

New Zealand Survey of Risk 2018

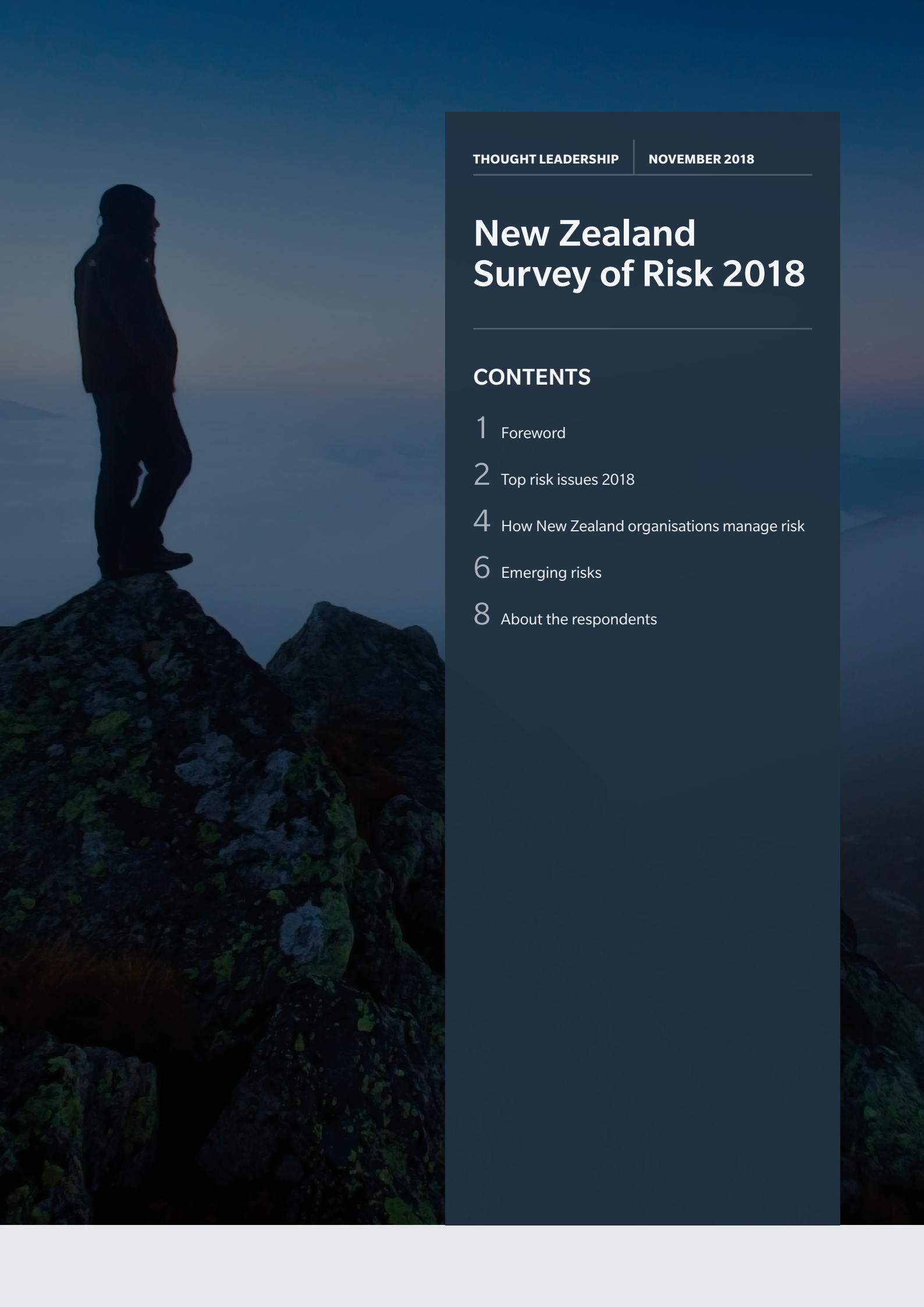
The Seventh Marsh Risk Report



New Zealand Survey of Risk 2018

CONTENTS

- 1 Foreword
- 2 Top risk issues 2018
- 4 How New Zealand organisations manage risk
- 6 Emerging risks
- 8 About the respondents



Foreword

Marsh prides itself on being the leading provider of risk advice and solutions in New Zealand.

