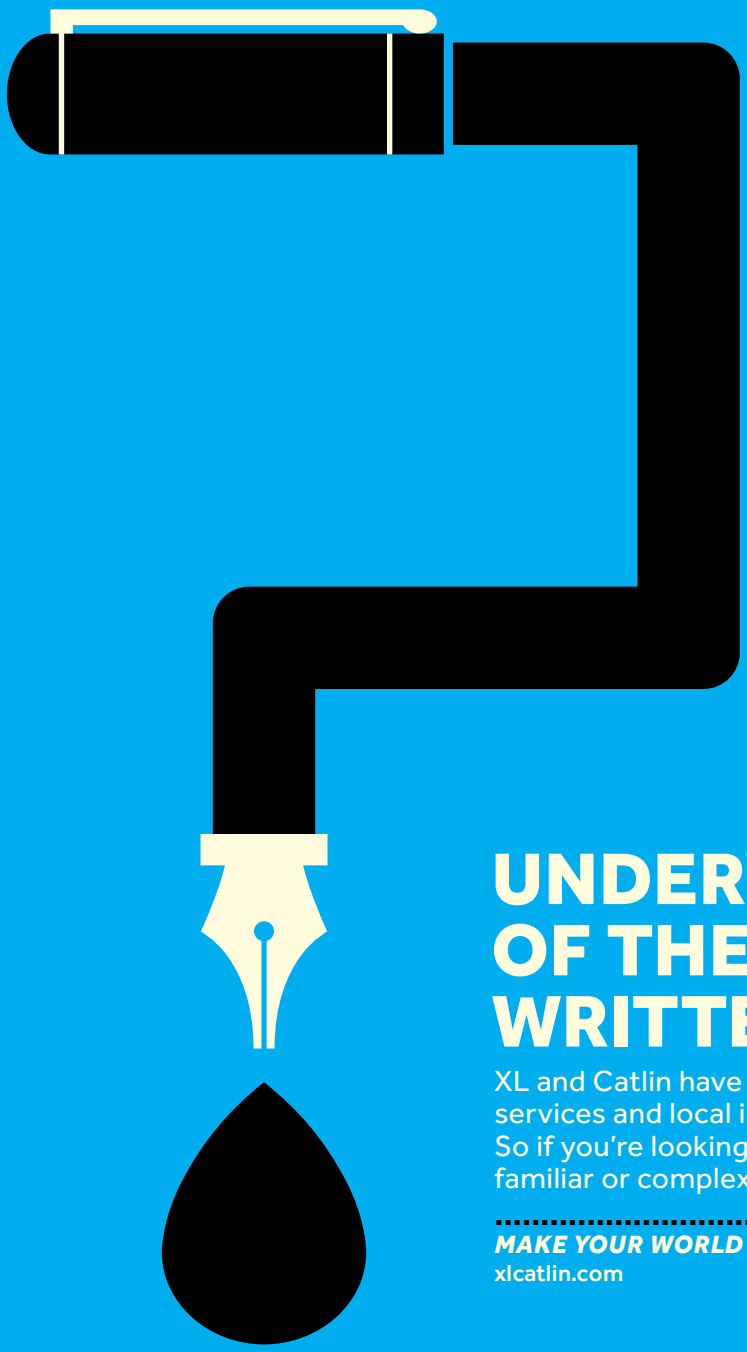
StrategicRISK

RIMS AUSTRALIA 2015

All the highlights from the Rims Australia conference in Melbourne last month, plus *StrategicRISK's* exclusive survey of the top risks keeping Australian risk managers awake at night

By Jessica Reid, *StrategicRISK* Asia-Pacific editor

XL CATLIN



UNDERWRITERS OF THE NOT YET WRITTEN.

XL and Catlin have come together to offer products, services and local insights on a global scale.
So if you're looking for insurance or reinsurance, familiar or complex, **let's chat.**

MAKE YOUR WORLD GO
xlcatlin.com

The third annual **Rims Australia Forum**, on 17-18 August in Melbourne, provided the perfect opportunity to reflect on progress made in advancing the **local risk and insurance professions**

Being relatively new to the risk management sector in this part of the world, one of my first priorities has been to gain an understanding of the industry's dynamics throughout Asia-Pacific and find out what makes it tick.

The Rims Australia Forum 2015 provided me with the perfect opportunity to do just that for the local market.

And from my early conversations and bird's eye view, it's clear that, like many other industries and parts of the world, there are some disparities between the goals and motivations of the different risk management and insurance bodies that play here.

But with so much consolidation and new players in the market, it would seem that now more than ever before there is a need for the risk management industry to speak with one voice. There is a concerted effort by some parties in the wider risk management industry to do this, but there is still some way to go.

However, whichever industry group I speak to, there is one common goal that comes up time and time again: to improve the standing of the risk management profession.

In the event's keynote presentation, Ferma president Julia Graham (page 3 and 14) went so far as to say that if she sees nothing else in her career, it's to see the word 'discipline' replaced with the word 'profession' when it comes risk management.

And there are great strides being made all around the world to see this come to fruition.

For one, the global body for risk management associations is launching an international standard for the certification of risk managers (see page 14-15). It will then be up to the local bodies to implement their own regional versions, with Ferma, Parima and Rims all launching within the next 12 months.

> "There is a common goal that comes up time and time again: to improve the standing of the risk management profession"

Jessica Reid
StrategicRISK

Other highlights throughout the conference were some interesting discussions on everything from the increasing risk of fraud and corruption (page 4) to the challenges over full compliance (page 5).

The main highlight of the conference for me, however, was meeting some of the many faces that make up this dynamic industry.

One of those was the newest board member of Rims Australia: Lend Lease group head of risk and insurance Kevin Bates. Among other things, he shared some interesting insights on the pros and cons of insurance in mitigating cyber and reputation risks – two of the top risks on almost any risk managers' radar today. He's on the record that he's willing to put some skin in the game with some of these risks through his captives, so it will be a fast race for insurers to see who will write the extra layers (see page 6).

Following the conference, *StrategicRISK* also undertook a survey of Australian risk managers. Many thanks to the 50+ risk managers that took part and shared some valuable insights on everything from their top risks to reporting lines and pay. Some of the highlights of the survey appear on the following pages, with the full results to appear in the Asia Risk Report 2015, out in December.

I hope you enjoy this special post-event publication and please do get in touch with any feedback, or any news story that you think needs telling at jessica.reid@nqsm.com.

StrategicRISK
ASIA EDITION

RIMS AUSTRALIA 2015
www.strategic-risk-global.com

Editor, Asia-Pacific
Jessica Reid

Executive editor, Asia-Pacific
Sean Mooney

Editor-in-chief
Mike Jones

Editor, Europe
Kin Ly

Commercial director, Asia-Pacific
Adam Jordan

Head of sales
Tomas Imrich

Senior production controller
Alec Linley

Senior data analyst
Fayez Shriwardhankar

Publishing manager
Tom Byford

Publisher
Jack Grocott

Executive publisher, Asia-Pacific
William Sanders

Managing director
Tim Whitehouse

Email: firstname.surname@nqsm.com

Cover image iStock

ISSN 1470-8167

Published by
Newsquest Specialist Media Ltd
Asia-Pacific office: 3/50 Carrington Street, Sydney, NSW 2000, Australia
tel: +61 (0)2 8296 7611

Hong Kong office: Suite 1003, 43-55 Wyndham Street, Central, Hong Kong

London office: 30 Cannon Street, London EC4M 6YJ
tel: +44 (0)20 7618 3456
fax: +44 (0)20 7618 3420 (editorial)
+44 (0)20 7618 3400 (advertising)
email: strategic.risk@nqsm.com

For all subscription enquiries please contact:
email: william.sanders@nqsm.com

Printed by Warners Midlands Plc

Complaints – Who to contact
StrategicRisk adheres to the Editors' Code of Practice (which you can find at www.ipso.co.uk.) We are regulated by the Independent Press Standards Organisation. Complaints about stories should be referred firstly to the editor-in-chief by email at: complaints@strategic-risk-global.com or by post at Mike Jones, Strategic Risk, 30 Cannon Street, London EC4M 6YJ.

