ukraine, and rising tensions in the South China Sea, only a quarter of organisations (25 percent) rate 'geopolitical risks' as a top 3 risk—down from 41 percent in 2023. Trade issues and disputes are a concern for more than a third of Australian organisations (37 percent), but surprisingly only 9 percent believe that the uncertain outcome of the US election will pose a significant challenge to their business.

02. Cyber concerns grow, as supply chains increasingly targeted

Cyber risk has now overtaken financial risk as the number one concern of 2024. As threat actors strategically target businesses along the supply chain, almost half of surveyed organisations (44 percent) are preparing for cyber risks and security concerns to increase in the year ahead. Alarmingly, 70 percent of organisations surveyed do not have basic controls in place to manage cyber risks in their supply chain including contractual obligations that require mandatory reporting by suppliers of any cyber or data breaches.

03. Insider risk is a 'human' problem

While many organisations are required to possess an insider risk management program under new Security of Critical Infrastructure (SOCI) legislation, no more than a third (ranging from 18 to 34 percent) of surveyed organisations have the basic insider risk controls in place that McGrathNicol would consider fundamental. These include risk-based vetting and due diligence frameworks for employees, suppliers and contractors.

04. Practical testing of supply chains is required

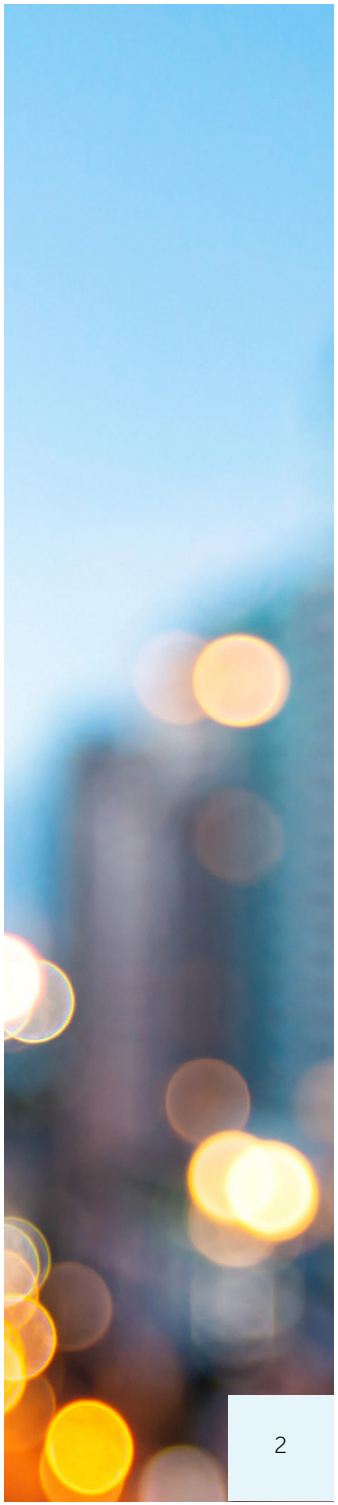
Awareness of supply chain risk is growing, with 80 percent of surveyed organisations now incorporating some element of supply chain risk into their broader risk management program (up from 26 percent in our 2023 survey). While nearly all organisations (96 percent) are confident in their ability to navigate risks and security issues impacting the supply chain, 74 percent continue to face internal challenges addressing supply chain risk including a lack of expertise, insufficient data, budgetary constraints, and limited access to tools.

05. Data management adds new layers of legal and regulatory complexity

More than half of all surveyed organisations (55 percent) rank legal and regulatory risks as a 'top five' concern, with 27 percent believing that these risks will increase in severity over the next 12 months. Data management, retention and privacy changes are posing significant challenges for business leaders, as regulators like the OAIC take a more proactive stance. Organisations must ensure they have good quality data to allow them to better understand compliance issues, and in the event of a dispute, defend or remediate appropriately.

