McGrathNicol

Uncovering Risks in the Supply Chain

Businesses are overconfident when anticipating their readiness to respond to operational, geopolitical, and cyber risks in their internal and external supply chain.

2023 Survey — In Partnership with YouGov Australia

Contents

The threats facing businesses of all sizes

Australians became aware of the importance of global supply chains during the COVID period. Businesses used to running 'just in time' logistics and selecting from a global pool of services suddenly found themselves pushed down the priority list and reacting to global events.

Today, our economy is more interdependent than ever before, and our supply chains are just as fragile. Most Australian businesses work with a vast network of customers and suppliers which, as we navigate challenging economic times at home and a fractious geopolitical environment abroad, are expected to come under increasing strain.

While many business leaders may consider the impact of geopolitical issues, natural disasters, cyber attacks, regulatory changes, monetary policy or labour unrest in isolation, the most effective leaders are those that address and plan for these risks, and many others, holistically. They are the leaders who think five steps ahead, bake supply chain resilience into their risk management plans, allocate experienced resources, and are poised to take advantage of new opportunities, when their competitors haven't.

To investigate current awareness of the risks that threaten our supply chains, McGrathNicol has partnered with YouGov to survey 300 Australian Directors and C-Suite leaders across multiple industries on the risks they are concerned about, their risk management processes, and the barriers they face in addressing supply chain threats. A key takeaway is that, despite the events of recent years, business leaders are confident that they can manage future risks to their supply chains but are perhaps underestimating or do not fully comprehend the real nature of these threats. Companies and their Boards must interrogate the steps their organisation has taken to understand, and mitigate, the many elements of risk that make up a modern supply chain.

Over the past six years, we have helped executives to enhance security, optimisation and resilience across all aspects of their supply chain. We hope you find the following pages informative.

Matt Fehon
Partner, Head of Advisory

92%

of business leaders are aware that the SOCI Act 2018 (Cth) requires organisations to develop a risk management plan.

27%

of businesses have failed to update their risk management plans in the past two years.

75%

of executives say their organisation has faced challenges in trying to address supply chain risks.

Overconfident or unprepared?

Australian businesses are confident in their ability to respond to risks in the supply chain, but the reality is that many are unprepared.

Unsurprisingly, many business executives (50 percent) identified financial risk as one of their top three risks and 22 percent said it was the risk most likely to increase in severity. Financial risk is the easiest to identify, quantify and attempt to address for business and respondents included in their responses interest rate rises, high inflation, working capital issues, wage increases, and supplier or client financial instability. However the survey results go on to highlight the difficulty for executives to similarly assess and address other categories of risk.

More than half of all business executives (53 percent) say they are very confident in their organisation's ability to navigate risks that will impact their supply chain. However, this means that 47 percent still have reservations and concerns. This initial confidence is also at odds with other details in the research, which found that 26 percent of businesses have never considered or discussed risks in the supply chain, and therefore haven't updated their plans accordingly.

Despite recent high-profile data breaches, some of which originated through third-party software providers, 73 percent of organisations have not considered cyber risks in their latest risk management plans. Almost 3 out of 4 businesses haven't considered geopolitical risks (74 percent), supply chain risks (74 percent), counterparty risks (73 percent), or legal/regulatory risks (80 percent) either. These findings demonstrate that Australian business leaders are either underestimating the current threats to their business, do not fully understand the intricacies of their supply chains, or are simply too trusting of their suppliers' ability to manage these risks.

