The sector body in NZ bringing together people + organisations managing risk.

RISKPOST

RISKNZ MEMBER NEWSLETTER

DECEMBER 2018

WEB
risknz.org.nz

POST
PO Box 5890, Wellington 6140

EMAIL
adminofficer@risknz.org.nz

RiskPost gratefully acknowledges the support of our premier sponsors JLT and SAI Global

SAI GLOBAL

JLT

IN THIS EDITION...

1. A word from the Chair
2. ARNZ Post Nominal timescale
3. From the Editor
4. RiskNZ Standards Update
5. The Breakfast Networking Forums
8. How effective is managing the risks of uncertainty with people
11. Turning the induction into a powerful risk management tool
13. Online reading – two thought provoking pieces
15. Building our disaster resilience
19. The woes of airline travel
22. RiskNZ Elections 2019
23. RiskNZ Information

A WORD FROM THE CHAIR

NIGEL TOMS – *Chair, RiskNZ*

Welcome to the fourth and final edition of RiskPost for 2018. The year seems to be passing incredibly quickly!!!

Most members of RiskNZ will be aware that following approval of a resolution at the 2017 AGM, the RiskNZ Board appointed an independent Professional Recognition Committee to develop and recommend to the Board the criteria by which RiskNZ will confer on members the right to use Post Nominals.

This work has now been completed and approved by the Board. The criteria will be published on the RiskNZ website in the next few weeks and this will be followed by guidance on the application process.

At this stage the criteria relate to the Associate of RiskNZ (ARNZ) Post Nominal which is intended solely to recognise that the user is a Member of RiskNZ and has been awarded the right to use the ARNZ Post Nominal.

Application for and use of these Post Nominals will be optional and there is no requirement to apply for these Post Nominals if a member does not wish to do so.

Continued on next page...

RiskNZ wishes you all a very Merry Christmas and New Year, safe and relaxing holidays, and best wishes for 2019.

A WORD FROM THE CHAIR CONTINUED...

ARNZ Post Nominal timescale
Below is an outline of the timescale for implementation:

1. The application form and related guidance will be published on the RiskNZ website in late January 2019.
2. The application process will open to members in February 2019.
3. Application review and approval will be completed by May 2019. We expect that some members may apply after our AGM, so there will be a regular review cycle for applications received after the initial wave of applications are processed.
4. Use of Post Nominals will be granted in 2019/20, dependent upon a member having paid their 2019/20 subscription.
5. The post nominals will be effective from June 2019.

I would like to thank the members of the Professional Recognition Committee and the Board for their efforts bringing this work to completion. I believe it will prove beneficial to the future development of RiskNZ and the risk profession in New Zealand.

In previous RiskPosts I have given my thoughts on Tesla and the accompanying Elon Musk saga. At the time of the previous RiskPost he had tweeted that he was THINKING about taking Tesla private. Interestingly, if he had stopped at that point, there would have been few repercussions and it would have been seen as venting in his usual style. However, he then went further and advised that he had the necessary private funding secured at USD420 per share. The market reacted to this announcement with the share price rising and then falling as the announcement was not followed by any further action.

The US Securites and Exchange Commission (SEC) laid charges against both Elon Musk and Tesla. Settlement of the charges cost him USD20m and Tesla USD20m. This is a very expensive twitter statement and would have cost most Chief Executive Officers (CEOs) their positions.

In this case the settlement included further sanctions requiring that Musk must step down as Chairman and be replaced by an independent Chair; with Tesla's board adopting reforms including additional independent directors, and controls and procedures to oversee Musk's communications. In November, Tesla announced that Robyn Denholm was appointed as Chair of the Tesla Board, serving as a full-time Chair upon completion of her 6-month notice period with Telstra.

Corporate governance structures and legislation varies across countries, and while not wanting to review the differences between the roles of CEO and Chairman in detail, in simple terms the CEO is a company's top decision-maker and is ultimately accountable to the board of directors for the company's performance. The Chairman of a company is the head of its board of directors and the board is responsible for protecting investors' interests, such as the company's profitability and stability. It is accepted that the balance of power between CEOs and Chairmen varies significantly between companies, however, in theory, a CEO cannot make major moves without the board's assent.