An important part of what we do is to ensure that you are kept informed about the latest market factors and risk issues that will have an impact on your organisation, to enable you to make the right decisions for your business.

I am therefore pleased to provide you with the findings of our seventh Survey of Risk, which provides some insights about the current and emerging risk factors impacting Kiwi businesses – from SME's to our large corporates.

Whilst many new risks have appeared in this latest survey – the current biggest risk concern for organisations is disruption to your business caused by fire, flood or another natural disaster. This has been consistent throughout the last four surveys.

Earthquakes, flooding, wildfires and cyclones are now a regular feature within New Zealand. It is also a global issue with economic loss from natural disasters in 2017 reported to be USD\$337 billion, according to Swiss Re. Unfortunately these incidents are only expected to increase over time with climate change.

Brand and reputation risk appeared in our report, as the second biggest risk, for the first time in the survey's history.

It certainly is not a new risk, however the use of modern technologies has made managing an entity's corporate standing a lot more challenging.

Misinformation, in particular, can spread instantaneously on social media and be created anywhere in the world with just a few simple clicks. It is such an issue that Facebook has recently been implementing scores and warnings for articles proven to be fake and has even started punishing users for flagging news from credible sources as fake.

The key to mitigating this risk is to try and anticipate the various scenarios that could impact your brand and then have plans in place to manage it. This may even include hiring or working with a public relations firm if you don't have the expertise in-house.

Disruption to your business following a major IT disruption eg server overheating, software failure etc was the third largest risk in our survey followed closely by loss of data, data corruption or failure of systems security or website security ("hackers" etc) or cyber risks. The theme continued with cyber risk also being the biggest emerging risk facing organisations.

There are new incidents of cybercrime occurring all the time – one day its ransomware, the next it's invoicing interception fraud. Businesses, regulators and government bodies around the world are struggling to keep up with the pace of change.

A big part of managing cyber risk, and in fact all of your emerging risks, is to keep informed about them and how they are evolving. Once this is understood, the next step is to develop a plan about how to manage them. Your client executive is an important resource to help you here and can bring in expertise from around Marsh and our Marsh & McLennan sister companies as required.

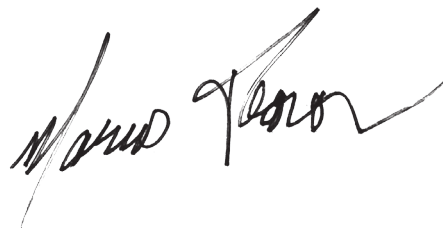
Many organisations unfortunately did not have plans in place to deal with some of the emerging risks that were coming through. It was especially the case when it came to increasing corporate governance requirements and talent and attraction risks – so remedial action in these areas is recommended.

Interestingly, 55% of our clients said that they are reviewing risk more than they were two years ago. Our ever changing and sometimes volatile environment is likely to be pushing the topic higher up the corporate agenda.

Companies that recognise the opportunities in innovating around corporate resilience, and can effectively identify emerging risks and integrate them into their strategic and operational planning can swiftly position themselves to improve their resilience and gain a competitive advantage.

With the exception of a few disastrous events like nuclear war, most risks also present an opportunity for those businesses that position themselves well to meet the challenge.

Thank you to the 132 respondents who took the time to complete our survey. Your time and insights are much appreciated.



MARCUS PEARSON
Country Head
Marsh New Zealand

Top risk issues 2018

Natural disaster risks are still the number one risk for businesses across New Zealand.

For the fourth consecutive survey, disruption to your business caused by fire, flood or another natural disaster was rated the risk issue of most concern to New Zealand businesses.

While our last survey was four years ago, the impact of environmental risk has not changed with earthquakes, flooding and coastal storms unfortunately continuing to be a part of Kiwi life.

The Insurance Council of New Zealand reported in June this year that insurers had received more than 27,000 claims for extreme weather in the first part of the year alone.

Cyclone Fehi, which hit in early-February, cost a total of \$45.9 million. Cyclone Gita, in late February, cost \$35.6 million while the 27-29 April storms, which saw severe flooding and a state of emergency declared in Rotorua, have cost \$16.1 million so far.