94%

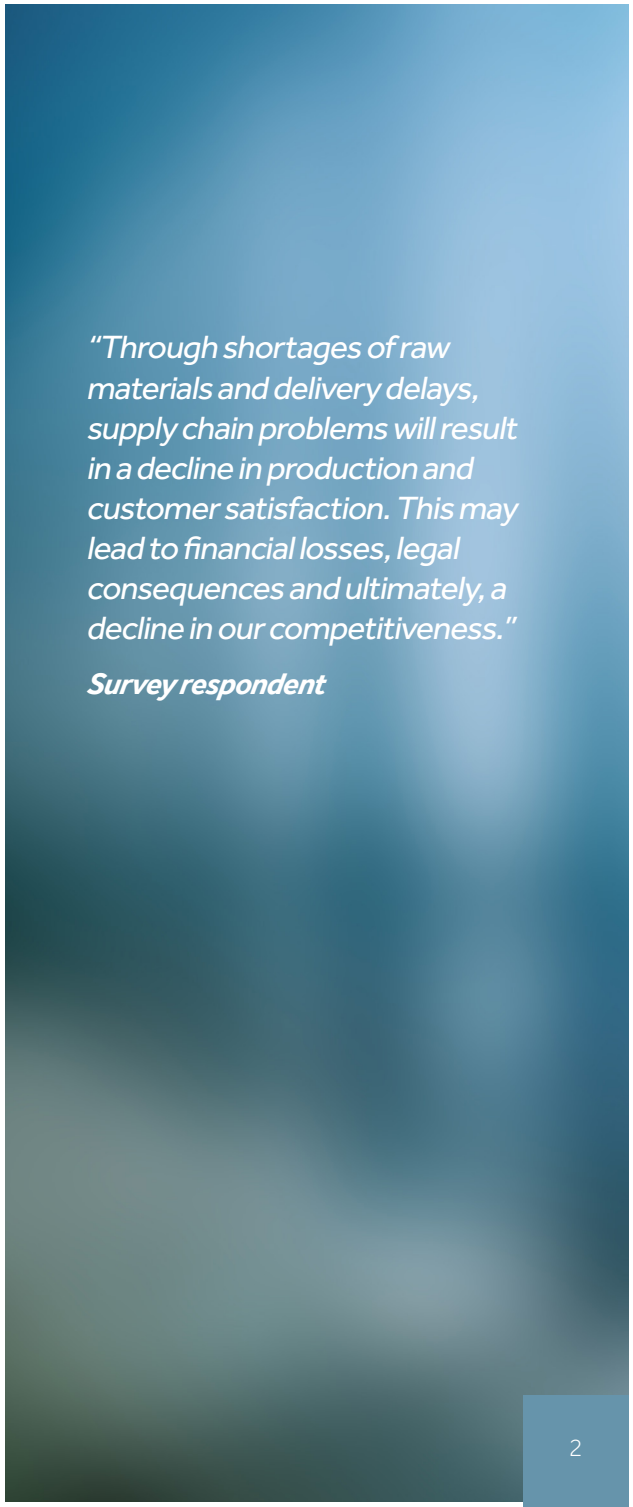
claim to have a high-level awareness of their supply chain risk management program.

42%

believe that these risks will not increase in severity and impact their organisation in the next 12 months.

17%

assume that because their supply chain is small, it doesn't require risk management.



"Through shortages of raw materials and delivery delays, supply chain problems will result in a decline in production and customer satisfaction. This may lead to financial losses, legal consequences and ultimately, a decline in our competitiveness."

Survey respondent

Key survey findings

01. Overcoming challenges to identify and address supply chain risks.

Three quarters (75 percent) of business leaders say their organisation has faced challenges addressing supply chain risks, with respondents citing a lack of awareness and understanding of their supply chain, apathy, limited data, unstructured planning, and the assumption that others are responsible for managing these risks. Education is needed to help businesses better understand the risks in their own supply chain, and that of their suppliers.

02. Market underestimates chance of increased geopolitical risk in 2024.

Only 16 percent of business leaders believe that geopolitical risk will increase in severity in terms of the impact on their organisation over the next 12 months; a figure which McGrathNicol believes underestimates the potential impact of the rapidly shifting geopolitical environment, including risks associated with upcoming Taiwan and US elections.

03. Third party cyber risks are misunderstood, as many businesses think a global supply chain attack won't impact them.

While 64 percent of Australian businesses rank cybersecurity as the second greatest challenge to their organisation (behind financial performance), businesses underestimate the likelihood or impact of an attack on their third-party suppliers to their business: just one in six (16 percent) predict that these risks will impact their organisation over the next 12 months, with only 27 percent including cyber risks within their supply chain management plans.

01. Overcoming challenges in the modern supply chain

Modern supply chains are far more than just the financial cost and physical movement of goods. From cloud-based payroll systems to CRM platforms, commercial manufacturers to global warehousing and data storage, an organisation's supply chain encapsulates all the suppliers, manufacturers, customers, contractors, service providers and software systems that enable it to operate and function.

Four in five (81 percent) C-Suites, Directors and Managers say that their organisation plans to implement strategies to better understand and mitigate supply chain risks.

A starting point needs to be developing a more holistic perspective of supply chain risks. While financial risk is well covered by organisations' supply chain risk management programs (57 percent), other significant threats, including cyber (27 percent), counterparty (27 percent), geopolitical (26 percent) and personnel risk (25 percent), are typically not included.

Too often, mapping the threats to a business' modern supply chain is seen as a daunting, time-consuming task. Many executives (75 percent) say their organisation has faced challenges when trying to do so.

The most common barriers to addressing supply chain performance and risk management include:

- Limited transparency and an inability to source appropriate data on the supply chain (34 percent).
- An assumption that the procurement team, logistics team or external suppliers are responsible for protecting the organisation's interests (33 percent).
- A general lack of awareness and understanding of supply chain risks due to limited or no supply chain expertise within the business (30 percent).
- A further one in four (23 percent) cite undocumented accountability and unstructured planning as key barriers.

"Supply chain risk management programs have failed to keep pace with the modern supply chain. While businesses fully understand financial risks, they need to better address the other operational risks that directly threaten and impact the company's bottom line."