06. Multiple risk factors fuel financial pressure

High inflation, wage increases, interest rate rises, and higher energy costs mean that the spotlight is on the CFO to identify areas where costs can be reduced. Newer categories of risk as well as their organisation-wide impacts will require CFOs to upskill, learn to interrogate risk investments in areas outside of their expertise, and recognise the intrinsic link between risk management and cost management.



01. Businesses underestimating the secondary impacts of geopolitics

Despite a geopolitical environment which has grown more contested and hostile in the last year, Australian businesses are perceiving fewer short-term impacts from geopolitical threats.

This is likely because Australia's 'China reset' agenda has led to the lifting of onerous trade bans, and as the shock regarding the wars between Russia-Ukraine and Israel-Hamas starts to wane. However, in our assessment the likelihood of further disruptive geopolitical events impacting risk categories that affect Australian organisations remains high.

While short-term impacts to Australian businesses may have declined, our survey results show that some are likely failing to identify and prepare for future geopolitical shocks to their organisation. Australian businesses' concerns about geopolitical risk have almost halved since last year's survey. In 2023, 41 percent of survey respondents rated geopolitical risk as a top three concern. By 2024, this number had dropped to 25 percent. Amongst small businesses, the decline is even starker: 42 percent do not believe that geopolitical risk will pose a significant challenge over the next 12 months, almost four times higher than last year's 11 percent.

Businesses are struggling to identify the link between geopolitics and other enterprise risk, such as cyber, insider and supply chain threats. This is despite the Russian invasion of Ukraine and Israel-Hamas war clearly illustrating how geopolitical events can create significant overnight risks. These are more overt threats, however, it is the cyber, insider and security threats that are 'covert' and often missed.

Political events are also a leading risk indicator. For example, 37 percent of Australian organisations are concerned about the impact of global trade issues and disputes over the next 12 months—led by the agriculture industry at 63 percent. Despite this, only 9 percent of organisations are concerned or preparing for changes following the November 2024 US election. If re-elected, a second Trump administration has proposed the introduction of new tariffs targeting Chinese-made goods of between 60-100 percent. This would almost certainly reinvigorate trade disputes and directly impact Australian businesses. Looking ahead, global strategic competition will continue to create tension along existing geopolitical fault lines.

"Organisations that identify their geopolitical risk exposure and track key indicators will significantly reduce their chances of being blindsided by tomorrow's election outcome, trade dispute or regional conflict."

Sam Boarder
Partner

02. Cyber concerns grow, as supply chains increasingly targeted

Cyber security is top of mind for Australian businesses, with 68 percent of organisations placing cyber risk within their top five concerns for 2024—the highest of any risk category.

This data is supported by the fact that threat actors are becoming more sophisticated and are increasingly targeting an organisation's extended supply chain to devastating effect. Organisations are correctly identifying that cyber risk is shifting further along their supply chains. The majority (80 percent) of surveyed organisations have implemented at least one measure to mitigate supply chain risk. McGrathNicol identified that there is still a significant gap in third-party and supplier security assessments, however.

According to detailed survey responses, organisations are not carrying out risk assessments to assess, address and prioritise critical assets, systems, data, or processes being operated, managed and accessed by their suppliers. Additionally, 70 percent of Australian organisations are not conducting due diligence checks on critical personnel of their suppliers who have access to their facilities, systems, data and people. Most surprising is that 70 percent of surveyed organisations do not have basic controls in place to manage cyber security risk in their supply chains, including mandatory reporting by suppliers when they have been breached. These findings highlight an urgent need to apply a more comprehensive approach to risk management in the supply chain.

Of particular concern is that 20 percent of the respondents within Healthcare & Pharmaceuticals and IT industries either do not believe third-party security assessments are applicable, do not consider that those in their supply chain pose a risk, or believe the onus is on their suppliers to address and manage these risks. Given the recent targeting of healthcare services and providers globally, these survey results indicate that too many organisations are underestimating security threats and controls within these industries.

"Cyber has overtaken financial risk as the primary concern for Australian organisations. These findings highlight an urgent need to do more to manage cyber risks in the supply chain."