It is essential that your email or letter is headed "Complaint" in the subject line and contains the following information:
- Your name, email address, postal address and daytime telephone number.
- The newspaper title or website, preferably a copy of the story or at least the date, page *number or website address of the article and any headline.*
- A full explanation of your complaint by reference to the Editors' Code.

If you do not provide any of the information above this may delay or prevent us dealing with your complaint. Your personal details will only be used for administration purposes.

If we cannot reach a resolution between us then you can contact IPSO by email at complaints@ipso.co.uk or by post at IPSO, c/o Halton House, 20-23 Holborn, London EC1N 2JD.

NEWS

Scenario planning essential for intangible risks

Ferma president Julia Graham tells Australian risk professionals that their **skillset needs to change to keep up** with the new reality of global and intangible risks

Scenario planning and modelling will become an essential tool for risk managers in mitigating intangible global risks, according to Federation of European Risk Management Association (Ferma) president Julia Graham (pictured, right).

Speaking at the RIMS Australia 2015 conference in Melbourne, Graham said "scenario planning was going to become a much more common tool that risk managers need to have in their toolkit" thanks to the increasing trend for intangible risks such as cyber, fraud and reputation to top global risk management surveys.

"The new normal is businesses are becoming more global, the pace of change is increasing, we're more dependent than ever on technology, there's greater connectivety and risks are more intangible. The balance of risk therefore on the boardroom table is changing," Graham said.

"Not only are these risks hard to manage, they're multi-dependent and this is a reflection of a fast and moving and more dynamic world that we're living in.

"Most risk managers focus on risks that are controllable. It's a natural thing to do – focus on the things in front of you which you have a bit more comfort in being able to do something about."

Global risks, however, are much harder to control and quantify. But they are increasingly the focus of boards around the world.

"The rising tide of board responsibility says that the buck stops with them for managing all risks that might affect their organisations – and that includes global risks. So [boards are] unclear on what to do these global risks but they're actually responsible for managing them."

> "The rising tide of board responsibility says that the buck stops with them for managing all risks that might affect their organisations and that includes global risks"
>
> **Julia Graham**
> Ferma

This is where effective risk management can help.

Graham said risk managers should not try to "intellectualise" the global risks, but focus on their potential impacts and outcomes.

"Don't try necessarily to manage the risks you can't do anything about – try to focus on some scenarios, for example, of what these risks might mean for your business.

"There's quite an art to doing scenarios well and I certainly think that's an area that risk managers can build up their skills on to help their board try and look over the horizon and look to the future," she said.

But Graham warned against focusing on intangible risks at the expense of the tangible.

"You really need to work very hard with your boards to keep the tangible [risks] on the table because they haven't gone – they've just been pushed slightly out of the way by things that are more likely to keep people awake at night than catastrophes of a physical kind.

The key is for boards to focus on crisis management.

"What we're trying to say to the board is as the risks become intangible you should focus your eye a little bit less on insurance for some of these [risks] but always have your eye on crisis management.

"Don't always think that a crisis is about a fire, a flood or a kidnap; it could be an issue that involves fraud, an issue that involves potential reputation harm – all sorts of things where you might want to invoke crisis management from different sorts of events which are much more like those global risks."

NEWS

Corruption risk 'has never been greater'

As **bribery and corruption risk rises** across Asia-Pacific, there is an expectation from employees, shareholders and customers that such risks are mitigated

Despite the risk expectations around the threats attached to bribery and corruption, many organisations are failing to cover themselves in terms of policies and employee training.

EY partner, fraud investigation and dispute services, Campbell Jackson said the firm's 2015 Asia-Pacific Fraud Survey provided a startling insight into the corporate bribery and corruption landscape.

Speaking at the RIMS Australia conference in Melbourne, Jackson said "there is no good news for corporates. The risk is just getting greater and greater".

The survey of 1,508 interviews in 14 Asia-Pacific territories found that business success is being challenged by three aspects: increasing regulation, slower than expected economic growth and stronger local anti-corruption enforcement.

"The really interesting aspect in the survey is the expectation requiring strong and robust controls around anti-bribery and corruption," Jackson said.

"These expectations come from staff members who want to see an ethical culture and a robust environment.

"The thing which really shocked me in the survey was that eight out of 10 people surveyed said they would be unwilling to work for a company involved in a bribery and corruption event, or with a history of bribery and corruption."

According to the survey, some 45% of companies do not have a whistleblowing hotline, one in four companies do not have an anti-bribery and anti-corruption policy, and a further 40% do not provide any training around anti-bribery and anti-corruption policies.

"This is all astounding considering the risk attached to bribery and corruption," Jackson said.

"The risk has never been greater. People expect a robust programme to be in place, but organisations are still not doing enough in the basic areas of anti-bribery and anti-corruption risk, and mitigation," he said.

Risk manager solutions

When it comes to the role that risk managers play in mitigating bribery and corruption risk, Jackson said communication is key.

"If you are not talking to your employees about the company procedures, mechanisms and controls, then you are not address the risk," he said.

"If ever a risk manager was going to do anything, now is the time. This is not scare mongering, the risk has never been greater."

Jackson said a bribery and corruption event not only has ramifications for the share price and value of the organisation, but the reputation and integrity of management.

"There is an expectation at a corporate level that risk managers should be across bribery and corruption risks, but this is not a one-size-fits-all exercise," he said.

"Certainly, from experience, it requires consideration and a clear strategy to do what is important at the right time and pick off the low-hanging fruits, and strengthen and customise their ethics and corruption programme.

"There is no point taking some 'off-the-shelf' risk management solution and embedding it if you are not going to promote the programme, customise it and actually think about it periodically.

"Yes, this risk is on risk managers' radar, but they are probably not doing enough currently," he said.

In terms of how risk managers can successfully communicate bribery and corruption risks to employees and management, Jackson said risk managers must "tell the story".

"There are high profile examples of bribery and corruption everywhere. Profit from the misfortune of other organisations – look at what they have gone through in terms of an bribery and corruption event, look at the impact on the organisation, including the resources it consumes, look at the impact on the share price and look at the overall perception of the customer base.

"That is before you even get to the financial implications."

THE SEVEN STAGES OF MANAGING BRIBERY AND CORRUPTION RISK

Jackson said risk managers can mitigate bribery and corruption risk by following seven steps:

1. Assessing risk at a granular level
2. Developing an anti-bribery and corruption programme that is robust and dynamic
3. Defining and implementing policies that are clearly articulated and digestible by employees and management
4. Build, enhance and operate effective internal controls through the use of technology and data analytics
5. Training and education
6. Monitoring and evaluation
7. Review, realign and report

"No industry is immune from bribery and corruption," Jackson said.

"We are seeing an increasing trend in financial institutions but, ultimately, the opportunity to influence an outcome [through bribery and corruption] is widespread.

"In short, you cannot stick your head in the sand anymore. The expectation is too great," adds Jackson.

NEWS

Full compliance 'unnecessary' in over-regulated world

Why a risk-based approach to compliance involves **not meeting all regulatory obligations** around **occupational health and safety**

The occupational health and safety regulatory environment is vast and overbearing, so attempts to be 100% compliant can hinder best practice risk management.

Michael Toomer, partner and head of occupational health safety and security, Asia-Pacific, at law firm Norton Rose Fulbright, said people are obsessed with regulation and full compliance.

"We have an obsession around talking about law and compliance," Toomer said at the Rims Australia conference in Melbourne.

"We need to start looking at regulation and compliance a little bit differently.

