As global supply chains take on a nightmare complexity, it’s hard to vouch for all third-party providers. In this edition of The Knowledge, we look at the issues that demand urgent attention.

By Jessica Reid, StrategicRISK editor (Asia-Pacific)
Why it’s folly to mind your own business

Failing to keep tabs on suppliers could prove a calamitous mistake – but as our latest survey shows, not all companies appreciate this.

In disaster-prone Asia-Pacific, firms don’t quite grasp how exposed their suppliers are to natural catastrophes

The vast majority of companies do not fully understand their suppliers’ exposures to natural catastrophes, according to the StrategicRISK Asia-Pacific Supply Chain Disruption survey.

Only 12% of respondents said they ‘comprehensively’ understood their key production facilities and logistics hubs’ exposures to nat cats. Almost three-quarters (73%) said they did ‘to some extent’.

The results should cause concern for risk managers in Asia-Pacific, the world’s most disaster-prone area when it comes to the frequency and severity of natural catastrophes.

But despite this, underinsurance in the region continues to be a major issue.

In the past 10 years, uninsured losses from storms, floods and earthquakes made up more than 85% of all economic losses in Asia’s emerging markets, according to a report by Swiss Re Corporate Solutions.

A common mistake, said Zurich Global Corporate global supply chain product leader Nick Wildgoose, was companies basing their suppliers’ locations on their mailing address or company headquarters, instead of their manufacturing or logistics location, which may be more exposed.

Parikshit Sen Gupta, vice-president, finance at hotel and resort company Shangri-La, said his biggest concern when it comes to managing the business’s supply chain is the “impact of [the] environment” and its flow-on effects.

Properties should be built to withstand earthquakes and typhoons, and risk managers should ensure they have adequate insurance. It is important to know what your policy covers and if it is adequate for your locations.”

Tan Shuh Lin
InterContinental Hotels Group

As the world becomes more connected, the ease of doing business across borders has never been easier. If that’s the upside of globalisation, one major downside is the ever-increasing complexity of managing global supply chains.

In this issue of The Knowledge, we wanted to get a deeper understanding of some of the key challenges facing supply chain risk management. We therefore sought the views of 55 risk managers from across Asia-Pacific in our StrategicRISK Advisory Panel.

Our survey found, on the surface, that things largely seem to be under control. Most risk managers (70%) gave themselves a score of eight out of 10 or higher for how well they know their critical, or tier-one, suppliers. Training also got a thumbs up, overall: four in five said risk management processes had been integrated into their supply chain and almost the same amount (70%) record any incidents and actions taken in supply chain disruption events.

Scratch below this top line, however, and you’ll find a different story. One where transparency of third-party providers is murky and viability of business continuity plans is severely limited. Clearly 100% transparency of the supply chain, from raw material to customer, is near-impossible, if even desirable. But equally clearly, there are gaps in supply chain risk management that need urgent attention. We hope you enjoy this special report.

Email jessica.reid@nqsm.com

In disaster-prone Asia-Pacific, firms don’t quite grasp how exposed their suppliers are to natural catastrophes

The vast majority of companies do not fully understand their suppliers’ exposures to natural catastrophes, according to the StrategicRISK Asia-Pacific Supply Chain Disruption survey.

Only 12% of respondents said they ‘comprehensively’ understood their key production facilities and logistics hubs’ exposures to nat cats. Almost three-quarters (73%) said they did ‘to some extent’.

The results should cause concern for risk managers in Asia-Pacific, the world’s most disaster-prone area when it comes to the frequency and severity of natural catastrophes.

But despite this, underinsurance in the region continues to be a major issue.

In the past 10 years, uninsured losses from storms, floods and earthquakes made up more than 85% of all economic losses in Asia’s emerging markets, according to a report by Swiss Re Corporate Solutions.

A common mistake, said Zurich Global Corporate global supply chain product leader Nick Wildgoose, was companies basing their suppliers’ locations on their mailing address or company headquarters, instead of their manufacturing or logistics location, which may be more exposed.

Parikshit Sen Gupta, vice-president, finance at hotel and resort company Shangri-La, said his biggest concern when it comes to managing the business’s supply chain is the “impact of [the] environment” and its flow-on effects.

Properties should be built to withstand earthquakes and typhoons, and risk managers should ensure they have adequate insurance. It is important to know what your policy covers and if it is adequate for your locations.”

Tan Shuh Lin
InterContinental Hotels Group

As the world becomes more connected, the ease of doing business across borders has never been easier. If that’s the upside of globalisation, one major downside is the ever-increasing complexity of managing global supply chains.