Rhyan Stephens
Partner, McGrathNicol Advisory

02. Market underestimates chance of increased geopolitical risk

Geopolitical events continue to impact global trade and markets and we assess several key events have the potential to significantly increase geopolitical risks in 2024. An increase in geopolitical risks in 2024 could be driven by a range of factors including COVID-style events, conflicts (Ukraine, Israel and potentially Taiwan), sanctions imposed on technology, goods or services and/or on our trading partners. All of these events have significantly impacted global trade in the past. However, several key elections, in Taiwan and the United States, have potential to cause serious disruption. As an example, in response to US House Speaker Nancy Pelosi's visit to Taiwan in 2022, the People's Republic of China (PRC) launched military exercises of an unprecedented scale, effectively blockading the island for a period of time. Some cargo ships and oil tankers were forced to re-route, adding half a day to voyages.*

What this could mean for Australian businesses

If paralysis emerges from either election or other geopolitical events, there is potential for more severe disruption. As an example, should sanctions or other trade restrictions be placed on our major trading partners, the implications for global supply chains could be costly and complex, ranging from:

- supply chain disruption, sanctions or trapped assets
- increased financing and insurance costs
- heightened regulatory burdens and demands, as governments look to de-escalate tension.

Underestimating geopolitical risks and overestimating ability to respond

Only 16 percent of Australian businesses believe that geopolitical risk will increase in severity in terms of the impact on their organisation over the next 12 months; a figure which McGrathNicol believes underestimates the potential impact of geopolitical risks over the coming period.

At the same time, business leaders overestimate their ability to respond: more than half of all business executives (53 percent) say they are very confident in their organisation's ability to navigate risks that could impact their supply chain. Geopolitical risk features in only a quarter (26 percent) of supply chain risk management plans updated in the past 2 years. This too, suggests a lack of understanding of the shifting geopolitical landscape.

"Comments in our survey indicated a focus on supply chain risks from the Russia/Ukraine war. Many executives are either underestimating, or do not fully understand, rising geopolitical risks in the Indo-Pacific, including risks of trade disruptions in the South China Sea... and the impact these geopolitical flashpoints may have on their business."

Sam Boarder
Partner, McGrathNicol Advisory

** Joe Brock, "China's military drills near Taiwan disrupt key shipping lanes", Reuters, 5-Aug-2022, https://web.archive.org/web/20230519143514/https://www.reuters.com/world/asia-pacific/chinas-military-drills-near-taiwan-disrupt-key-shipping-lanes-2022-08-05/.*

03. Cyber due diligence doesn't stop at the back door

Only 27 percent of Australian businesses have considered 'cyber risk' in their supply chain risk management programs.

In the wake of high-profile ransomware and cyber attacks, Australian business leaders, Boards and regulators are paying greater attention to cybersecurity concerns: 38 percent of businesses rank cyber risk as a top 3 challenge. Yet, businesses are underestimating the likelihood of an attack on their third-party suppliers, and the impact on them directly. Just one in six (16 percent) predict that cyber risks will increase and impact their organisation over the next 12 months.

Over two thirds (68 percent) of organisations that haven't updated their risk management programs in the past two years, state the reason being: "suppliers are responsible for understanding and managing their own risks". The attitude, that supply chain risks are someone else's problem, is no longer good enough. Australian regulators like ASIC and APRA are increasingly holding organisations, their Boards, and Directors, responsible for managing all risks associated with their business' supply chain, including cybersecurity and data protection concerns.

A strategic cyber risk assessment

1. Carry out a robust assessment of the local, national and global environments in which your business is operating, to uncover gaps in your end-to-end supply chain and potential weaknesses that may be exploited.
2. Determine your risk appetite within an updated supply chain risk management plan that includes cyber and data privacy risks. At a Board level, this should be reviewed on a quarterly basis with the aid of assessment tools and dedicated cyber risk and strategy experts.
3. Ensure that both cyber and operational systems security is included in all tenders, evaluation criteria and supplier agreements to promote accountability across counter parties.
4. Review and audit your organisation's risk appetite statements and ensure that cyber risk is being treated accordingly. The supply chain risk management plan must also be updated to include assessments of suppliers' cyber credentials.

"The supply chain is only as strong as its weakest link. Increased digital connectivity often means that link is outside of your organisation.

If your business is dealing with external suppliers, global contractors or other service operators, extra caution must be exercised as a lack of transparency may conceal unidentified risk."

Blare Sutton
Partner, McGrathNicol Advisory

Contacts

McGrathNicol can assist in the exploration and illumination of your supply chains, using our multi-lens analysis. Our Supply Chain team works collaboratively with our National Security, Geopolitical Risk, Cyber Security, Financial Due Diligence and Counterparty Due Diligence Experts to identify potential areas of threats and hazards, mitigate vulnerabilities and risks, and develop supply chain strategies that drive competitive advantage.

Matt Fehon
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.

Joss Howard
Partner, Cyber
M +61 460 972 700
E jhoward

Joss advises Boards and senior management on effective information and cyber security strategies, helping to set the 'tone from the top'. Built over a 25 year career leading and implementing security programs, she is an expert in risk assessment and cyber resiliency.

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.

This study was conducted online between 1 August and 11 August 2023 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 308 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.