The World Economic Forum's annual Global Risks Report, found that extreme weather events and natural disasters were the 2nd and 3rd greatest risks to society in terms of impact – only preceded by weapons of mass destruction.

Unfortunately, New Zealand will only continue to experience increases in the frequency and intensity of extreme events such as flooding, droughts and even wildfires. There will also be slowly emerging changes such as ongoing sea-level rises – so we need to be prepared for this.

Brand and reputation management was seen to be the second biggest risk currently facing New Zealand organisations.

This is the first time that the issue has been in our top five risks since the survey began in 2004.

With the growth in social media platforms, and information being able to be spread around the world in seconds, it is no wonder that organisations are concerned.

With so-called “fake news” and an environment of volatile social issues, organisations should re-evaluate whether they are doing enough to protect and manage their reputation with customers, employees and other stakeholders. Rumour and allegation are not new problems for companies, but in today's “always-on” world, the rapid spread of mis-information can be more

challenging to overcome. How an organisation responds can minimise the reputational fallout.

Disruption to your business following a major IT disruption eg server overheating, software failure etc was the third largest risk in our survey followed closely by loss of data, data corruption or failure of systems security or website security (“hackers” etc) or cyber risks.

Business today revolves around cyber-physical systems, the Internet of Things and the Internet of Services. Our hyper-connectivity in this new digital world has been a boon for productivity— connecting and executing tasks with a speed that was previously inconceivable – however it does of course bring a range of risks with it.

The concern about IT disruption to a business is correlated by a global report run by Marsh and Microsoft – The Global Cyber Risk Perception (GCRP) Survey.

80% of New Zealand respondents to the GCRP survey cited business interruption as the most worrisome consequence of a cyber-attack. It was not just the physical damage of equipment and / or disruption to services that was a concern it was also the brand damage that a cyber event can cause with 73% of respondents highlighting this as a key issue.

Interestingly, the top five risks identified by the respondents in this 2018 Survey of Risk were very similar to the top risks identified by the Global Risks Report – extreme weather, natural disaster, cyber attacks and data theft.

How are these risks being managed?

Organisations appear very confident when it comes to the management of some of these key risks with 95% saying that they have processes and procedures in place to manage their natural disaster risks.

An area that is sometimes overlooked however is how events may impact your supply chain. We have seen companies that have good plans in place to protect their local assets in the case of disaster but have overlooked what to do if there is an event that impacts their suppliers. For example, if you rely on goods or services from offshore, how would you manage if your vendor can't deliver due to a hurricane or flooding impacting their business? Even from a local perspective, your supplier could be impacted by a cyber attack that shuts their business down. 45% of the organisations we surveyed said that they did not have these plans in place.

FIGURE

1

Top five risks 2018, compared with 2014

2018

- 1 Destruction and disruption of assets by fire, flood or some other natural disaster / extreme weather event.
- 2 Brand and reputation management.
- 3 Disruption to your business following a major IT disruption eg. server overheating, software failure etc.
- 4 Loss of data, data corruption or failure of systems security or website security ("hackers" etc) or cyber risks.
- 5 A breach of security of your business premises.

2014

- 1 Disruption to your business following a major incident, such as fire, earthquake, flood, act of terrorism.
- 2 Disruption to your business following a major IT disruption eg server overheating, software failure etc.
- 3 Loss of data, data corruption or failure of systems security or website security ("hackers" etc).
- 4 Changes in demographics and customer trends.
- 5 Drop off in demand.

Another area requiring attention is around brand and reputation management. 32% of the respondents said that they didn't have a plan in place to deal with this risk.

Warren Buffet famously once said "It takes 20 years to build a reputation and five minutes to ruin it."

One of the key things that you can do to reduce reputational damage, is to plan what you would do before it happens.

Identifying some of the potential issues your organisation could face is the first step. For example, if you are in manufacturing it could be a product recall or environmental incident. If your business is in professional services think about people risks, data breaches or a disgruntled client expressing their views.

Once you have done this you need to develop a communications strategy that addresses these issues and identify a team of people who can come together and manage all of the various elements of a crisis when it hits.

Managing losses

Only 15% of our survey participants had suffered a high impact financial loss in the last three years. This has come down from 26% four years ago.