In this issue of The Knowledge, we wanted to get a deeper understanding of some of the key challenges facing supply chain risk management. We therefore sought the views of 55 risk managers from across Asia-Pacific in our StrategicRISK Advisory Panel.

Our survey found, on the surface, that things largely seem to be under control. Most risk managers (70%) gave themselves a score of eight out of 10 or higher for how well they know their critical, or tier-one, suppliers. Training also got a thumbs up, overall: four in five said risk management processes had been integrated into their supply chain and almost the same amount (70%) record any incidents and actions taken in supply chain disruption events.

Scratch below this top line, however, and you’ll find a different story. One where transparency of third-party providers is murky and viability of business continuity plans is severely limited. Clearly 100% transparency of the supply chain, from raw material to customer, is near-impossible, if even desirable. But equally clearly, there are gaps in supply chain risk management that need urgent attention. We hope you enjoy this special report.

Email jessica.reid@nqsm.com
Most risk managers recognise the importance of supply chains and are active in improving their resilience, according to the StrategicRISK Supply Chain 2016 survey.

Almost four in five (78%) respondents have incorporated risk management processes into their supply chain management approaches, and more than half (56%) have provided risk training to their supply chain management team.

This is an encouraging result, considering that all respondents said a disruption to a critical supplier would have an impact on their business – be it ‘significant’ (65%) or ‘limited’ (35%).

Commenting on the results, Myanmar Brewery head of risk management, internal controls and processes, and board member of the Pan-Asia Risk and Insurance Management Association, Jagath Guru, said: “In today’s highly competitive, complex and interconnected supply chain environment, we cannot over-emphasise the importance of helping external stakeholders such as partners and service providers (and the third/fourth-tier suppliers) with risk management through training.”

“I see this as an excellent opportunity to facilitate engagement with stakeholders, provide better visibility of the supply chain and, consequently, provide assurance of compliance with legal/regulatory requirements and a resilient supply chain.”

The task has its challenges, however. Guru, like many other risk professionals, said a key issue is “getting stakeholder buy-in for risk management training and designing a training programme that would meet the respective stakeholders’ needs.”

Many corporates are putting themselves at unnecessary risk by failing to properly check the financial stability of their critical suppliers.

In the StrategicRISK survey, only 54% of respondents said they had timely systems for measuring suppliers’ financial health (see chart, right).

“Frameworks for measuring financial stability are either not in place or are inconsistent across business functions,” one respondent said. Another remarked: “While in place for some operations, it’s not consistent across all.”

Worryingly, some respondents admitted that carrying out the checks may be no more than a box-ticking exercise. “We collect credit/financial information of these suppliers, but I’m not sure if these indicators are truly sufficient,” said one.

Many respondents said suppliers’ financial stability and performance was reviewed as part of their onboarding process and again at contract renewal.

Zurich Global Corporate global supply chain product leader Nick Wildgoose said that while this is a good start, it may not be enough for all suppliers.

“Due diligence may be once a year. But where [the supplier] is critical to your business, you need to be monitoring them more often than that,” he said.

“Also, when suppliers are in difficult territory, like Hanjin Shipping [which went bankrupt in August] for example, I don’t think it’s a good assumption to operate on the basis that the government’s going to keep bailing them out forever.”

Wildgoose’s comments echo the results of the Business Continuity Institute’s 2016 survey on Supply Chain Resilience, which saw supplier insolvency come 10th in the list of concerns around supply chain disruption events.

To improve resilience, Wildgoose recommended companies identify their most profitable products/services and then look at the suppliers that are critical to delivering these. The answer may not necessarily be the supplier that the company spends the most amount of money with.
Should you fear a cyber attack on your colleagues?

Risk managers are understandably anxious about breaches of their suppliers’ cyber defences. Is the threat as bad as it’s painted, and how can the risks be minimised?

Looking solely at their own cyber defences is no longer a tenable position for firms. Increasingly, they must look at their suppliers’ as well.

The StrategicRISK Supply Chain Disruption survey found that a ‘targeted cyber attack (internal or external)’ was risk managers’ top concern out of 10 possible disruptive events (see graph, right). A cyber attack on a critical supplier was considered most likely to bring a company to its knees.

Human operating error was next, with government/regulatory intervention in third place.

“This vote reflects [risk managers’] uneasiness at being able to grasp the likelihood and consequences of such a cyber attack: since I don’t understand it, I fear it, and since I fear it, I give it high marks,” says Huawei Enterprise’s chief security and privacy officer, Pierre Noel.

“Cyber security is among the least understood type of risks at the moment. Risk managers hear about those cyber incidents happening here and there, and they feel like the sky is about to fall. In reality, cyber attacks follow some rather specific patterns, based on the origins of the attacks, as well as the motivations behind those attacks.”