With this in mind I looked back at the training I received long ago regarding how to describe a risk. While most initially spend time trying to create an overall title for the risk, followed by the supporting detail, I was taught to:

1. Describe the cause
2. Then describe the consequence on achievement of objectives
3. Finally create an overall risk title based on 1 and 2 above.

This is much quicker and produces a much more accurate and useful risk description.

4. The next consideration is the Mitigation Action(s) which should, where possible, target the cause, as this will have a much greater effect in most cases than just trying to reduce the consequence. This is a good test of the accuracy and veracity of proposed mitigation actions, and in the past, I have come across a number of cases where mitigation actions proposed would not have impacted the cause or consequence.

In the case of Elon Musk and Tesla, I cannot deny feeling uncomfortable about the effectiveness of appointing a separate Chairman who is responsible for, but may not be able to achieve the desired stability. In reality a CEO who can cost Tesla USD20m and personally lose another USD20m, may remain in total control.

I would end by repeating what I have stated previously, the real story for Tesla is around financial performance and moving the company into sustained profit. This is still a very real challenge for Tesla and has the potential to threaten Tesla's survival.

FROM THE EDITOR

SALLY PULLEY - *RiskNZ Deputy Chair*

This is the fourth and final edition of RiskPost in 2018. As we accelerate towards the end of the year, a big thank you to all who have contributed to this Edition:

- Brent Sutton presented a paper at the 2018 RiskNZ AGM which asked the question 'Is the effect of uncertainty on objectives' relevant to health and safety risks'. Upon request, Brent has structured that paper for publication in this edition of RiskPost.
- David Turner provides insights on how induction can become a powerful risk management tool.
- Jane Rollin and Jo Horrocks of DPMC provide an overview of the recently released National Disaster Resilience Strategy.
- Sue Trezise identifies another two thought provoking online reads - Enhancing interactions through Cognitive diversity and Psychological safety, and the recently issued Gartner report on Risks Facing Large Public Companies, and
- With the upcoming holidays when many will be traveling, our sponsor SAI Global provides a timely reference to the woes of airline travel.

THINKING AHEAD

Best wishes for the holidays season and for the New Year. We are already planning for Edition 1 of RiskPost 2019.

If you get time to do some risk-related reading over the holidays, and you see an interesting article in a magazine or on a website that would be of wider interest to RiskNZ members, please let me know. RiskNZ will seek the rights to republish, or provide links to the content, on the website and in RiskPost.

All feedback is welcome because I need to know what you would like RiskPost to cover in 2019. Please contact me at *editor@risknz.org.nz*

RISKNZ STANDARDS UPDATE

KRISTIN HOSKIN - *RiskNZ Management Board Member*

OB-007 met in Adelaide 19-20 November 2018. The majority of the meeting was spent on HB 436: 2019. This will be a companion guide to ISO 31000:2018 Risk Management and will be known as *The Executive Guide to Risk Management*. The target audience is executives, rather than risk practitioners, and it is intended to help them apply 31000 into their strategic decisions. The draft of this document is now well progressed.

Once this project is complete OB-007 will focus on the Practitioner's Guide. Both Guides will be written to work collaboratively to help an organisation use 31000 to best advantage in implementing risk management.

Aside from progressing this project, the meeting also covered off progress and happenings on a number of other projects and initiatives.

Of note:

- Project proposals will, starting in January be considered monthly by Standards Australia. So, whereas previously there was only two intakes of project submissions per year, there is now opportunity to initiate projects in a more timely manner.

- OB-007 is looking for appropriate people to discuss currency of HB 192:2007 Guide for managing risk in motorsport, but at this point it is likely to be withdrawn. HB-141:2011 Risk Financing Guidelines is under review, subject to specialised insurance industry input.

- We are also looking at other aged standards and how they may be brought up to date, or if they should be withdrawn. In addition to the above, HB 246:2010 Guidelines for managing risk in sport and recreation organisations, HB 266:2010 Guide for managing risk in not-for-profit organisations, and HB 327:2010 Communicating and consulting about risk are currently under review.