Blare Sutton
Partner

03. Insider risk is a ‘human’ problem

The Risk and Security Survey suggests that businesses are unlikely to have considered the appropriateness of their existing insider risk management measures in the context of heightened insider risk and an increasingly insider risk-focused set of regulatory frameworks.

As Australia's threat environment has deteriorated over recent years, regulatory requirements have expanded to try to harden business and government to an increasingly challenging economic and geopolitical environment in which we see more companies experiencing and reporting malicious insider threat incidents – year on year. Yet surprisingly businesses are still not connecting the dots between cyber and insider risk even though our survey results show that Cyber is the number one risk for executives. In cyber attacks, there is always a person behind the keyboard.

Despite these shifts, less than half of surveyed businesses (46 percent) rated insider risk as a top five risk. Most businesses face two distinct hurdles when it comes to managing insider risk: siloes of relevant information and a lack of awareness of potential insider mitigations. While 87 percent of organisations surveyed were confident that their business has a comprehensive insider risk management program in place, less than a third of businesses have implemented some of the most fundamental insider risk controls – with only 28 percent using a risk-based vetting and due diligence framework for employees and suppliers or contractors; 27 percent having some form of education and awareness program; and just 18 percent appointing an authority that is accountable for insider risk. Crucially, 82 percent of surveyed organisations identify that they are covered under the federal Security of Critical Infrastructure Act 2018 (the SOCI Act), which requires Critical Infrastructure assets to maintain a Risk Management Program (CIRMP) incorporating insider risk protections. This requirement also applies to the management of supply chains, and therefore flows to numerous supporting industries.

In our experience, organisations that proactively consider insider risk will achieve distinct commercial advantages over those reacting to an insider incident after it has occurred.

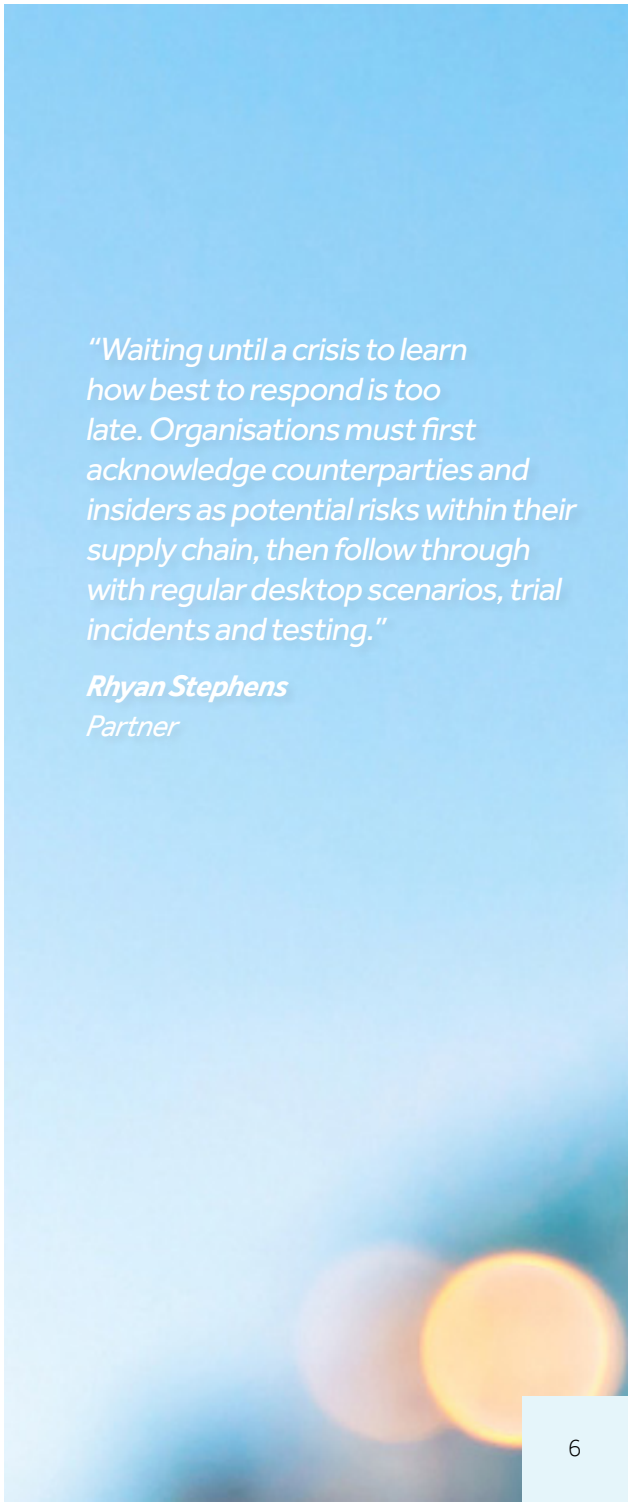
04. Practical testing of supply chains is required