“This doesn’t give much comfort to Shangri-La vice-president, finance, Parikshit Sen Gupta. He says he’s very concerned about the implications of a cyber breach at one of the hotel and resort group’s critical suppliers.

“For some of our suppliers who store our customer data, this risk is imminent,” he says, stressing that it would be Shangri-La’s brand at risk – and not that of the third party at fault – if a data breach occurred.

A PERFECT STORM

Jagath Guru, Myanmar Brewery head of risk management, internal controls and processes, agrees. He says: “Third-party vendors do play a vital and growing role in supporting organisations’ systems, applications, and devices.” But he thinks many organisations are not fully aware of their reliance on such suppliers.

“Organisations often have limited visibility or control on what the engaged third-party vendors’ activities are connected to [within the] organisation’s own network. The combination of dependence, trust and lack of control [is] the ideal situation for creating a ‘perfect storm’ for security breaches across the organisation, regardless of organisation size,” he says.

If an organisation’s network gets into the wrong hands, adds Guru, there is a high risk of data being compromised or stolen, or of critical systems being shut down.

“Cyber risk is one of the most dynamic I have ever encountered: a device or a program that is deemed safe today could become vulnerable tomorrow and be attacked on a worldwide basis the day after.”

Pierre Noel
Huawei Enterprise

“Cyber risk is one of the most dynamic I have ever encountered: a device or a program that is deemed safe today could become vulnerable tomorrow and be attacked on a worldwide basis the day after.

The only way to address this dynamic is to be accountable and keep a finger on the pulse.”
SUPPLY CHAIN RISKS
10 POSSIBLE DISRUPTIVE EVENTS, RATED BY LIKELIHOOD AND FINANCIAL IMPACT

How Telstra dealt with the Pacnet hack

Australian telecommunications company Telstra has already experienced a data breach via a third party. Last year, the group acquired Asian telecommunications provider Pacnet. But two weeks before the $697 m deal was finalised, an unknown third party hacked into Pacnet and gained complete access to its network, including emails and other administrative systems. Telstra wasn’t told until after the deal’s completion. Its chief risk officer, Kate Hughes, says it voluntarily went to eight different regulators about the breach. “Each one had different expectations about whether or not we would or should tell them,” she told StrategicRISK. “We’ve always felt better to be upfront and honest. The worst thing you can do is look like you’re hiding it.”

Australia is looking to introduce data-loss notification laws that will force companies to advise customers when their details have been unlawfully accessed. It is unclear how far-reaching the laws will be, however, and what the fines and procedures will be. Singapore is considering similar legislation.

For Telstra, Hughes says the key focus for cyber security is on employees, often considered to be the weakest link in any cyber security programme. “We run drills to see if we can trick our employees into doing something that they shouldn’t have,” she says. This might mean clicking on a link or opening a suspect attachment. In the first drill, 30% of employees failed. This dropped to 18% in the second round.

Thinking of your critical suppliers, how much would the failure/inability to supply impact your company profits?

65%
Their failure would have a significant impact on our company’s profits

35%
Their failure would have a limited impact on our company’s profits

METHODOLOGY
Respondents were asked to rate 10 supply chain disruption events individually, by likelihood and financial impact, on a scale of 1-5 (1 being very low, 2 being low, 3 being medium, 4 being high and 5 being very high). The scatter graph plots the average score for both likelihood and financial impact.

BIG NUMBERS
Unplanned IT and telecommunications outages remains the top cause of supply chain disruption for the fifth consecutive year, according to the Business Continuity Institute.

How Telstra dealt with the Pacnet hack

Australian telecommunications company Telstra has already experienced a data breach via a third party. Last year, the group acquired Asian telecommunications provider Pacnet. But two weeks before the $697 m deal was finalised, an unknown third party hacked into Pacnet and gained complete access to its network, including emails and other administrative systems. Telstra wasn’t told until after the deal’s completion. Its chief risk officer, Kate Hughes, says it voluntarily went to eight different regulators about the breach. “Each one had different expectations about whether or not we would or should tell them,” she told StrategicRISK. “We’ve always felt better to be upfront and honest. The worst thing you can do is look like you’re hiding it.”

Australia is looking to introduce data-loss notification laws that will force companies to advise customers when their details have been unlawfully accessed. It is unclear how far-reaching the laws will be, however, and what the fines and procedures will be. Singapore is considering similar legislation.

For Telstra, Hughes says the key focus for cyber security is on employees, often considered to be the weakest link in any cyber security programme. “We run drills to see if we can trick our employees into doing something that they shouldn’t have,” she says. This might mean clicking on a link or opening a suspect attachment. In the first drill, 30% of employees failed. This dropped to 18% in the second round.