"In relation to every aspect of our operational requirements, we take risks. Those are measured risks. But when it comes to law we have zero tolerance – we think we must be fully legally compliant."

Toomer explained that health and safety laws are about 700-800 pages long, just in acts and regulations alone. Then there are company codes of practice too.

"Is it desirable to comply with all laws? Should we actually be building in risk management in our legal compliance strategies?" he asked.

"When you think of those 700 to 800 pages of law in relation to safety, some of them are quite valid. You have got some very specific regulations, dealing with high-risk activities which need to be regulated. Then there are requirements which can be considered nothing more than administrative compliance.

> "Is it desirable to comply with all laws? Should we actually be building in risk management in our legal compliance strategies"
>
> **Michael Toomer**
> Norton Rose Fulbright

"There is a lot of red tape in terms of how you set-up a committee for health and safety purposes, how often it meets, how it records minutes, and a whole range of reporting and recording-keeping requirements, plus a whole other world of transactional-based regulations," he said.

Toomer said many firms attempt to achieve a "nirvana of 100% legal compliance".

"You cannot meet all your obligations effectively and when you try to mobilise your procedures and deal with the vast array of obligations as if they are all of equal importance, then you are going to have a blow-out in the size of your policies and procedures.

"The more that you expect people to do, the less likely they are to do it.

"It is ironic because that obsession to be 100% compliant is what is driving us not to be compliant due to the burdensome system we have built," he said.

Legal compliance

Toomer suggested that firms should take a "risk-based approach" to legal compliance.

"For all the talk of productivity, compliance and law, the actual reality of workplace health and safety is that no inspector comes knocking on your door unless you have had a significant incident. That is usually a fatality or serious near-miss," he said.

"If you spend all your time preventing that event happening, in all likelihood no-one will come knocking on your door to ask you about compliance.

"So rather than being obsessed by the law, do what the law is intending for you to do – protect the health and safety of your people," he said.

Dr Sarah Jones, group manager for road transport compliance at Toll Group, added that the biggest challenge in transport and logistics risk management is ascertaining what exactly is supposed to be done in a legal and regulatory sense around health and safety.

"Compliance is extremely difficult and there is a vast depository of legal risk obligations. The majority of companies in our industry are small businesses and only have one truck," Jones said.

"So I pose the question: is compliance even possible for the average individual?"

Andrew Lewin, vice president of safety and security at BHP Biliton, said there had been an evolution from full compliance to using risk management as an optimisation tool.

"In the past it seemed like you had to manage all your risks and that drove a lack of optimisation," Lewin said.

"It is impossible to manage every risk to the same level. You really need to understand what are your biggest risks and optimise them.

"Having legislation which drives you to manage all of those risks just creates issues when you are trying to prioritise risks," he added.

PROFILE

Safety first: managing risk at Lend Lease

From running terrorism simulations to debating the **merits of cyber insurance**, no two days are the same for Lend Lease group head of risk and insurance **Kevin Bates**

On 15 December 2014, Lend Lease chief executive Steve McCann called a crisis meeting. It was not a drill. A lone gunman had entered a café near their head office in Sydney, Australia, and was reportedly holding 18 people hostage.

The event would become known as the 'Sydney Siege' and end after a 16-hour standoff, which left three people dead.

Lend Lease group head of risk and insurance Kevin Bates was responsible for coordinating the response to the crisis.

"Within 30 minutes of the crisis meeting we'd booked a fleet of buses and we'd chartered two ferries and we just kept them all running until there wasn't another person arriving to get out of the city," he says.

About 600 staff used the chartered transport to safely get out of the CBD that afternoon.

Within an hour of police arriving on the scene, emails and text messages were being sent to all Lend Lease employees to keep them updated as the event progressed.

"I'm particularly proud of [how the event was handled]. We train hard in these simulations and when it happens it's good to know that it works," Bates says.

Talking to *StrategicRISK* at the RIMS Australia conference in Melbourne, Bates has just finished conducting another terrorism simulation drill. This time in Singapore.

> "When I'm talking about business resilience, I'm looking at how we can keep our future leaders satisfied, performing and engaged"
>
> **Kevin Bates**
> Lend Lease

It's just one of the many activities on the risk management calendar at Lend Lease, a multinational project management and construction firm. And from multi-billion dollar urban redevelopments to small-scale corporates refurbishments, Bates and his team around the world are responsible for managing the risk and insurance of every project.

It's no surprise then that much of Bates's time is spent travelling.

Most recently the trips have been to deliver the news of the risk and insurance team's restructure, which has seen significant changes to roles and reporting lines.

"We will now be running efficiently and we will have the correct people in the correct roles," he explains.

Despite the restructure, it's clear that Bates is passionate about the business and the people within it. When asked how he views the company's resilience, it's not the usual risk manager reply about business continuity, crisis management and enterprise risk management.

Instead, he says, it's focusing on people.

"When I talk about business resilience, I'm looking at how we can keep our future leaders satisfied, performing and engaged, and what can we learn from them in order for us to do our jobs better," he says.

"I get calls from recruiters every other week asking me about CRO and COO roles that are available. But instinctively

I'm wed to the business; I believe in what we do. I believe we're making a difference and I feel part of that.

"So what is my role in trying to make the next generation of Lend Lease leaders believe that they're part of it as well and their contribution is critical to our growth and our success?"

The cyber debate

If people risk is one of Bates's top priorities, cyber is not far behind.

"I don't have my blindfold on; I don't think we're a boring company that no one's interested in.

"People are in – they're in everyone's systems – it's a question of why they're in and what are they doing while they're in there," he says.

And like most of his peers, Bates has insurers knocking on his door trying to sell him cyber protection. But he's not likely to be answering any time soon.

"I just can't see what a [cyber] insurance product is going to give me. I can't see what they can write that I've lost," he says, explaining that insurance can't replace stolen personal data, bid documents or design details, for example. Plus, certain losses from a cyber event at Lend Lease would be covered under the company's other insurance policies.

Instead, when it comes to cyber, Bates is focused on ensuring the company's security systems are robust, that business continuity plans are in place should the networks go down, and that staff are trained to be the fist line of defence as a "human firewall".

So insurers looking to win Bates over on cyber insurance might be fighting a losing battle. They'd have more luck with a product for another of his top risks: reputation. Bates says he's yet to find a policy that gives him the coverage he needs.

Reputation insurance products are still in their infancy, with most policies typically covering the costs of public relations and legal fees that arise out of an event. But those are costs that Bates is willing to take on the balance sheet should they arise.

What he wants is an insurance product that protects Lend Lease's share price and future earnings should the company's reputation take a hit.

"So if my share price is sitting at $15.5 and there's an event, it drops; there's a correction period and we accept that – it might be three months, it might be six months – but we agree that on correction period. In a sense then there's a parametric trigger. So if I have lost more than 'x'

percent of my share value, thereby market cap, [the insurer] pays that market cap."

But for a company with a market cap of about $8bn, Bates is yet to find an insurer that's willing to write the risk.

He is having "extensive conversations" with one carrier, however. And self insurance through one of Lend Lease's two captives is also on the table.

"That's the part I'd love to see insurers get a lot more creative around. I'd be happy to take some of that [risk] and put it in a captive; I'd put some skin in the game.

"It's those levels of creativity and engagement that I'm excited about seeing and at the moment I'm not seeing. People don't have the appetite for it and there isn't the capacity."

So where does Bates believe the innovation come from?

"It's going to come from the intelligent carriers who have built strong relationships with clients," he says.

Country challenges

While people, cyber and reputation are risks that affect the entire business, there are also myriad of operational and region-specific challenges that Bates and his team have to manage.

Regulatory risk in China and political risks in Malaysia, for example.

But whichever market Lend Lease operates in, Bates says they have a "zero tolerance" for bribery and corruption.

"We are a completely compliant business and we will absolutely not encourage, condone or authorise anything that is illegal," he says.