- There has been considerable work on security related standards of late with the Standards Australia Security Futures Forum taking place on 14 November. Recent work being considered includes progressing a proposal for development of HB-188 - Physical Protective Security Treatment for Buildings Handbook.

On the TC262 front, the legal risk management draft and the new work proposal for ISO31073 (proposed to replace ISO Guide 73 Risk Management Vocabulary) were voted on this month (26 November). The outcome of these votes will be known and advised to you soon.

For further information on current risk related standards activity (NZ, AS/NZS, ISO) please contact Kristin Hoskin kristin@risknz.org.nz

NEWLY PUBLISHED BOOKS

Recently Routledge published a new book; *Disaster Health Management* - A primer for students and practitioners, edited by Gerry Fitzgerald, Mike Tarrant, Peter Aitken and Marie Fredriksen.

A book review will be provided for the next edition of RiskPost, which is scheduled for February/March 2019.

The textbook offers a standard guide to terminology and management systems across the entire spectrum of disaster health. It is current to and draws on ISO 31000: 2018.

Available from: https://www.routledge.com/Disaster-Health-Management-A-Primer-for-Students-and-Practitioners/FitzGerald-Tarrant-Aitken-Fredriksen/p/book/9781138911185

THE BREAKFAST NETWORKING FORUMS

The Breakfast Networking Forums are an opportunity for RiskNZ members to meet and talk about risk management outside of workplace meetings or conferences and seminars. Meetings are relaxed and collegial, have a definite practical focus, and enable experienced and newbie risk practitioners to share thoughts and experiences. All attendees are encouraged to get involved in the conversation.

Topics for discussion are picked for their relevance and interest for attendees. We are always looking for facilitators with risk related topics. Your continued involvement is what has made this happen, so volunteers please step up and get involved!

Contact details are:

Miles in Wellington at *miles@risknz.org.nz*

Kristin in Christchurch at *kristin@risknz.org.nz*

Darroch in Auckland at *darroch@risknz.org.nz*

RECENT WELLINGTON BREAKFAST MEETINGS

The Wellington meetings usually take place every second month, but can be more frequent if members want to meet and discuss a particularly salient topic.

Sally Pulley facilitated the latest meetings of 17 October and 14 November. Discussions covered a wide range of risk management concepts, with some directly related to project / programme management and some much wider, relating to establishing context and scope for how an organisation approaches risk management, and linking programme risks into strategic / enterprise risk oversight.

Participants noted the importance of induction processes, and David Turner has provided an article on 'Turning the induction into a powerful risk management tool' - see page 11 for more information.

INTRODUCING THE BREAKFAST MEETINGS IN AUCKLAND

Our inaugural Auckland Breakfast meeting on 20th September was a success, with Nick Hill, Chief Executive of Auckland Tourism, Events and Economic Development (ATEED) talking about the economic development future of Auckland and some current projects being led by ATEED on behalf of Auckland Council. The Kumeu and Auckland Film Studios, both managed by ATEED, have nearly doubled the New Zealand film industry turnover to over $1.3 billion. The planning for the 36th Americas Cup is underway, with ATEED leading the event planning together with Emirates Team NZ, while Panuku is leading the Infrastructure build. APEC 2021 planning is also underway with ATEED, again on behalf of Auckland Council, assisting with the planning. It is going to be an extremely busy couple of years for Auckland, with huge gains for the city as well as wider New Zealand.

Our second Auckland Breakfast meeting on 13 November was hosted by Panuku Development Auckland Ltd, commonly known as Panuku. About 15 people turned up for a great breakfast and networking session, before our guest speaker, Panuku's CE, Roger MacDonald, spoke about their initiatives to develop parts of Auckland.

Panuku's job, on behalf of Auckland Council, is to buy, sell and manage Council's $2 billion portfolio of land and buildings. Their aim is to encourage economic development through urban redevelopment, by looking for new ways to generate income for the city. Roger spoke about a number of projects that Panuku is working on. Examples included the massive transformation of the Wynyard Quarter, including the America's Cup development, and the redevelopment and transformation of Onehunga, which includes a major restructuring of Onehunga Wharf and a light rail link. The presentation was interesting and a real insight into some massive Auckland projects, as well as a great opportunity for Risk NZ members and guests to network and get to know each other.