Thinking of your critical suppliers, how much would the failure/inability to supply impact your company profits?

65%
Their failure would have a significant impact on our company’s profits

35%
Their failure would have a limited impact on our company’s profits
Hidden problems that can trigger a chain reaction

Few companies have full transparency of their supply chains. What are the implications of this, and how can this impact a company’s reputation?

When it comes to risk, a company’s supply chain is like an iceberg: much of it is submerged and out of sight. For some major corporations with thousands of third-party vendors, full transparency of their supply chains is not deemed a necessity, let alone feasible. In fact, a StrategicRISK survey found that very few corporates have transparency of their supply chains (see graph, opposite). But what are the implications of this lack of transparency, and how can this impact a company’s reputation?

“We are seeing an interesting shift in supply chain management – and it’s been driven by consumers and customers,” says Kate Hughes, chief risk officer at Telstra, the Australian-headquartered telecoms firm.

“Expectations are changing. [Customers] want to know exactly where products are coming from, how they were made and under what conditions.

“They want to know who their service providers, such as banks and technology partners such as Telstra, are working with, and how they are managing their impacts.”

Hughes says companies are responding to this – and they need to respond – as they will be held to account by those who buy their products or services, as well as by investors and the court of public opinion.

“They want to know who their service providers, such as banks and technology partners such as Telstra, are working with, and how they are managing their impacts.”

Kate Hughes
Chief risk officer, Telstra

“Responsible and sustainable supply chain management doesn’t end with the contract, it’s ongoing. Because if a supplier acts outside of the law, or indeed in a way that doesn’t match societal – or company – expectations, it is most likely the big, well-known brand associated with that supplier who will be targeted.”

MailGuard chief executive and founder Craig McDonald says that over the past six months, he has seen an increasing number of emails being sent to businesses from what appear to be brands that we trust, like a telco, bank or government body.

“The problem is that staff are being ‘happy clickers’, leaving the company and being taken offline due to ransomware, for example,” he says. “A major problem is failing to understand the ramifications of these problems within the supply chain.”

Several manufacturing and warehousing groups have come under attack, he adds, and customers are no longer able to reach them. “That has put a lot of pressure on the companies they supply, even those companies have not directly been affected.

“This has highlighted some of the touch points that can undo a business.”
These supply chain transparency issues all beg the same question: how does a risk manager go about mitigating the risks they create? Leesa Soulodre, RL Expert’s chief reputation risk officer, suggests several avenues to explore.

“Implement an early-warning system to increase transparency and monitor risks and issues in all tiers of the global supply chain, and ensure a life-cycle risk management approach,” she says. “Point-in-time analysis does not work. Reviewing a supplier not only when they are onboarded, but also on a daily basis throughout the relationship, will ensure that sustainability, security and reputation risk issues are identified early for risk mitigation.”

Tools for this measure include SAP, Oracle, WorldCheck, SmartWatch, RepRisk and SAS, says Soulodre. “Get the board and CEO on board,” she adds. “Leverage tone at the top to build an active reputation risk management and risk-aware culture around the importance of a responsible supply chain and CSR programme. Without this, tactical efforts will fail.”

ZERO TOLERANCE

She says it is vital that staff are educated on the programme and understand the consequences. “You need to ask, is this supplier’s activities legal, ethical, acceptable, defirable, sensible? If we make the decision to support this supplier, does this change who we say we are as a company?”

Soulodre says all tiers of the supply chain must show zero tolerance of child labour, modern slavery, bribery and corruption, money-laundering and extortion. “This should be clearly articulated as part of the signed supplier code of conduct and checks for breaches must form a critical part of the ongoing factory audit process by a specialised and independent third party.”

In addition, risk managers must factor outrage and velocity into their risk assessment: “Implement a rating system and rate the supplier based on the audit result and what is published in the public domain. Understand their sensitivity to this topic as gauged by your risk intelligence.” A red rating, for example, could be assigned when one of the audit requirements has not been met for critical risk issues and when stakeholder outrage is low.

“Make sure a regular audit cycle forms a part of the ongoing supplier due diligence programme, and records and results are located in a central place, easily accessible by frontline staff. Also, when an issue occurs in your supply chain, do not defer the blame to your supplier. Reputation risk is your responsibility and yours only.”

Soulodre says risk managers must accept accountability and demonstrate empathy to those affected.

“Explain the facts: who was affected, what was affected, when it happened, where it happened and why it happened. Articulate a clear action plan and timeline to address the issues and advise immediately once the risk has been contained.”