It's a noble stance, particularly when corruption is a key issue in some of the markets that Lend Lease operates in.

China, for example, scored 36 out of 100 on the corruption index last year, where zero is corrupt and 100 is clean.

"China is a core market for growth for sure but we're not in the business of competing with local players there," Bates says, adding that the group will only work for other multinationals in the country with the same safety standards as their own.

"If we cannot guarantee the safety of a project, we're not going to play in it," he says.

In fact, safety is one of the reasons that Lend Lease has pulled out of certain regions over the years, including Indonesia, India, Brazil, Argentina, Peru and Chile.

"In those areas the local subcontracting market is perhaps not as mature as it is in Australia, for example, and you'd find that you'd give them all your PPE (personal protection equipment) and they'd just sell it off."

In other emerging countries, the high safety standards have paid off.

In Malaysia, for example, contractors were resistant to wearing eye protection because they would steam up in the humidity. To solve the problem, Lend Lease put in eye wash stations and gave them anti-fog.

"Now they're taking that anti-fog to new projects because they've seen a stray nail come flying out and take someone's eye out. They've seen really traumatic things that we've now given them the tools to prevent," Bates says.

"It's enormously satisfying but the journey's never going to be complete in that. It's about the hearts and minds. You can tell people what to do and attempt to make them compliant but until you have them thinking and believing and feeling it for themselves you'll never quite get there."

It's a journey that Bates has been on since he joined the Lend Lease legal team 11 years ago. Like many of his peers, a job in risk management was not his original plan.

In 1994 Bates had the world at his feet: a spot in the Scottish swimming team, a scholarship to a US university and place at the Commonwealth Games. But fate intervened during a high school rugby match, when he was "nuked" by a disgruntled opposition player and left with a knee injury that took him out of the sport for 18 months.

So with a swimming career off the cards, Bates turned his focus back to his studies and completed a Bachelor of Laws with honours from the University of Dundee. From there he moved to Edinburgh to complete his two years of legal training, before taking a role in London as a corporate lawyer for Tite and Lewis.

But law was never quite for him. Fast forward to 2004 and he was looking to leave the legal profession altogether. Instead he took an in-house legal role at Lend Lease, based in Singapore, before moving into risk management role with the firm in 2007.

So what's next for Bates and the risk and insurance team at Lend Lease?

Aside from helping to keep and promote future leaders within the business and embedding in the new team structure, he's got a few KPIs of his own.

For one, he needs to come up with at least two non-traditional risk transfer or financing solutions that will help Lend Lease achieve its 2016-20 strategy.

So any insurer that can help him with that, you know who to call.

SURVEY: TOP RISKS

Australian risk managers rate their top risks

But the **top perceived business risks** have not yet translated into financial losses

Australian risk managers have rated economic conditions, targeted cyber attacks and damage to reputation as the top three risks to their businesses.

This was one of the key findings of the Australian segment of the *StrategicRISK* Asia Risk Survey, completed this month.

But these top risks are not necessarily reflective of the top losses.

According to the survey, injury to workers is the number one loss event in financial terms (as chosen by 31% of risk managers). But this risk event came in eighth on the risk radar.

Economic conditions came in second for losses at 29%; with natural catastrophes, fire or damage to property, and fraud and corruption all equal third at 27%.

Damage to a company's reputation – the third top perceived risk – only resulted in a financial loss for 10% of respondents.

But AIG Australia chief executive Noel Condon said there was a significant link between the top risks and claims experience.

"These risks not only drive losses but also influence premium rates. The concern about economic conditions is certainly closely linked to actual losses – the GFC certainly pummelled our loss ratios," he said.

"Contractual risk and injury to workers have also resulted in actual insured losses. Many of the other listed risks represent concerns that may give rise to financial loss in the future rather than exposures that have resulted in insurance claims. For cyber risk, we expect to see increasing claims activity as cyber threats come to bear."

Aon Risk Solutions managing director global and corporate Jason Disborough agreed. He said: "From our experience the number of Australian companies that are purchasing cyber insurance has increased exponentially over the past 12 months and we expect this trend to continue."

Indeed, Scentre group risk director Eamonn Cunningham said he would have expected 'cyber' to top the list, and 'terrorism' and 'failure to innovate' to be rated higher up the list of concerns.

"Given the spectre of increased business complexity, the rapidly changing pace of technology [and] increased competition, those that fail to innovate put their own competitive position in jeopardy," he said.

AIG's Condon said it was important that the risks weren't viewed in isolation.

"We've found that one of the key concerns about cyber risk is the associated reputational risk, over and above the financial risks, as the damage to trust in a brand following a cyber breach can be devastating."

Seven West Media head of risk and audit Mark Wilson also stressed the importance of brand reputation.

"There is no uncertainty when it comes to reputation. Your survival absolutely depends on it," he said.

But Wilson argued that "reputation damage" itself is not a risk at all. Rather, he said, it is a consequence of failing to manage other risks.

"'Brand' is the promise the organisation presents to its customers and brand damage would be caused by a failure of the marketing function. Conversely, 'reputation' is the perception that customers, investors and other stakeholders have of that organisation. It's a consequence of an organisation's actions and inactions, ethics and motivations. It's absolutely essential to an organisation's long-term survival," he explained.

In addition to the risks that made the top 10 in the *StrategicRISK* survey, EnergyAustralia risk manager and Rims Australia president Brad Tymmons said he expected some new risks to rate in the top 10 soon, including "changing consumer behaviour, social media and climate change".

BIGGEST CONCERNS FOR AUSSIES

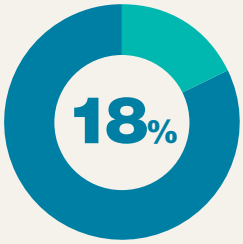
Methodology

Respondents were asked to rate 35 different risks by the likelihood of each one occurring in the next 12 months and the estimated financial impact this would have on their business. They were asked to rate each political risk event by both 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).

To plot the scatter graph, the average likelihood and financial impact score was calculated for each risk and plotted along the x-axis and y-axis, respectively. The scatter graph also displays the average likelihood and financial impact scores across all risks. Those risks in the top right hand corner of the graph were rated by respondents as having above-average likelihood of occurring in the next 18 months and were deemed to have an above-average financial impact if they were to occur.

To identify the risks of highest concern (that is, those most likely to occur with the highest financial impact) a combined average score was calculated for both likelihood and financial impact for each risk and ranked in order of size. The higher the score, the more likely a risk is to occur and have a high financial impact.