Of those who had suffered a loss, only 30% had it covered by their insurance policy. Unfortunately we don't know whether this risk had been insured to start with or if the claim was denied by the insurer. Either way, a thorough review of your policies should be undertaken when your policies come up for renewal. This should include the consideration of new and emerging risks.

We also asked those who had had a loss if 12 months was "long enough for your business to return to the same gross profit you enjoyed prior to the loss". 40% said it wasn't.

The amount of time that your business is covered by insurance following an event is called an indemnity period. 12 months is typically the timeframe that entities choose for this purpose however it is often found to be woefully inadequate. This is reinforced by the clients completing the survey who said that 24 months (63%) and 36 months (37%) were more realistic timeframes for getting back on their feet.

85% of those who sustained a loss had used the opportunity to put plans in place to help reduce future losses within the area affected.

How New Zealand organisations manage risk

Who carries the responsibility internally?

The second section of this report looks at how New Zealand businesses are managing risk.

When it comes to governance and who is accountable for ensuring risk management is in place and appropriate investment in mitigation is undertaken, 37% said it was the role of the board of directors and 31% the owner or proprietor of the business. 18% said it was the CEO / managing director or general manager.

However, when it came to who has the ultimate responsibility for implementing, managing and reporting risk management procedures within your organisation, it was either the CEO / managing director / general manager (37%) or the owner / proprietor (31%).

These results are an interesting contrast to the Directors' Risk Survey Marsh ran in May this year. When asked the same question 49% of directors responded that it was their responsibility while 26% said the CEO.

The key to this issue is to ensure that there is no confusion as to who is ultimately responsible for the management of the risk.

What external advice is being sought?

61% of the entities surveyed use external advisors to help identify, manage and understand risk. These ranged from insurance brokers (21%) to auditors & accountants (22%), to legal counsel (18%).

Seeking external advice has dropped from four years' ago when 73% of respondents were going outside of their organisation for risk support. It raises the question – are companies and directors getting the appropriate level of specialist advice?

A higher proportion of those surveyed in 2018 are seeking risk advice from their auditors and accountants.

Is risk reviewed more regularly?

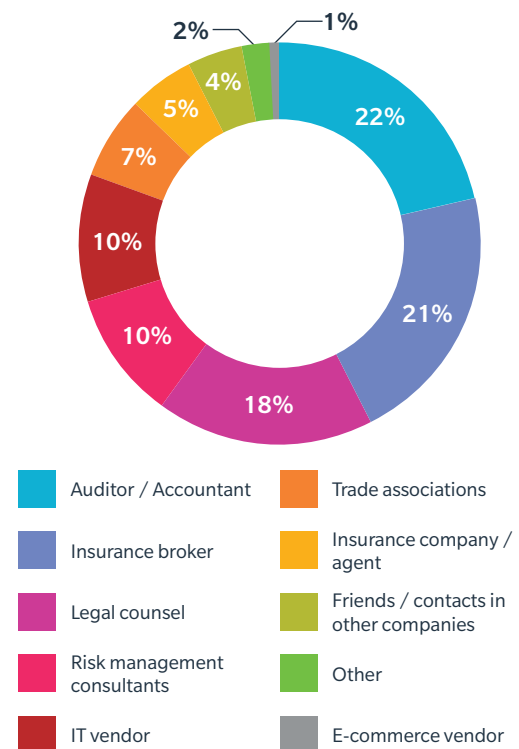
55% of our clients said that they are reviewing risk more than they were two years ago.


We believe that this is reflective of the extraordinary pace of change in the world, which ultimately shapes the global risk environment.

Changes in technology, such as artificial intelligence and robotics, and rapid change in the political landscape are just some examples of the risks that impact our day-to-day business activities.

Organisations should therefore consider how societal and political changes impact their operations and profitability and look at whether they have strong operational frameworks in place to deal with the likes of IT and cyber disruption.

FIGURE 2 Who do companies go to for advice?





Changes in technology, such as artificial intelligence and robotics, and rapid change in the political landscape are just some examples of the risks that impact our day-to-day business activities.