At the third event on 3 December the Auckland Council hosted Terence Lee, Head of Strategic BCP at SAI Global. This session focused on Business Continuity Management strategies and technologies.

Winners of the 2018 RiskNZ Awards of Excellence were announced on 12 September 2018.

To see details of all the winners please visit our website: *http://www.risknz.org.nz/news-and-events/awards-2018/*


JLT
PRINCIPAL SPONSOR &
INSURANCE PARTNER TO
RISKNZ
JLT is one of the world's leading providers of insurance, reinsurance and employee benefits related advice, brokerage and associated risk services.
CONTACT JLT FOR
FURTHER INFORMATION
DEBORAH FISHER
T: +64 (0) 300 3763
M: +64 (0) 21 902 864
deborah.fisher@jlt.co.nz
www.jlt.co.nz

HOW EFFECTIVE IS MANAGING THE RISKS OF UNCERTAINTY WITH PEOPLE

BRENT SUTTON – *Principal, Safety Associates*

At the RiskNZ 2018 AGM I presented a paper which asked the question of 'Is the effect of uncertainty on objectives' relevant to health and safety risks?'.

ISO 31000:2018 describes the meaning of risk as the 'Effect of uncertainty on Objectives'.

It also provides some additional clarification in that:

1. Effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
2. Objectives can have different aspects and categories, and can be applied at different levels.
3. Risk is usually expressed in terms of;
    a. risk sources
    b. potential events
    c. their consequences
    d. their likelihood.

When we think about the context of risk management with health and safety, it is people who are at risk of harm. The risk source (something that can cause the harm) is called a hazard. The potential events for the harm to occur are hazardous situations that can lead to hazardous events. The risk of the resulting harm is often described in terms of the likelihood/probability of the hazardous event and the consequence/severity of that hazardous event to a person.

We then have a legislative framework of Acts, Regulations, Safe Work Instruments, Approved Codes of Practices, Guidance and Standards that govern the management (duties and responsibilities) of these risks in so far as reasonably practicable. If someone commits a breach of this framework, they could face criminal charges as described in the various Acts and Regulations, including penalties of fines and imprisonment.

With the eighth anniversary of Pike River we are reminded of the human toll and tragedy of such events - when our risk management practices are not effective in not only preventing the event but also in the response and recovery to tragic events.

I ask people a simple question, Is the likelihood of the event happening relevant if the consequence can cause a life changing event?

A translation from Jens Rasmussen in his academic paper 'Human errors. A taxonomy for describing human malfunction in industrial installations'[1], described that human error can occur;

- 1 in 1000 in a rules-based environment, due to misinterpretation
- 1 in 10,000 in a skills-based environment, due to inattention

If the hazards in this environment can cause a life changing event, is it relevant if it happens (on the scale of 1 to 1000 or 10,000) or should we work on the basis of when it happens and control the hazard as far as reasonably practicable to prevent harm from occurring and have secondary safeguards for the response and recovery for the event occurring.

An example of this departure from our accepted thinking can be found from the organisation ICMM (International Council on Mining and Metals). In 2015 they published a guide called 'Health and Safety Critical Control Management' or CCM approach.

The CCM process is a practical method of improving managerial control over life changing events by focusing on the critical controls. These sorts of events they called material unwanted events (MUEs).

Continued on next page...

[1] Jens Ramussen, *'Human errors. A taxonomy for describing human malfunction in industrial installations'*, Journal of Occupational Accidents. Available via the ScienceDirect website.

Mining industry examples of MUEs include underground fires, coal dust explosions and overexposure to diesel particulate matter and also include the potential exposure of groups of workers to carcinogenic or other agent at harmful levels over a protracted period.