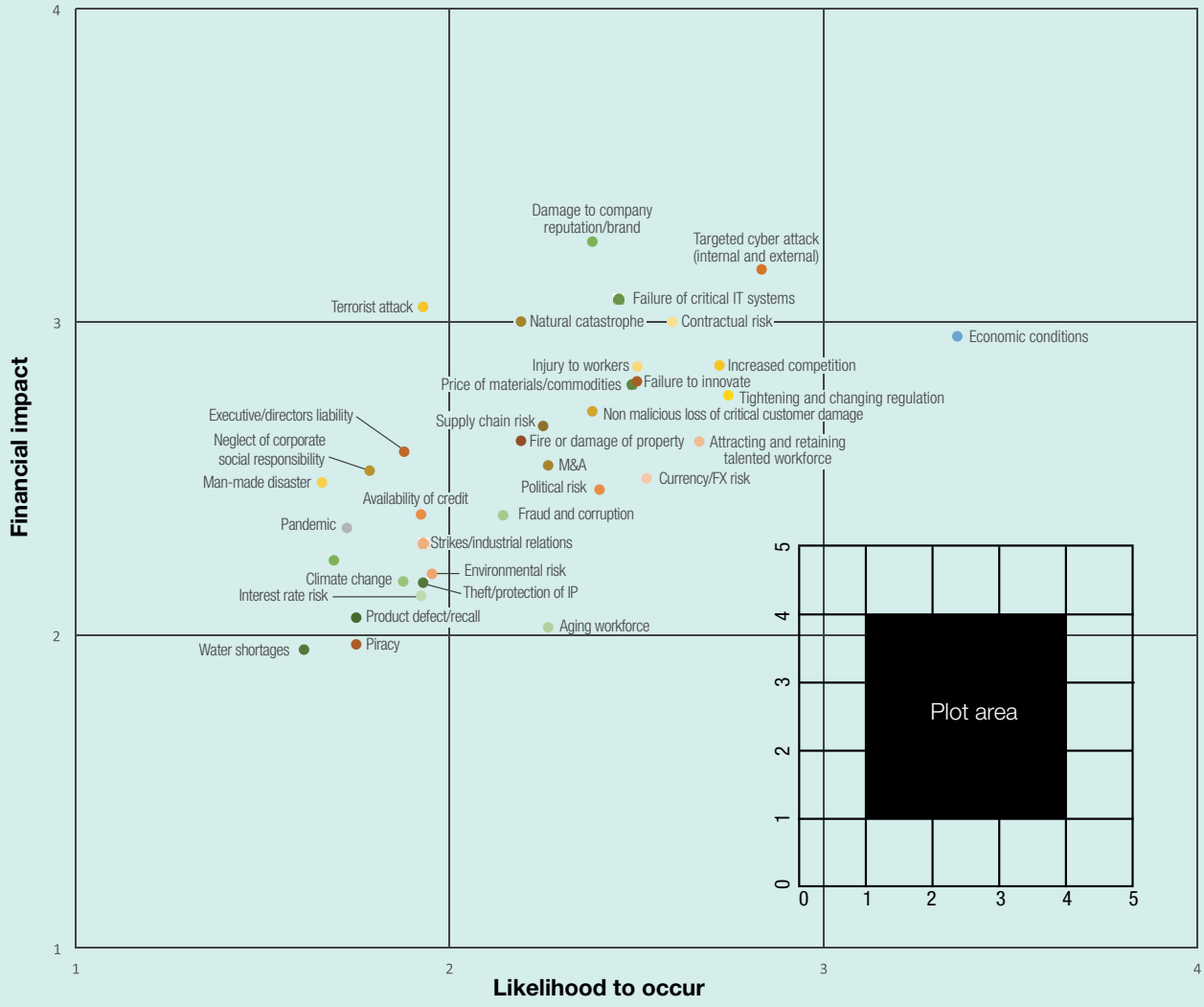
BIG NUMBERS



Number of Australian risk managers earnings $250,000 or more

AUSTRALIAN RISK MANAGERS RATE THEIR TOP RISKS

Economic conditions, cyber attack and reputation top list of concerns



RISK	OVERALL
Economic conditions	3.16
Targeted cyber attack (internal and external)	3.00
Damage to company reputation/brand	2.82
Contractual risk	2.80
Increased competition	2.79
Failure of critical IT systems	2.76
Tightening and changing regulation	2.75
Injury to workers	2.68
Failure to innovate	2.65
Price of materials/commodities	2.64

RISK	LIKELIHOOD
Economic conditions	3.36
Targeted cyber attack (internal and external)	2.83
Tightening and changing regulation	2.73
Increased competition	2.72
Attracting and retaining talented workforce	2.67
Contractual risk	2.60
Currency/FX risk	2.53
Injury to workers	2.50
Failure to innovate	2.50
Price of materials/commodities	2.49

RISK	SEVERITY
Damage to company reputation/brand	3.26
Targeted cyber attack (internal and external)	3.17
Failure of critical IT systems	3.07
Terrorist attack	3.05
Contractual risk	3.00
Natural catastrophe	3.00
Economic conditions	2.95
Increased competition	2.86
Injury to workers	2.86
Failure to innovate	2.81

SURVEY: REPORTING LINES

Risky reports

Australian risk managers are **getting a foot in the door with chief executives** and other c-suites, but does that mean they are engaged in a risk-aware culture?

It's often said that the culture of an organisation is shaped by the worst behaviour that its leader is willing to tolerate.

If that is true, then where should the risk function sit to best promote and embed a risk-aware culture?

EnergyAustralia risk manager and Rims Australia president Brad Tymmons said that a firm's risk culture starts from the top and that the most senior risk/insurance person in a firm should be reporting in to someone within the c-suite.

"If not, you would definitely question whether the valuable risk management insights are being analysed to drive decision-making for the long-term sustainability of the company," he said.

But according to the results of the Australian segment of the *StrategicRISK* Asia Risk Report Survey, only 16% of Australian firms' most senior risk/insurance professional report into the chief executive.

Scentre group risk director Eamonn Cunningham said this figure needed to improve "if that is what it takes to have a permanent seat at the table when the enterprise's risk committee or board audit and risk committee meets".

The vast majority of respondents – 30% – said the most senior risk professional reports into the chief financial officer (see table, right).

Seven West Media head of risk and audit Mark Wilson said a lot of senior risk professionals benefit from having a reporting line direct to the audit and risk committee.

> "It's the chief executive and his or her executive team that define risk culture. Not enough can be said about the importance of tone at the top"
>
> **Mark Wilson**
> Seven West Media

"While it may not work for every organisation, there are some real benefits to be derived from being independent of the management team who are responsible for managing key business risks. For one, it certainly helps avoid the misconception that the risk team does it all!"

Two-third of respondents rated their board/senior management's commitment to embedding a risk culture within their firm as 'high' or 'very high'. That leaves one-third of respondents fighting an uphill battle to improve their plight.

But Wilson argued that it was not the sole responsibility of the boardroom to set a company's culture.

"Certain expectations may be set, but it's the chief executive and his or her executive team that define risk culture," he said.

"Not enough can be said about the importance of tone at the top."

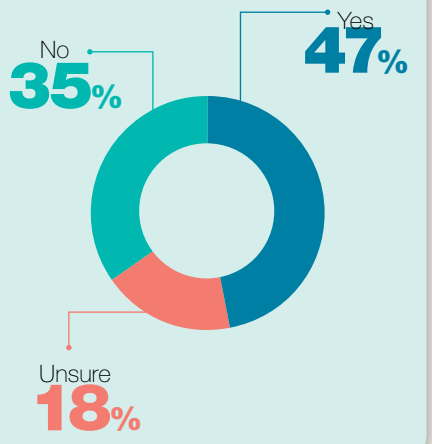
Indeed, most respondents (42.86%) said it was the responsibility of the risk management function to set the risk culture. This was closely followed by the executive board (40.82%) and the chief executive (34.69%).

STATEMENT OF INTENT

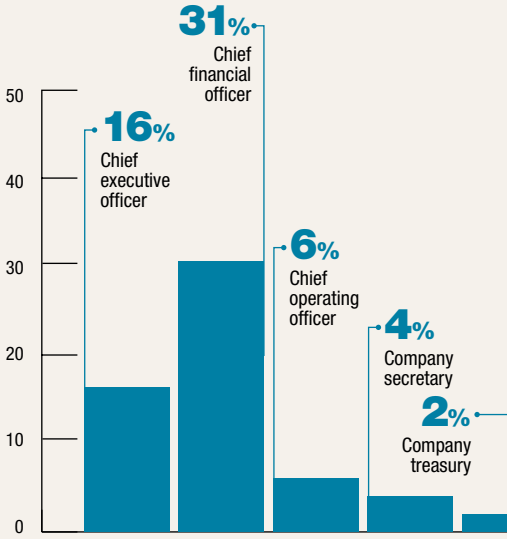
AUSTRALIAN RISK MANAGERS RATE THEIR FIRMS

RISK TARGETS

Is risk management a KPI for senior management in your firm?