It is also important to collaborate with your supplier to achieve this objective, she says. “Put them on notice, if they must be terminated. Live up to your promises to your stakeholders and demonstrate the steps your company has taken to ensure this will never happen again. Communicate. Communicate. Communicate.”

Once your stakeholders allow you to go back to business as usual, Soulodre says, then and only then can you address the liability and responsibility of your supplier.
The bankruptcy of South Korean shipping company Hanjin in August, which left $14bn worth of cargo stranded in ports and open waters across the globe, could also result in further insolvencies along the supply chain.

The world’s seventh-largest shipping firm filed for bankruptcy on 31 August following a failure to restructure its debt. It operated 98 container ships (some owned, some chartered) and several other types of ship.

Within a day, ports began to turn away Hanjin vessels for fear of not being paid fees.

A report by Marsh noted that goods due to be shipped on those vessels were building up. “The owners of the goods have consequently been exposed to financial risks following the failure of the ship operator, as contractually agreed delivery dates would be missed, goods would need to be stored, and extra expenses incurred as alternative routes for delivery would need to be arranged.”

Marcus Baker, chairman of Marsh’s global marine practice, added there is considerable concern in the industry as to whether or not companies are insured against this scenario:

> “Unfortunately there is no simple answer that fits all cases, as marine cargo insurance policies are written on a wide variety of terms and conditions, for which there are going to be very different answers.”

The marine insurance market is carefully following the situation, said Bart Hoogstad, European head of marine and transportation at Crawford & Company: “Whilst at this early stage, we have not heard reports of claims for material damage to cargo, it is inevitable there will be some physical loss, damage or expense to a variety of cargo.”

Due to lack of space, ports and terminals may have to close their gates to Hanjin-scheduled containers. As Marsh noted: “This will then have an adverse effect on independent truck companies, rail freight companies and hauliers, as they will be refused entry to ports and will have to find a means of storing these containers.”

It added that “such companies may have to refuse to load boxes scheduled to be carried on Hanjin vessels. While this would reduce the problem of storage, it would also reduce their income.” Since many trucking firms work on very tight margins, Hanjin’s insolvency “could lead to the financial default of others all along the supply chain”.

The case highlights why companies should assess the business continuity plans of their key suppliers, said Zurich Global Corporate global supply chain product leader Nick Wildgoose. But in the StrategicRISK supply chain survey, 46% of respondents said they were unsure if their tier-one suppliers had viable and tested BCPs. Only 23% said they did (see graph).

Wildgoose said: “I appreciate there’s no way that clients can monitor BCP plans for every single supplier, but for those that are feeding into let’s say 25% of their profitability, the board should expect and give the resource to monitor [their BCP plans].” New technology will help in monitoring new suppliers, he added.

“Investors in those companies would also expect them to do some kind of due diligence and make sure in the pre-contract discussions with suppliers that they see the business continuity plans … And then preferably that they test it to different common sets of disruptions. So, for example, how would we cope with a failure in our logistics supply (such as Hanjin)? What’s our back-up plan: is there another logistics supplier, do we air freight it, or do we need more inventory?”

According to Wildgoose, companies often assess only those suppliers they spend the most money with, when it may be a much smaller supplier that causes problems. He recommends companies assess their most profitable products or services first, then look back to the suppliers they depend on.

“When you look at the value at risk, that’s also what wakes the executives up to take their supply chain resilience seriously.”

He added: “One of the most common key performance indicators across all industry segments is as simple as ‘delivering for your customer on time’. So obviously supply chain performance and lack of disruptions feeds into that. Hanjin is just another event that shows how global just-in-time supply chains are exposed to black swan events. The trouble is, there’s quite a lot of black swan events [in general] at the moment.”
“We review critical supply chain events only.”

“Incidents are not reported in a consistent manner.”

“An Embedded Incident Management tool is used to report and monitor incidents globally, which includes in-built escalation rules depending on the severity of the incident and the action required.”

“Our HSE Dept records all near-misses.”

“Contingency and business continuity plan for in the event of incidents, and we specifically emphasis this on our contract agreement.”

“All supply chain incidents (such as failure to deliver within the stipulated timeline) are documented and would be used in the suppliers’ annual performance appraisal and review.”
The wonder – and the woes – of Woolworths

Unforeseen crises forced Grant Katz, the retailer’s risk and assurance general manager, to postpone his interview four times in a fortnight. The stress left him feeling exhausted. So why does he like his job so much?

Woolworths risk and assurance general manager Grant Katz has one small request at the end of our hour-long interview and photoshoot.

“Please can you Photoshop the big bags out from under my eyes?”