The guidelines recognised that;

1. The majority of MUEs within the mining and metals industry are known, as are the controls.
2. Most life changing events are associated with failures to effectively implement known controls rather than not knowing what the risks and controls should be.
3. More can be less. A hazard management plan of 50 pages will often contain a large number of controls, which can be complex to understand, implement and monitor. This can lead to less robust management of critical controls.
4. Less can be more. The fewer number of controls, the more robustly they can be monitored.
5. Some controls are more important than others. These controls should be monitored more regularly.

The simplicity of the CCM approach is based on 5 key steps;

1. Have clarity on those controls that really matter, which are called critical controls.
2. Define the performance required of the critical controls i.e. what the critical control has to do to prevent the event occurring.
3. What needs to be checked or verified to ensure the critical control is working as intended.
4. Assign accountability for implementing the critical control – who has to make it work?
5. Report on the performance of the critical controls.

There was a pattern amongst risk professionals in this industry to produce risk bowtie diagrams that were comprehensive and overwhelming for management to determine the effectiveness of risk management. They recognised the need to create a filter for critical controls that could be applied to determine what controls could be effective as event prevent, response and recovery.

They determined that for a control to be a critical control it had to meet all three criteria of:

1. Be an object, system of human act.
2. Prevent or mitigate an unwanted event.
3. Be performance specified, observable, measurable and auditable.

When this filter was applied, management was able to see how few, if any, critical controls existed.

This shifted the management view of risk management from:

'Good risk management is measured by the absence of accidents and incidents'

to:

'Good risk management is measured by the presence of critical controls to prevent, response and recover from unwanted events'

This then shifts risk management from the uncertainty of events to managing the certainty of events.

To prevent such tragedies as Pike River happening again, we need to consider rethinking our view of managing controls that can lead to life changing events.

Continued on next page...

The issues are complex because of the uncertainty and unpredictability that humans bring to the equation. For whatever reason we use human error as a way to explain away our inability to manage this uncertainty. Blaming others for something we can't manage gives us comfort in many ways. Humans are not good at foreseeing the potential of something going wrong, but we are all experts in hindsight once it goes wrong.

I constantly remind risk management professionals that we should focus on managing the risk of certainty by controlling hazards. Controlling hazards is essential with health and safety.

Organisations can't control risk, at best they influence risk through rules, knowledge, training and supervision. Risk is in the eye of the beholder.

People make risk decisions every day. We are highly adaptable in our work and how we see the risk in that work. Get a group of people together and you will see a wide range of knowledge and understanding. No two views are the same. We all have varying tolerance, appetite and acceptance of risk, even from a day to day basis. We believe that the more times our work goes right the less it can go wrong. We also believe that something that could have gone wrong today (like a near miss), won't go wrong tomorrow. These biases are part of being human. It is this adaptability that allows people to be unpredictable, we are all prone to fail at some point.

If we control the hazard, we can allow people to fail safely. Embrace failure, it will allow you see risk in a very different way.

BRENT SUTTON

Brent is a member of the Management Board of RiskNZ. He brings over 17 years' experience in occupational risk management and health and safety to Safety Associates. Working in partnership with clients, providing practical advice to address health and safety risks and develop strategies, Brent drives improvements in safety culture. He is well regarded as a safety coach and for assisting clients to understand the importance of safety governance, setting clear and understandable safety objectives, and providing safety leadership.

Brent is also a specialist in H&S critical event management of serious harm and fatality incidents and works with insurers and legal firms on WorkSafe NZ enforcement matters.

TURNING THE INDUCTION INTO A POWERFUL RISK MANAGEMENT TOOL

DAVID TURNER – *Organisational Risk Specialist*

While assessing risk for organisations during the past 15 years I have found one major driver of organisational risk, and this is an inadequate induction.

This makes me think, do we really understand how risk management can form the strong backbone of our organisations, especially when data breaches alone remain high due to human error? After all, people are the organisation and this is the biggest point of failure that needs close care and attention.

We have company policies, compliances, risk frameworks, audits, and … many more procedures. However, many of these are not used because they are often hard to read and understand, with a possible 60% (from what I have seen) not being utilised, not used correctly, or not implemented with due care. These documents are of course important as they form the traditional base line and legal safety net that guides our businesses. True avoidance of issues and the mitigation of risk lie within having relevant policies and procedures that are easily understood, easily taught and passed on, and available to all, combined with a good focus on our people and the way we manage ourselves.