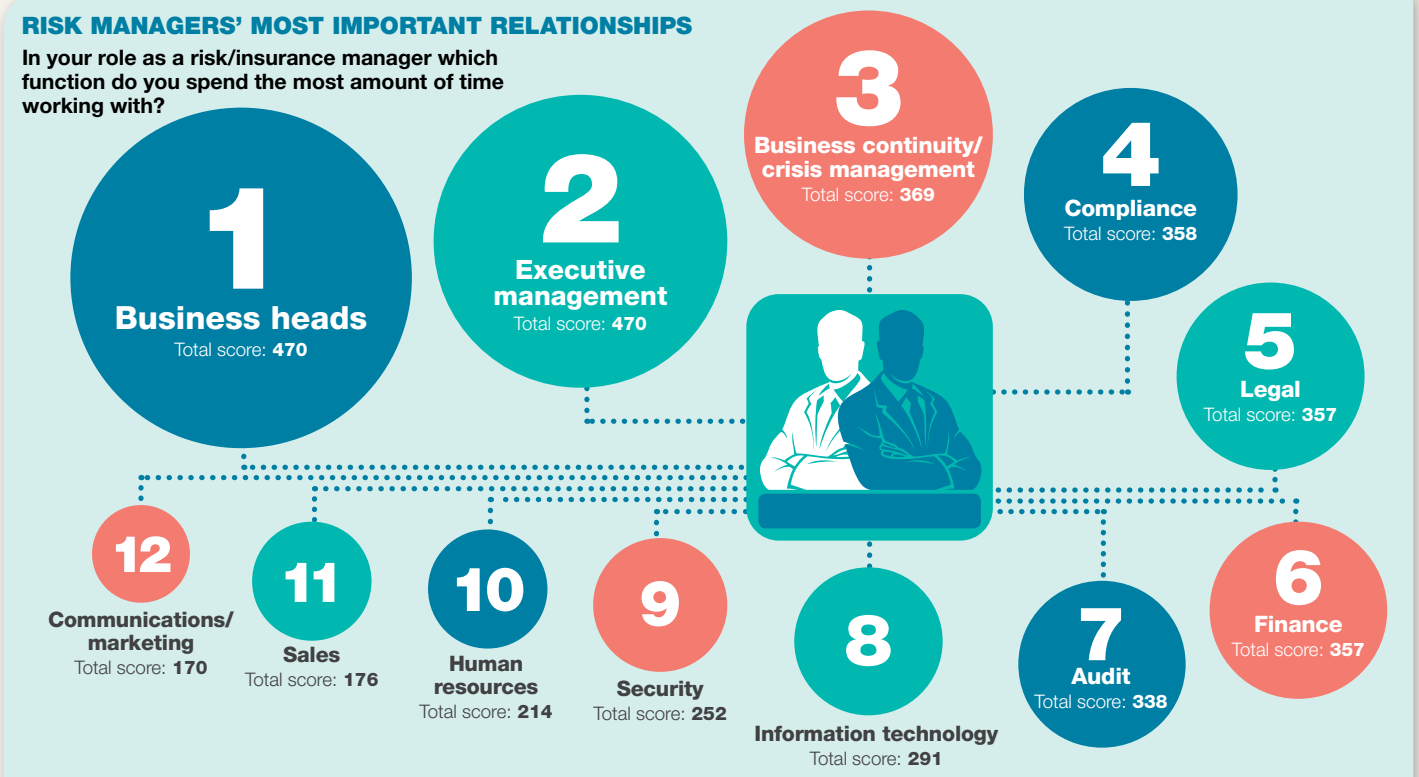
REPORTING LINES OF RISK



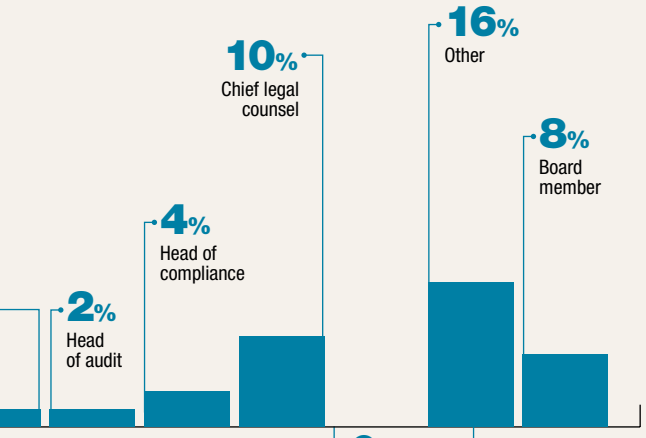
> Firms that fail to innovate put their own competitive position in jeopardy"
>
> **Eamonn Cunningham, Scentre Group chief risk officer**

RISK MANAGERS' MOST IMPORTANT RELATIONSHIPS

In your role as a risk/insurance manager which function do you spend the most amount of time working with?

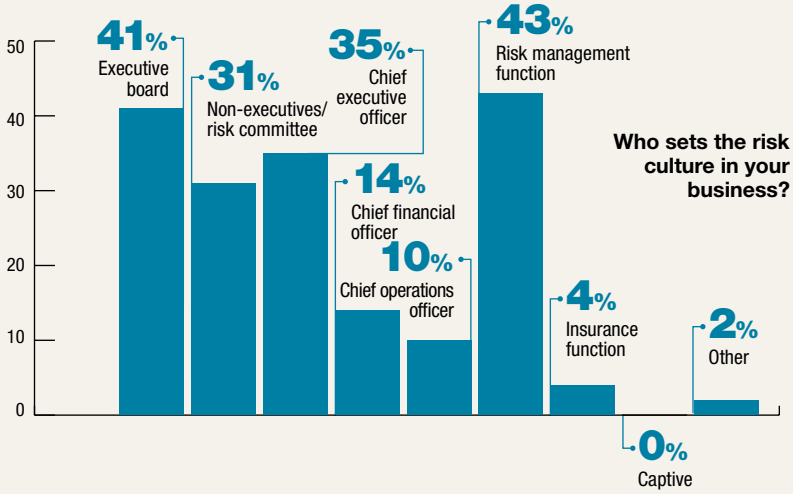


Who does the most senior risk/insurance professional in you organisation report to?

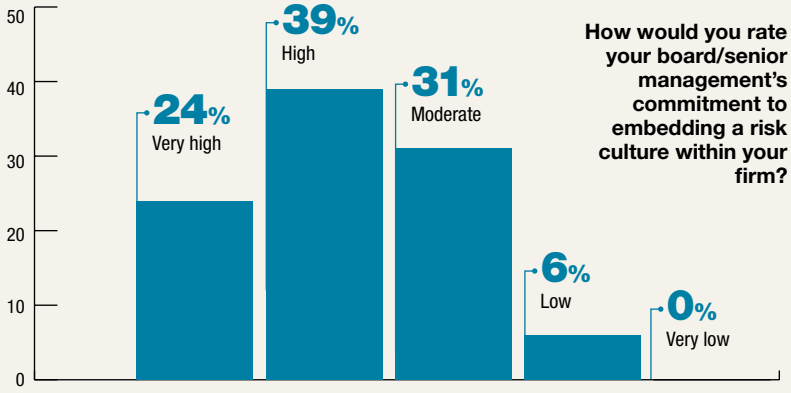


OTHER
General financial controller, director safety environment quality risk, head of region – who is also a board member, general manager castes risk and management systems, head of human resources

Who sets the risk culture in your business?



How would you rate your board/senior management's commitment to embedding a risk culture within your firm?



SURVEY: TRAINING AND EDUCATION

Global risk management association to set certification standards

Rims, Ferma and Parima all understood to be launching **risk management certifications** within 12 months

The global body for risk management associations is to launch an international standard for the certification of risk managers.

The International Federation of Risk and Insurance Management Associations (Ifrima) will oversee the global risk professional framework and code of conduct, which will then be implemented by local risk manager associations.

Ferma, Parima and Rims are all understood to be in advanced discussions about launching their regional versions, which will be based on the international governance standards but with variations for the local operating environment.