Emerging risks

Cyber the biggest emerging risk

Our increasing reliance on data and electronic processes to operate effectively, makes us more susceptible to cyber-incidents. These are not only increasing in frequency, but are also becoming more severe, diverse and complex, with significant consequences. It was no surprise therefore that cyber was seen to be the biggest emerging risk over the next 24 months.

According to CERT NZ's second 2018 quarterly report, cyber incident reporting has increased 143% since Q1 2018. In that period, 507 cyber incidents were reported by organisations. Direct financial losses from all cyber incidents for the period were \$2.2 million.

Marsh has seen a rise in Cryptojacking events this year due to the rise of cryptocurrencies – this is a method of essentially hijacking an organisations computer server horsepower to 'mine' cryptocurrency for a cyber threat actor. Additionally, invoice interception fraud – altering bank accounts of an expected invoice – is also becoming a quick and effective method for cyber criminals to earn money.

The World Economic Forum estimates the economic loss of cyber incidents is between US\$1.5-4 trillion a year. Transferring cyber risks to insurers is therefore an appropriate risk management strategy. In fact in 2017, Marsh saw almost a 50% increase in the cyber insurance premium placed in New Zealand. Organisations need to better understand the value at risk to effectively decide how much insurance to purchase however.

Increasing corporate governance requirements, which was the biggest risk in our last survey, came in at number two on the emerging risk scale.

Organisations are consistently faced with new legislative changes that need to be reviewed and adhered to. This year alone, for example, there has been the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT) come into force, new hazardous substances regulations, and various changes to New Zealand employment law. There is also more to come with the Privacy Bill passing its first reading in the House of Representatives. This will have implications for Kiwi organisations who will have to report any notifiable privacy breaches.

Talent attraction and retention has been a consistent theme across all of the surveys we have run this year and was ranked the third biggest emerging risk in this survey.

The shortage of good quality candidates within the market has made it challenging for New Zealand organisations to find the right people. A lack of applicants, skills and experience available at the moment and the Government's tightening immigration policy has caused considerable frustration amongst employers.

According to Mercer's Global Talent Survey 2018, "To compete in the war for talent, organisations must design jobs that people want and careers that they crave, invest in employee's professional growth and personal wellbeing and show employees how their work is tied to the organisation's mission and positively impacts society. This is because today's individuals need to find relevance and purpose in their work."

Marsh has seen a rise in Cryptojacking events this year due to the rise of cryptocurrencies.

This is a method of essentially hijacking an organisations computer server horsepower to 'mine' cryptocurrency for a cyber threat actor.

Preparedness for these emerging risks

Despite the potential financial impacts and reputational risk, 23% of the clients we surveyed said that they did not have a procedure in place to deal with cyber risk.

Previous research by Marsh has shown that, in many cases, business lack the confidence around understanding or responding to a cyber incident and don't comprehend the risks their suppliers pose. A big part of dealing with this risk therefore is understanding where to start.

The first line of defence is to carefully identify your key areas of cyber risk and what your most critical systems/processes are that may cause a catastrophic 'worst-case-scenario' for you in the event of a cyber attack. Like any other area of risk, identification would allow you to put the correct measures in place, such as staff training and awareness, developing emergency response plans and even reviewing your supply chain risks and how your vendors handle their cyber exposures.

43% did not have plans in place to deal with increasing corporate governance requirements and 44% were similarly placed when it came to talent attraction and retention risks.

Keeping abreast of what is happening in the regulatory environment is a key starting point to ensuring that you have any related risks. Marsh often send out Client Briefings that provide a summary of any key legislative changes and what the implications are from a risk and insurance perspective.

When it comes to talent attraction and retention, a well structured employee benefits programme can go a long way to attracting new employees and retaining existing ones. Mercer's 2018 Global Talent Study shows that the top talent trends are the ability to change and change quickly, working with purpose, flexible workplaces, diverse talent ecosystems and improved digital employee experiences.

Are Kiwi entities prepared to deal with these risks?

The answer is not really.

FIGURE
3

Top 5 emerging risks 2018, compared with 2014

2018

1	Cyber
2	Increasing corporate governance requirements
3	Talent attraction & retention
4	Earning volatility
5	Business continuity

2014

1	Increasing corporate governance requirements
2	Cyber
3	Business continuity
4	Identity fraud / theft
5	Environmental issues

About the respondents

132 senior executives from a range of industries, organisational sizes and geographic locations from around New Zealand responded to the seventh Marsh Survey of Risk.