Katz makes the request in jest, but there is more than a spec of truth behind his tired eyes.

In the two weeks leading up to our interview, the meeting had to be rescheduled four times on account of a string of unexpected crises.

First there was a data leak of customer details from the group’s major retail chain, Big W. The leak saw it in the headlines of national news outlets and resulted in the website being closed to online trade for a number of days. Then, a few days later, a 7.5 magnitude earthquake struck New Zealand, damaging a number of the group’s Countdown grocery stores and distribution centres. That’s not to mention the product recall and customer injury issues that can happen daily across the group’s 4,000 stores.

Wearing the hat of the crisis management lead, it is Katz’s job to co-ordinate the 80-strong risk and audit team. “Every day is all well planned, except when it goes wrong, and things do go wrong a lot,” he laughs. “I have incident management, fraud and forensics, internal audit, product safety and enterprise risk [in my remit]. So we’re the ones that are getting fed the information [from incidents] and we’ve got to co-ordinate what actually happens in response.”

Katz joined Woolworths Group in June last year, following a four-year stint as the chief audit executive for Metcash, a wholesale grocery distribution and marketing company.

Woolworths is the one of Australia’s most recognisable brands, known primarily for its ownership and operation of one of the country’s two major supermarket chains. It’s also the largest takeaway liquor retailer in Australia, through outlets including Dan Murphy’s and BWS, and the largest hotel and gaming poker machine operator in the country via its ALH Group business.

The company, once a star performer on the Australian Stock Exchange, has had a tough couple of years, with its supermarkets business trounced by rival Coles and its Masters hardware chain proving a big drain on the balance sheet.

That triggered a collapse in its share price, which sliced $15bn from its market capitalisation in 12 months alone. In its 2015/16 annual report, the group posted a $1.2bn loss – its first loss in 23 years as a public company.

“Unfortunately, the perception of Woolworths was we were too expensive and the customer experience was poor,” Katz explains. Which is precisely what attracted him.

GREEN SHOOTS

“I liked the fact that Woolworths was going through some challenges and I wanted to be part of the solution to those challenges,” he says.

It’s a slow-moving beast, but Katz says the fruits of their labour are starting to show.

“Especially in the food space, there’s lots of green shoots. We’ve had positive sales growth in the quarter that’s just passed.”

Company culture is another thing he speaks about at length. “With a lot of new board members, a new CEO and a lot of change in the
senior management team, you feel as though you’re part of something completely new. There’s a cultural shift. Culture doesn’t change overnight, but we’re starting to see little things occurring,” he says.

“When you look at what’s happened with Woolworths… you had a more ‘command and control’ organisation previously. That works well when things are going great, but in my opinion it doesn’t work well when you’re going through challenges. You’ve got to make people accountable,” he says.

Under new chief executive Brad Banducci, the operating model is essentially to make the businesses run independently, within a framework set by the group.

“Freedom within framework,” explains Katz. “That goes a long way to change the culture but it’s not a quick fix.”

BIG STICK

Still, like most risk managers, he faces the challenge of getting internal buy-in from stakeholders on the value of his work. “The challenge is that Woolworths is not highly regulated like a bank. When you look at the bank, you’ve got big stick APRA,” he says.

“For us, it’s very easy to tick the box in terms of ASX principles to say I do [risk and compliance]. But to really show how [risk management] adds value is the challenge.

“If you don’t make mistakes, or you do things better, how do you articulate that in terms of the value? When you look at people safety, it’s very easy to measure because people are getting injured on a daily basis. So, by just looking at the number of incidents, you know whether you’re doing better or not. But things that might occur once every five years or more, how do you know risk management is actually working? That’s the difficulty.

“That’s the toughest part of a risk role in a non-highly regulated company.”

But Katz says the relationships he has built internally over the past 18 months are helping to change this.

“You have to have difficult conversations a lot of the time, but it’s about building relationships. So, if you get those relationships, then people are willing to trust you,” he says. He is lucky, he adds, to have a supportive boss in chief financial officer David Marr.

So, what’s the biggest risk he and his team have to manage? “It’s around the customer value proposition. You’ve got to make sure that what you’re delivering satisfies the customer,” he says simply.

Some of the key risks to this are around cyber security and brand reputation, he adds. “Cyber security is a big risk in all organisations. We have online facing websites – Dan Murphy’s online, Woolworths online – and if you have a major leak or someone hacks in, it’s going to be front page of the paper. The Big W one was in the paper and that was minor.

“We have a CISO – a chief information security officer – and their remit is looking at all of these things. I don’t believe you can prevent it completely … the question is how will you react.”