Ferma president Julia Graham said this was the first time that a global benchmark had been set for risk managers.

"This is the way that the profession is converging and raising its game," she said.

But Graham stressed that Ferma was not turning into an examination body.

"What we're doing is taking details of an individual's professional qualifications, academic qualifications and experience – validating those if we feel we need to – and putting people through a process of application at a regular and advanced level."

Ferma's model, which others are likely to emulate, will involve various risk management certifications – which are currently being piloted – accreditation for professional academic bodies, and licenses for groups that provide ongoing professional development.

The full details of the model will be announced at the Ferma conference in Italy, in October.

Parima president Franck Baron said the group was "very serious about professional certification" and was in discussions with Ferma to ensure that any certification it launches is compatible.

Rims president Rick Roberts also said the association was looking at launching a risk management certification next year.

Roberts also announced that Rims would soon launch its new information network tool, Opis.

"What Opis will allow you to do is save time searching for content you need, connect you with others that are interested in the same topics no matter where in the world they're located, and bridge knowledge across experience levels and generations," Roberts said.

The announcements are part of a growing global push to improve the standards of risk management and recognise the increasingly important role it plays in achieving strategic business objectives.

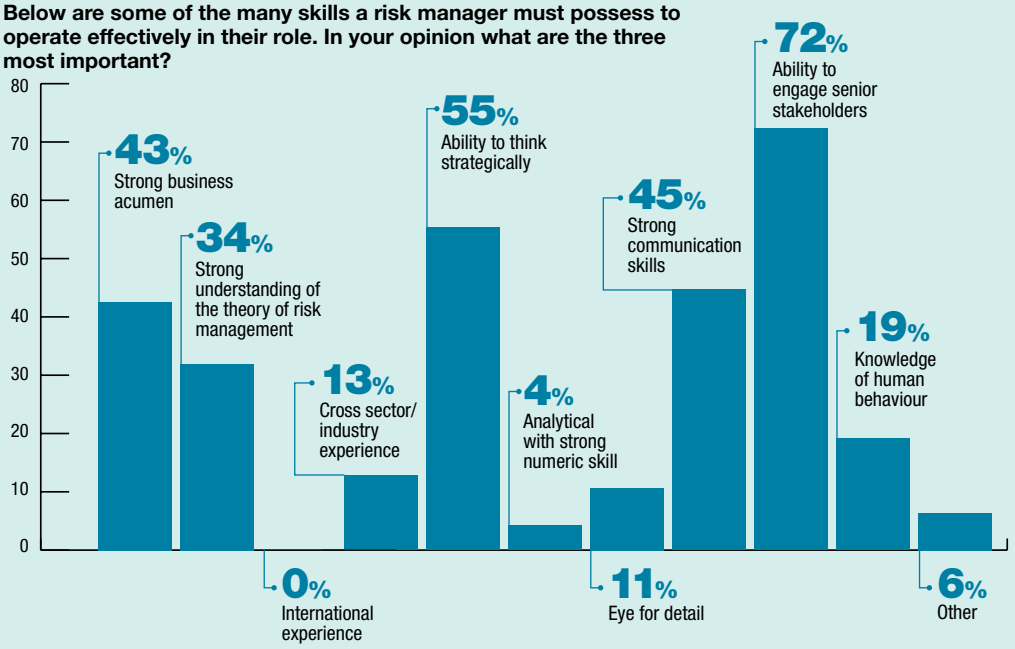
Graham said: "Well risk-managed businesses make more money, it's as simple as that.

"We're now in a new era of revolution. But the difference is that the 'new normal' is more sophisticated and more challenging … so are we as risk managers up to that new world? In some cases, absolutely, and in other cases, possibly not.

"If we're going to take this journey and be the type of risk managers for tomorrow's businesses I think risk managers have got to change. We've got to change our skillset; we've got to change how we use that skillset. We need to up our game."

SKILLS FOR SUCCESS

Below are some of the many skills a risk manager must possess to operate effectively in their role. In your opinion what are the three most important?



RISK BODIES WITH AN AUSTRALIAN PRESENCE

IFRIMA

The International Federation of Risk and Insurance Management Associations (Ifrima) is an "association of associations". It is the international umbrella organisation for risk management associations, representing 20 organisations and more than 30 countries.

Its primary objective is to provide a forum for interaction and communications among risk management associations and their members. The association says its priority this year is the implementation of its recently created International Risk Management Education and Competency Framework and international code of conduct principles, which local member associations will adopt and manage.

RIMS

The Risk and Insurance Management Society (Rims) brings networking, professional development and education opportunities to its membership of 11,000 plus risk management professionals located in more than 60 countries.

Rims president Rick Roberts says Rims has a variety of learning experiences, including online webinars and its annual conference and exhibition. "Over the course of the next 12 months, Rims will explore ways to strengthen its international networks, its network of rising risk professionals and internal network," he says.

"Rims has cemented itself as a source for information regarding the procurement of commercial insurance, and is now paving the way for leading insight on enterprise risk management and strategic risk management applications and opportunities."

PARIMA

The Pan-Asia Risk and Insurance Management Association (Parima) is the professional membership association for the development of risk and insurance professionals in Asia, which claims to be "by risk managers for risk managers".

Parima chairman Franck Baron says the organisation differs from others as the composition the board and members offers a blend of Asian cultures and Western philosophies.

"Seminars and workshops are organised throughout the year to share the best practices between peers and gain knowledge on latest developments," adds Baron.

"Our focus moving forward is the continuous development of our local footprint across all Asia-Pacific countries and the successful launch of our professional certification initiative across the region."

ANZIFF

The Australian and New Zealand Institute of Insurance and Finance (Anziff) is the membership body and provider of education, training and professional development services to the insurance and financial services industry in Australia, New Zealand and the Asia-Pacific region.

Its education and training includes formal qualifications in 10 different insurance and risk courses, workshops across a range of foundation, intermediate and advanced subjects, plus more than 80 professional development events annually.

In the next 12 months it is launching a major education offering, which offers education in smaller pieces, enabling insurance professionals to undertake shorter, career-specific units, alongside engaging the industry through the Careers in Insurance and Know Risk programmes.

RMIA

The Risk Management Institution of Australasia (Rmia) is the professional industry association for risk management practitioners in the Asia-Pacific region.

It facilitates linkages between members and offers continuing professional development opportunities via annual national conferences, Risk Odyssey conferences, special interest groups, and chapter networking events and education programmes.

Rmia hosts short courses across risk management disciplines, endorses courses run by like-minded organisations or universities, and offers a three-level certification programme for professional risk managers.

Moving forward, Rmia will continue to implement its RISK2020 initiative, which will see RMIA aim to improve the quality of risk management throughout Australia by 2020, with the assistance of EY, its strategic sponsor for RISK2020.

IRM

The Institute of Risk Management (IRM) is a body for professional risk management, providing qualifications and training, publishing research and guidance, and attempting to raise professional standards.

Its members work in several roles across the public, private and not-for-profit sectors across the world.

IRM's International Certificate and International Diploma in Risk Management trains several risk practitioners every year. It also provides short courses on various risk management topics, from the fundamentals to specifics like presenting risk workshops.

The IRM plan moving forward is to raise awareness of its recently launched certification and professional standards among members, employers and regulators, while further extending its global reach.

CII

The Chartered Insurance Institute (CII) is the professional body for the global financial services and insurance professions. It has more than 115,000 members in over 150 countries, which covers all disciplines within the insurance industry – claims, broking, underwriting and sales – those working in the life and pensions sector, the mortgage advice market and financial advisers.

Headquartered in the UK, it is a sizable examination awarding body, providing education to more than one million students in 150 countries.