31% were the owner / proprietor of the business, 20% CEO and 20% CFO.

56% of the organisations were private or family owned, 9% a public limited company 8% not for profits plus a range of central and local government institutions.

In regards to organisational size 37% had 1-20 employees, 25% 21-100 employees, 14% 101-300 employees and 24% over 300 employees.

There was a wide range of industries represented from financial services to construction, through to healthcare and manufacturing.

The biggest group of respondents was from Wellington (34%), followed by Auckland (19%) and Canterbury (18%).

FIGURE 4 Respondents by job title



FIGURE 5 Respondents by organisation type

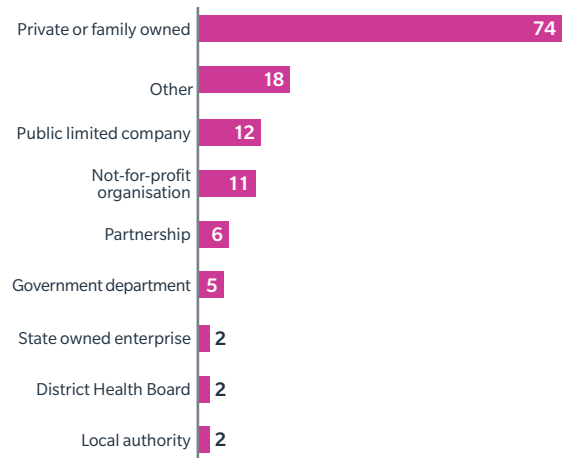


FIGURE 6 Respondents by organisational size in number of employees

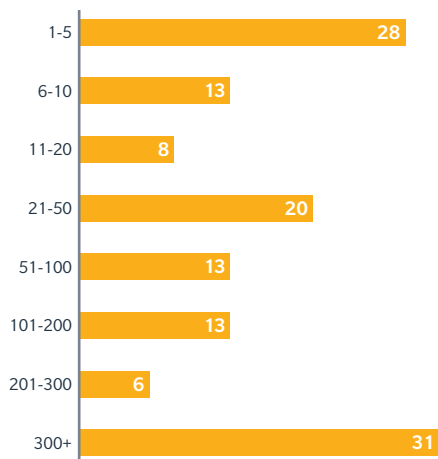
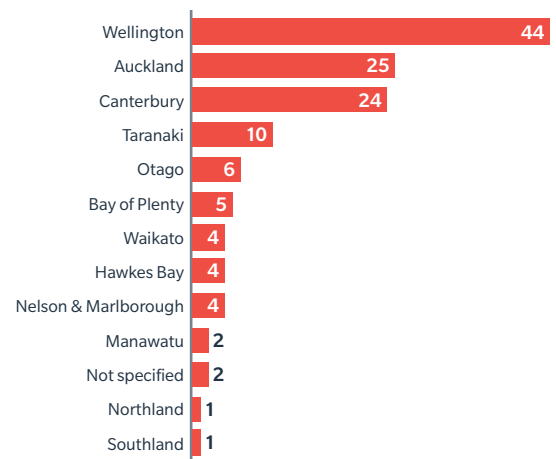


FIGURE 7 Respondents by region





ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, [Marsh's](#) 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly owned subsidiary of [Marsh & McLennan Companies](#) (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US\$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of [Guy Carpenter](#), [Mercer](#), and [Oliver Wyman](#). Follow Marsh on Twitter [@MarshGlobal](#); [LinkedIn](#); [Facebook](#); and [YouTube](#), or subscribe to [BRINK](#).

To find out more about the risk issues discussed in this report and / or talk about your own organisation's risks please contact us:

0800 627 744

www.marsh.co.nz

Disclaimer: This publication is for general information and does not take into account your individual objectives, financial situation or needs. You should obtain and read the policy wording or product disclosure statement prior to acquiring an insurance product, which is available from Marsh. This brochure is not a substitute for specific advice and should not be relied upon as such. We accept no responsibility for any person or corporation acting or relying on this information without prior consultation with us.

© Copyright 2018 Marsh Ltd. All rights reserved. NZ18-1231