How much care and attention we give to ensuring these documents are relevant, assimilated by all and truly understood can directly equal how much risk we may incur and how much damage that risk causes our organisation.

This leads us to the induction and refresher process for staff, contractors, and visitors who are all key in the management of risk.

Many times this critical induction process is not completed, is delivered too quickly or is presented in a manner which after a short time is quite forgetful. Online inductions have the potential to encourage people to conduct other activities while keeping one eye on the screen. Honesty inductions where you say that you have completed the induction and will provide the proof when needed have the potential to be placed aside in importance, or completed as quickly as possible without adequate assimilation of the information by the participant. Hence the induction process can itself lead to misunderstandings, gaps, and ultimately risk to the organisation. So we need to craft inductions to be engaging, meaningful, and something to remember.

Continued on next page...

To improve the induction and refresher process we need to take time to firstly really know and understand our organisational cultures and the teams that are the life blood of all organisations.

When we know how organisations work and why, then we can create an induction that is relevant and people feel engaged with. In turn this is another form of risk management because it is a simple way to decrease risk and liability through people remembering more and immediately practicing what they are taught.

Below are a few points I have learnt from assessing inductions and refreshers that people remember and help produce the right outcomes. By doing this I have seen risk decrease almost immediately because when people become interested, involved and feel part of something then they remember more of the key messages; this also helps later refresher processes.

- Make the induction and refresher interesting with a good presentation that is very relevant and hits the main points in the first instance, and include key subjects such as cyber security, risk management, health and safety, and personal wellbeing and security.

- It's all about quality so keep the induction within the shortest time period while focusing on the key information you ***need*** to get across, and provide interactive examples where each attendee can comment, ask, and also think about and share their own experiences; this brings more interest and thought to the induction training.

- If you have slides keep them and the words to a minimum to enable only the key messages, pictures and colors to do the talking, and make those images captivating and interesting to make it engaging. In turn this enables risk management to be more front of mind and become a daily habit.

- Include a physical office tour and introduction to staff so better connections are made between the induction theory and what happens on the ground.

- Then, refresh ***all*** staff and contractors in this training each 6 – 12 months.

One thing to keep in mind is to keep accurate records of who was inducted and when. This record keeping needs ownership and can differ depending on how your organisational structure is set up; this may be one manager designated with the responsibility to oversee and manage the induction process, or, a combination that may include human resources, the risk manager, and the security / health and safety manager, whatever may suit your organisation best. However the must have is good ownership and clear direction and management of the induction process.

Induction can be the first step off point into an organisation and getting it right is crucial, so carefully consider the question 'what are the risks to the organisation?' and therefore what do we need to get across within our inductions.

DAVID TURNER

With over 18 years' experience in the risk management industry, David has a unique blend of expertise across diverse areas with a focus on risk management and human behaviour – one of the more complex, dynamic and often over-looked areas of the industry.

Starting his career in the military and later working for government and private organisations, as well as building his own risk management company between 2007 - 2015, gave David an insight into the causes of organisational risk and what is needed to control those risks. This knowledge has enabled him to play critical roles in significant projects across Australia and New Zealand.

ONLINE READING - TWO THOUGHT PROVOKING PIECES

SUE TREZISE – *Sue-lutions Ltd*

Enhancing interactions through Cognitive diversity and Psychological safety

A recent Harvard Business Review (HBR) article reported that the most successful teams are cognitively diverse and psychologically safe. These traits work together to foster high-quality interactions. While the terminology sounds newly ostentatious (to this reader at least!), the underlying definitions are a worthwhile prompt for further enabling risk-based thinking.

Cognitive diversity is the inclusion of people who have different styles of problem-solving and can offer unique perspectives because they think differently. The aim is to achieve a mixture of how people carry out intellectual activities, such as making associations or drawing conclusions.