SURVEY: EMERGING RISKS

Risk managers ponder cyber cover

StrategicRISK's survey results indicate that risk managers are increasingly turning to insurance to stem the flow of **concern around cyber attacks**

A majority of Australian risk managers are considering an insurance investment in the next 12 months to protect their cyber and technology exposures, according to the *StrategicRISK* survey.

Some 54.5% of respondents are considering insurance for targeted cyber attacks, both internal and external; 38.9% are considering cover for a non-malicious loss of critical/customer data, while 20% are considering cover for failure of critical IT systems.

The results echo the findings of Aon's 2015 Asia-Pacific Cyber Impact Report, which found that Asia-Pacific companies are only protecting 13% of their information assets compared to 49% of property assets.

"The results from *StrategicRISK*'s survey reinforce that cyber is a complex risk issue that has become a leading concern for many organisations," Aon cyber risk practice leader Eric Lowenstein says.

"With its potential to cause major financial and reputational damage, cyber is a boardroom issue, not simply a problem for the IT department.

"There is a significant need for organisations and boards to become more aware of the threat that cyber risk poses to their bottom line, and brand and reputation."

Lowenstein says some overseas cyber criminal networks have sophisticated business models with established business strategies, executive management teams and even employee health plans and performance reviews.

"[Cyber risk] is not going away, particularly as Australia moves up the ranks to become a number one target.

"The [*StrategicRISK* survey] results emphasise there is an appetite for more information and solutions around cyber-related issues," says Lowenstein.

But not all risk managers are convinced about the merits of cyber insurance.

Lend Lease group head of risk and insurance Kevin Bates (see page 6) says that although cyber risk is one of his top concerns, he's never seen a cyber insurance product "that does anything I need it to".

"There are a number of other lines – be it your ISR (industrial special risks insurance), property (insurance), GL (general liability insurance) – you will have some level of coverage for a cyber risk if it's an infrastructure-related issue," he says.

Bates warns that a cyber attack could impact the personal information of clients and an insurance product is not going to solve problems caused by that breach.

"I'm a big fan of the human firewall in terms of educating your staff. The human firewall is the first line of defence and that's what everyone has got to get better at," he says.

Lowenstein suggests four key steps when developing a cyber-risk mitigation strategy: manage the process, identify the risks, understand the risks, then work closely with partners such as insurers and specialist lawyers.

"Cyber is an exposure that exists across many parts of the organisation. The development and implementation of an effective insurance programme requires a project champion who can manage the process across every level of management," says Lowenstein.

"A comprehensive and analytical approach is required to identify the number of potential cyber exposures within the organisation."

EXPERT VIEW FROM COSTA ZAKIS, GENERAL MANAGER PACIFIC, MARSH RISK CONSULTING

"Cyber risk is considered by some as a new risk to be managed. I have a differing view that cyber-related risk has been with us for some time but it is certainly more front-of-mind for many today as we are becoming more technology dependent in our work and personal lives.

Access, interest and reliance on technology has never been greater so we should rightly broaden our views to cater for this change in technological and cyber reliance. But, in a sense, cyber is only a medium, whereas the risks of data, information and system security have been there for some time.

In a broader sense, the evolving risk landscape needs to take into account our ability to adapt to change in the way we work, the clients we service, the people we work with, the resources available to us and the overall environment we are in.

We have always considered assets, people, services, finance, governance and the like, but the evolving landscape needs to look at how all of these are changing, the impact this has on our business environment and how we manage more concurrent and interconnected risks.

Our traditional risks are still there, but the evolving risk environment will consider items such as managing the rate of technological and societal change; managing a highly mobile and physically separated workforce; recruiting; training and maintaining a suitably skilled contemporary workforce; managing the ever-growing volume of information that we generate and collect; and understanding the increasingly complex world of international governance and how it relates to how we conduct our business, manage and protect our information and delivery of services.

Not one of the risks is simple and easily solved, but each has a significant bearing on how we operate our businesses and each is a good example that risk is never static but always evolving."

EXPERT VIEW

ROBIN JOHNSON, COUNTRY MANAGER AUSTRALIA, XL CATLIN

DATA BREACH NOTIFICATION LAWS TO CHANGE RISK PROFILE IN AUSTRALIA

Cyber risk has fascinated me for over a decade now, because it cuts across the two industries I've worked in. I spent the first seven years of my career working in technology in London, through the dotcom boom and bust, before falling – gratefully – into underwriting in the early 2000s.

Back then the only breaches that hit the news were lost or stolen government records – typically laptops and backup tapes. Private companies simply didn't disclose breaches – not because they weren't happening, but because until the US enacted laws requiring that customers were notified, they were under no obligation to do so.

It's been the spread of breach notification legislation around the world that has put cyber on the front pages, and forced companies and government to face up to a risk that's now completely pervasive. In the US, it's now a matter of national interest, and likely a top three agenda item for Obama's summit with Xi Jingping this month.

Here in Australia the issue of notification is also coming to the fore with legislation making notification of data breaches compulsory likely to be imposed in just a few months' time. I am new to the Australian market – I moved down here in June after six years in Asia and am watching with interest as to how this is going to play out.

To date, very few data breaches have made the Australian press, but I'd expect a massive spike to be reported once the new act comes in, in line with the US experience. And our clients are telling us that this proposed change in the law is driving cyber right up the risk register and into the boardroom, no doubt helped along by the salacious headlines regarding Ashley Madison.

This was reflected at last month's Rims event in Melbourne, where cyber was the topic of the moment, with several panels discussing how it's best addressed, and clients at various stages in the buyer's journey sharing their experiences. One of the panellists described how his board knew it was time to take cyber risk seriously when their head of IT security proudly told them the number of attacks they were repelling every day (the number was in the thousands), and I think this neatly encapsulated the knowledge gap that exists in many large corporations.

> "To date, very few data breaches have made the Australian press, but I'd expect a massive spike to be reported once the new act comes in, in line with the US experience'
>
> **Robin Johnson, XL Catlin**

Outside of the tech sector, most companies' board members have little technology experience and simply aren't aware of the legions of relentless hackers trying to pierce their security, nor the variety of their motivations. The archetypal bored teenage geek testing his hacking skills from his bedroom has long since been superseded by a rogues' gallery of well-resourced and sophisticated criminal gangs, hacktivists, and so-called state-sponsored "buccaneers".

So how do risk managers best address this rapidly evolving cyber threat? One of the first things I was taught as a technology consultant was that you can only provide a client with a solution once you both thoroughly understand their problem. It's a truism that I've carried with me throughout my career and it matches XL Catlin's philosophy of partnering with clients to find solutions.

So I'd advocate that clients take a collaborative approach, and approach brokers and underwriters to see how they can design a solution which meets their specific needs. No two clients' cyber risk profile is alike, and our experience is that the more the product and services are bespoke for a client's needs, the better it will perform in a claims situation.

CYBER RISK CHECKLIST

It is true that cyber risk is more complex than ever. It has to be mapped and measured accurately, for insurers to be able to offer appropriate cyber policies.

Companies should create a cyber risk map, starting with the link in the cyber chain closest to them. That is an internal risk. Then they should move through their chain of contractors and subcontractors, inspecting security protocols and risk aggregation nodes.

Once all possible risk has been mapped, the probability and cost of a breach or system failure at each risk node should be measured, and a cost assigned. Adding all of the costs up will determine maximum cost exposure. This is also a good time to review the risks. Can any of them be reduced by improving systems, or hiring different contractors or subcontractors?

Next, companies should check their cyber risks against existing liability, property and reputational risk policies. Are there coverage gaps for non-physical business interruption, third-party business interruption, or other risks? The more detailed the risk map, the better insurers can help clarify whether existing coverage is sufficient for certain risks, or whether cyber coverage is necessary.

Companies may decide that they want to retain risk up to a limit, so they should define a maximum deductible, and discuss it with insurers.

With a solid cyber risk map and a defined deductible, we advocate meeting your broker and underwriter to discuss coverage and services that meet these specific needs.