With a large-scale effort to turn the company around, a number of major projects are being launched that also need to be seen through a risk lens. From greater automation of supply chains to store upgrades and new technology, Katz’s role is varied, to say the least.

“It’s constantly changing. Every day’s completely different. Part of risk management is being part of strategy, so you need to be across what’s happening in the market, what’s happening in the organisation and what are the things that are emerging,” he says.

LOOKING FOR STABILITY

Like many of his peers, Katz didn’t grow up with ambitions to work in risk management. Having qualified as a chartered accountant, he held a number of finance and investment banking roles in his home country of South Africa before moving to Australia in 1999.

“I was reluctant to have kids in South Africa because I didn’t know what the future might hold. I was looking for more stability in terms of lifestyle,” says the father-of-two.

His first role in Australia was at construction and engineering firm Lendlease as the GST project delivery manager.

“South Africa had GST long before Australia … so I thought I’d use [the job at Lendlease] as an opportunity to learn the Australian systems and, with GST being a transaction tax, what a great way to learn. I did that for 12 months.”

Katz then took a role at the ASX, which was a combination of finance, treasury, risk management and strategic planning functions. While working there, he completed his MBA, which he credits as the turning point in his career.

“When you look at risk and strategy, they go hand in hand. That was the start of my exposure to risk management,” he says.

After a few years, he was lured back to the accountancy firms, which at that time were looking to grow their risk management offerings.

But while on secondment to Mirvac, he was offered a permanent position to lead the company’s internal audit and risk management team.
When you look at what’s happened with Woolworths... you had a more ‘command and control’ organisation previously. That works well when things are going great, but it doesn’t work well when you’re going through challenges. You’ve got to make people accountable.”

As any risk manager in the construction or engineering space will attest, ‘optimism bias’ is one of the key challenges to overcome – so after a few years at Mirvac, Katz took on the role of chief audit executive at Metcash, the Australian wholesale distribution and marketing company.

**FAST-MOVING**
Metcash specialises in grocery, fresh produce, liquor, hardware and other fast-moving consumer goods; IGA, Cellarbrations and Mitre 10 are some of its best-known brands. As Katz puts it, he went from a low-volume, high-margin business (in property) to a high-volume, low-margin business (in retail). “One is all about the detail and the other is all about balancing the risk that you take,” he says.

Summing up, he says he’s enjoying both the challenge and the reward of using risk management to make a difference.

And as Woolworths’ fortunes start to turn, hopefully that means Katz can work on his beauty sleep.
THE PEOPLE

WE ASKED TWO SENIOR RISK PROFESSIONALS: WHAT ARE THE BIGGEST CONCERNS IN YOUR SUPPLY CHAINS?

I’m concerned about companies not having visibility over their supply chains. I find it intriguing that many companies continue into the unknown without having visibility over key areas such as country of origin, shipment/delivery accuracy, physical security, internal processes & social and environmental accountabilities/ responsibilities.

“I think there is a dichotomy between strategy and operation and we need to stop treating [the] symptoms and instead get to the root cause. As an in-house risk manager for two decades, I find that many companies [don’t] see the forest for the trees, treating operational risks and symptoms instead of strategic risks and the root cause in their supply chain risk management.

“The key [to overcoming this] is to align strategy with risk management by establishing governance, leadership and management in the supply chain with a robust risk assessment regime to treat the root cause and mitigate risk in an accurate and timely manner. The culture of resisting change and maintaining the status quo would be the biggest challenge [to mitigating this]. It is dangerous when we allow apathy and complacency to grow in the organisation and when we assure ourselves that we are ‘good’.

“Recently the Institute of Singapore Chartered Accountants (ISCA) and KPMG conducted a study, supported by the Singapore Exchange (SGX), which showed that ‘many firms sought only to comply with rules but might not see benefits of practice’. KPMG added that ‘we need to see more improvement on the behavioural aspects – the part about people, about the tone of the [risk] culture, and the rationale of why a company should care about risk governance’.”

“Growing in the organisation and when we assure ourselves that we are ‘good’.

Our organisation and the products we produce are dependent on machinery. As such, the associated risks or factors that could curtail or hinder the machinery and equipment from operating at an optimum level is our single biggest concern.

“This risk is strongly linked to other risks. One of these is the disruption to electrical supply. Another is the breakdown of machinery and the time required in getting machines up and running again.

“To manage the risk of electric outages, we have generators that automatically kick in within seconds once there is an outage. We also have regular preventative maintenance scheduled in, which is part of our internal supply chain processes.

“Our supply chain department carries out business continuity planning exercises with simulation scenarios or desktop scenarios. The idea is to go through the thinking process, determine the ‘gap’ rectification required, and work towards addressing the ‘gap’ as part of working towards readiness if a similar situation occurs.