Psychological safety is the belief that you will not be punished or humiliated for speaking up with ideas, questions, concerns, or mistakes. Without behaviours that create and maintain a level of psychological safety in a group, people do not fully contribute, anxiety rises and defensive behaviour prevails.

It is not just the presence of the positive behaviours that count, it is the corresponding absence of the negative behaviours. We need to encourage ourselves and others to be more curious, inquiring, experimental and nurturing, and to stop being hierarchical, directive, controlling, and conforming. Everyone in the group needs to strengthen and sustain psychological safety through continuous gestures and responses. People can only express their cognitive diversity if it is safe to do so.

This approach is especially relevant for risk practitioners when facilitating risk discussions. The key benefit being that people who bring different perspectives can see threats and opportunities that others may miss. However, this relies on participants being able to express themselves, their thoughts and ideas without fear of social retribution. They need to know it is okay to be forceful at times, where this means having the confidence to persist in expressing what you think is important, without it being perceived as aggressive.

How people choose to behave determines the quality of interaction and the emergent culture. Risk leaders and facilitators need to consider not only how they will act, but just as importantly, how they will *not* act. They need to disturb and disrupt unhelpful patterns of behaviour. Enhanced discourse between people who see things differently leads to a deeper understanding, more creative options, reduced resistance, and strengthened commitment. The results will be reflected in better informed decision making, a healthier working environment and improved business performance.

Source: https://hbr.org/2018/04/the-two-traits-of-the-best-problem-solving-teams

Top risks facing large public companies

The recently issued Gartner report on Risks Facing Large Public Companies (FY 2017-2018) provides a useful benchmark for risk practitioners in both public and private sectors. The report analyses annual disclosures (made to the Securities and Exchange Commission via Form 10-K reports) of S&P 100 public companies to identify and aggregate key risk factors.

The top three risks for each of the key categories are identified below.

Top legal and compliance risks:
1. Litigation and government investigations
2. Regulatory compliance
3. Regulatory change

Top operational risks:
1. Third party and vendor
2. Attraction and retention of talent
3. Natural disasters and extreme weather events

Top strategic risks:
1. Mergers, acquisitions and joint ventures
2. Competition
3. Macroeconomic conditions

Top technology risks:
1. Cyber attack
2. Information security
3. Data privacy

These top risk lists can be used to validate existing organisational risks, prompt a deep dive discussion with executive or senior management teams or potentially highlight emerging/escalating risks for the organisation. It may provide some reassurance where your organisation's risk thinking shows some alignment or trigger conversation where it doesn't (or is not considered relevant).

For the most part, any opportunity for risk engagement should be beneficial.

Source: https://www.gartner.com

SUE TREZISE

SUELUTIONS Ltd
An independent and practical approach

Sue Trezise is an independent risk advisor providing specialist assistance to government, businesses and community organisations. Her cross-sector experience and pragmatic approach help boards, CEOs and managers embed risk thinking to improve strategic decision making and business performance. An experienced facilitator, Sue assists communication between technical experts and non-technical stakeholders and makes managing risk practical and effective.

BUILDING OUR DISASTER RESILIENCE

JO HORROCKS – *Principal Advisor Emergency Management, Ministry of Civil Defence & Emergency Management*

JANE ROLLIN – *Senior Regional Emergency Management Advisor, Ministry of Civil Defence & Emergency Management*

Our increasingly complex risk landscape

New Zealand is exposed to a range of significant hazards and threats. Natural hazards, such as earthquakes, volcanoes, or extreme weather, is only one type. Our economy relies heavily on primary production and is thus vulnerable to adverse impacts from pests and diseases; the potential for an infectious disease pandemic has been highlighted in recent years through the SARS, bird flu and swine flu crises. Heavy reliance on technology and just-in-time supply chains means we are vulnerable to disruption from a wide range of domestic and international sources. The shifting global geopolitical environment means threats to our trading environment, security and economy are complex and often unpredictable.

If realised, these threats can be extremely costly. Globally, the economic cost of disasters has increased steadily over the last 40 years, in largely due to the expansion of the built environment: damage to infrastructure and buildings causes huge cost – public and private – when impacted. Insurance tensions add to this escalating picture.