The Risk and Security Survey shows that most enterprise risk management programs (80 percent) now include supply chain risk as a core pillar.

This is a positive finding and reconfirms the criticality of proactive assessment of all facets of supply chain interactions and associated engagement with third parties. Supply chain risk continues to intensify, linked primarily to the risk of foreign ownership of suppliers, continued skilled labour shortages, escalating geopolitical situations impacting material flows, emergence of more sophisticated third-party cyber attacks, and ongoing trade defragmentation affected by consumer sentiment, increased protectionism, and the resultant repositioning of supply sources. Senior executives cannot afford to be complacent or neglect supply chain risk management activities in the year ahead.

Similar to last year's survey results, most organisations (74 percent) acknowledge internal issues in addressing supply chain challenges due to a shortage of expertise, insufficient data and visibility tools, budgetary constraints, and competing priorities. The detailed plans, skills, technology adoption, supplier assurance programs, and controls uplift needed to identify and address supply chain risks remain under-prioritised. Compounding these issues, there is a troublingly low number of respondents that are focusing on insider (7 percent), counterparty (6 percent) and ESG (8 percent) risks, and the potential effect these might have on their operations.

Supply chain challenges are broad ranging and can therefore have significant impacts and flow-on effects during a crisis. A lack of comprehensive business continuity planning (BCP) and proactive scenario workshops can lead to unpreparedness when responding to payroll issues, technology and data interruptions, operational delays and KPI failures, client satisfaction and reputation issues, contract termination, supplier liquidity or default concerns, and safety issues, among others. There is often lethargy or denial until an incident occurs, but it is this lack of documented accountability and activities that recent legislative changes (i.e. SOCI obligations and mandatory ESG reporting) are trying to prevent. Practical, robust and ongoing testing and monitoring of supply chains is recommended and is now expected by more businesses and regulators.



"Waiting until a crisis to learn how best to respond is too late. Organisations must first acknowledge counterparties and insiders as potential risks within their supply chain, then follow through with regular desktop scenarios, trial incidents and testing."

Rhyan Stephens
Partner

05. Data management adds new layers of legal and regulatory complexity

More than half of surveyed business leaders (55 percent) see legal and regulatory risk as a top concern for their organisation and 27 percent believe these risks will increase in severity.

The regulatory landscape is complex. In the past few years, legislation has been introduced with regards to payment times reporting, wage underpayments, changes to the Privacy Act and the SOCI Act (to name a few). Regulatory bodies have notably shifted focus from market education and awareness to enforcement.

Legal and regulatory risks related to data retention and privacy are posing significant challenges as our survey respondents noted. Recent examples include the Australian Communications and Media Authority's legal action against Optus and the OAIC's action against Medibank—both concerning data breaches in 2022. Considerable corporate governance implications for Directors have emerged, with the headline penalty currently sitting at $21 billion. In reality though, the civil penalty will likely run in the hundreds of millions. Privacy Act amendments this year will create further obligations relating to Board accountability, cyber security compliance and the governance of data.