“More training is needed, however, to build up technical staff capability and robust processes built through understanding supply chain and forecasting and to understand the other bottlenecks.

“In managing the risks, it is important for me to understand the risk appetite of the organisation in relation to its business model, strategy and its business execution and, accordingly, from here the need to map all relevant risks that could lead to undesired risk appetite – and to best disseminate them by cascading them to the relevant risk owners and following up, to see how they could effectively manage this with the organisation’s risk appetite with necessary actions.”
THE FUTURE OF SUPPLY CHAIN INSURANCE

When it comes to supply chains, companies have been very much focused on cost and supply chain optimisation. Supply chain risk management is a relatively new topic. However, supply chain risk has been thrust into the limelight following recent natural disasters and disruptions to global supply chains such as the Hanjin Shipping line.

The challenge presented by such risks for companies and their risk managers is how to close this ‘protection gap’. Companies need to find ways to address this gap through either risk mitigation strategies and/or risk transfer solutions. The wide scope of supply chain risks is likely to redefine the role of risk management as an integral strategic function.

Previously, due to the scope and nature of supply chain risk, the insurance options available were limited. The risk was only addressed through the purchase of business interruption insurance, or through the purchase of multiple policies to address the risk (such as marine, business interruption, political risk, trade credit etc). Both options have the potential to create a significant protection gap. Business interruption policies, for example, would in most cases include sub-limits for suppliers’ extensions, only cover the direct/tier-one suppliers and also only cover physical damage losses. Our research shows that a significant number of supply chain disruptions occur below the direct/tier-one supplier level and that many of these are non-physical related in nature.

A good example of this protection gap and the need for adequate cover is perhaps the Japanese tsunami and earthquake in 2011. Many companies had purchased business interruption policies and saw their businesses interrupted, but were not covered as there was no physical damage to their or their suppliers’ premises.

So, what is the solution? What are we seeing now is more demand from customers for a holistic approach to covering supply chain risk. A complaint from risk managers is that business interruption insurance in its current form does not go far enough and can result in coverage and protection gaps from individual policies. This is the reason Zurich created a supply chain insurance solution to cover supply chain risk which can occur anywhere, emanate from a diverse range of causes (both physical and non-physical in nature) and throughout the various supply chain tiers.

There is also a question of relevancy for major insurers. For a lot of large insurers, particularly in the corporate space where companies can have substantial balance sheets, the important question is “if they are big enough to take on the risk themselves, what is the benefit for risk managers?”

The solution we provide, and which our competitors are starting to do also, is around the protection of the supply chain. The way we approach this is to carry out a specific supply chain risk assessment, where we are looking at the potential risks and vulnerability of the supply chain from the critical/strategic suppliers. The critical suppliers are those that have the potential to impact the balance sheet and profitability of the company. This enables the risk manager to present the business case to their executives. Often a company will want to know its vulnerability, how bad it is, what is it going to cost and what are the options to mitigate this?

We look at all of these issues in our risk assessment, which extends over 23 individual supply chain risk factors. We put numbers to all of that, so we are able to quantify the potential risk and even suggest some mitigation measures outside of insurance. The intention of our policy is to mitigate any potential supply chain disruption so it does not have a negative impact on the company’s performance and ability to function – and thereby help to protect the company’s reputation and market share. By closing this insurance protection gap, risk managers are driving a vital piece of risk mitigation for their corporations.

A complaint from risk managers is that business interruption insurance in its current form does not go far enough and can result in coverage and protection gaps. Hassan Karim

Technical underwriting manager, Zurich

then what is the relevance of the insurer? It might not always be around risk transfer, as that may be something they can manage themselves. However, the insurers can provide valuable insight and a holistic view of the risk by bringing in risk expertise across multiple industries and geographies. This in turn can help companies become more resilient and better at managing potential supply chain risk.

So what’s the benefit for risk managers? Supply chain risk is a challenging area that often falls outside the control and remit of the risk management function. A divergence of opinion about the importance of supply chain risk between the risk management function and perhaps the company finance team can lead to challenges finding budget resources to address supply chain risks. Risk managers are often under pressure to reduce their risk management budget. We found that when we spoke to senior executives, usually the CFO, they could see the black hole in failing to obtain this protection. Risk managers need to quantify the impact of a supply chain disruption on the business, articulate what the risk is and present a strong business case to the executive team and board. Doing this successfully also enables the risk manager to start the discussion on other emerging risks.

The solution we provide, and which our competitors are starting to do also, is around the protection of the supply chain.
NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

FIND OUT MORE AT zurich.com/my-zurich

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.