The Board's role is to understand the threat environment, set the risk appetite, allocate adequate resources, and monitor the development, maintenance, and implementation of suitable processes for risk management. Executives need to be aware of their duty to take reasonable care and protect their organisation from foreseeable risk of harm too, including effective oversight of a compliance and data risk-management framework. Concerns about data are justified, but the focus must extend beyond security and retention to understand what data is being used and why. Executives must ensure they have good quality data to allow them to better understand compliance issues and in the event of a dispute, defend or remediate appropriately. Whilst data is valuable, it can be a liability if not protected.

"Changes in laws may impact how my organisation must handle and protect users' personal data, which may lead to increased legal obligations and costs."

- Survey respondent

06. Multiple risk factors fuel financial pressure

High inflation, wage increases, interest rate rises, and higher energy costs mean that the spotlight is firmly fixed on the CFO to identify areas where costs can be cut.

Many organisations are already making cuts to discretionary spending and this trend is expected to continue into 2025. Many will also identify and assess efficiency initiatives to help free up capacity, redirect resources to more valuable activities, and ultimately, reduce costs. Both approaches will help CFOs to determine if, and how, things can be done for less across their organisation.

McGrathNicol's Risk and Security Survey found that nine in ten organisations (89 percent) believe that risk and security issues will increase in severity over the next 12 months (up from 58 percent last year). Whilst cyber risk was the highest-ranking risk among organisations surveyed, financial risk ranked second, with 66 percent of surveyed organisations categorising it as a top five risk.

The balancing act for CFOs is in shielding their organisation from an increasing number of risks whilst sufficiently cutting costs to preserve earnings. For instance, where investment is required for new technology and automation processes to strengthen the organisation's resilience against cybersecurity and other related risks, the CFO must develop new capabilities to be able to effectively work with, and at times challenge, the CTO and CRO on the validity of project expenses. Additionally, expected returns on investment for both soft and hard costs should be established before implementing any new risk management solution. Managing security risks is becoming more complex and costly, ensuring you have the right systems is critical.

.

Contacts

The McGrathNicol team works collaboratively to identify potential areas of threats and hazards, mitigate vulnerabilities and risks, and develop strategies that drive competitive advantage.

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

Matt has more than 30 years investigative and consulting experience, dealing with a diverse range of assignments, clients and people. In identifying emerging issues and risks, Matt assists clients to combat geopolitical threats, cyber, financial crime and foreign interference.

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

Sam is an experienced forensic expert with a background in security threat investigations and vulnerability assessments. He has led a range of complex investigations into counter terrorism, insider threat, espionage, and foreign interference – in partnership with domestic and international law enforcement and intelligence agencies.

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

Sara specialises in financial crime and regulatory investigations, funds and asset tracing and proactive fraud and corruption risk management. With more than 15 years of dedicated forensic experience, Sara has led a number of Australia's highest profile civil and criminal investigations across a broad range of industries.

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

Rhyan has managed large scale supply chains and industrial businesses in Australia and internationally, for over 25 years. He specialises in strategic transformation, supply chain network development, operational execution, risk management, technology adoption, governance & compliance, market entry, and deals.

Blare Sutton
Partner
Cyber
M +61 417 252 739
E bsutton

Blare is a highly regarded forensic expert with more than 20 years of experience in technology and cyber. He manages highly sensitive engagements involving internal and external actors, law enforcement, financial institutions and civil remedies.

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

Janine has over 20 years of experience and is skilled in dispute advisory and forensic assignments, including the preparation of consulting and independent expert reports in legal proceedings, and interaction with key stakeholders such as lawyers, management, regulators and law enforcement.

Sean Wiles
Partner
Strategy & Performance
M +61 437 097 180
E swiles

Sean delivers insightful advice to improve operational and financial performance. He works with clients across a range of industries including construction and engineering, food, beverage and agriculture, transport and logistics, manufacturing, and education, to help them manage risks and challenges and adapt to change.