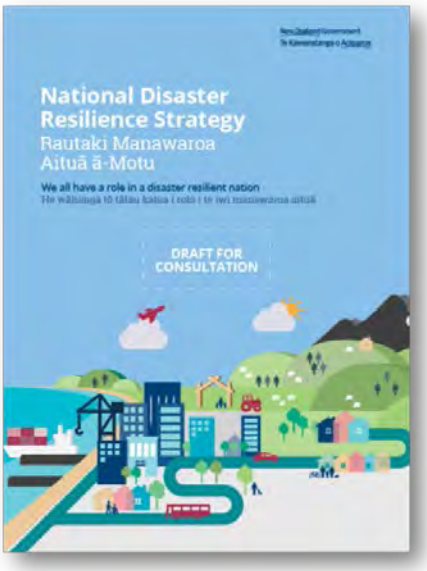
However, it is the impact on wellbeing that can have the most profound effect. In 2011 New Zealand suffered one of its worst ever natural disasters in the 22 February Christchurch earthquake. New Zealand Treasury in 2013 estimated the capital costs to be over $40 billion, the equivalent of 20% of gross domestic product. Beyond the tangible costs of damage and rebuild, lay a web of social and economic disruption and upheaval: flow-on effects to business and employment, psychological trauma, dislocation of communities, creation or exacerbation of existing social issues, disruption to normal lives and livelihoods, and uncertainty in the future.

Resilience is –

a wide range of tolerance to disruption

Many of the risks we face both now and, in the future, can be readily identified. However, we also need to recognise that the future is uncertain: major, unexpected, and hard-to-predict events are inevitable. Moreover, the further we probe into the future, the deeper the level of uncertainty we encounter. Within this uncertain future environment, **resilience** is an important requirement for success. ***Resilience is our – or a system's – ability to anticipate, minimise, absorb, respond to, adapt to, and recover from disruptive events. In essence it's about developing a wide zone of tolerance – the ability to remain effective across a range of future conditions.***

Given our risk landscape, and the uncertainty of the wider domestic and global environment, it is important for us to take deliberate steps to improve our resilience and protect the prosperity and wellbeing of New Zealand – of individuals, communities, businesses, our society, the economy, and the nation as a whole.



Developing a National Disaster Resilience Strategy

It is within this context that the Government, in partnership with a wide range of stakeholders from local government, non-government, business, and civil society, has been developing the framework for a National Disaster Resilience Strategy[1].

The Strategy is made under the mandate of the Civil Defence Emergency Management Act 2002, but has broad intent to strengthen the resilience of New Zealand, so that the hazards, crises, and emergencies we will inevitably face do not become *disasters* that threaten our wellbeing and prosperity.

The Strategy proposes a three-pronged approach to improve our nation's resilience to disasters:

1. **minimising the risks we face and limiting the significance of impacts to be managed in a crisis**
2. **building the capability and capacity to manage emergencies when they do happen, and**
3. **a deliberate effort to strengthen our wider societal resilience to risk and disruption.**

The Strategy promotes a whole-of-nation, whole-of-society approach, and promotes a strong message that "everyone has a role in a disaster resilient nation". It describes a model of a resilient nation, being resilient practices across the social, cultural, economic, built, natural, and governance environments, and at a household/whānau, community, business/organisation, city/district, and national level – a blend of bottom-up, grassroots initiatives, and an enabling and supportive policy environment.

As a document, the Strategy is intended to be the 'common agenda' for resilience that individual organisations, agencies, businesses, and groups can align with for collective impact – a common direction of travel, for improved national resilience in the long term.

[1] The National Disaster Resilience Strategy and other supporting documentation can be found here https://www.civildefence.govt.nz/cdem-sector/plans-and-strategies/proposed-national-disaster-resilience-strategy/

Relevance to businesses and organisations

Managing risk is a core component for any business. Making decisions that acknowledge assumptions and recognise uncertainties inherent in any business planning is becoming increasingly difficult. The recent past is littered with examples of businesses failing to notice or navigate growing global complexity where multiple factors simultaneously disrupt business strategy, operational processes, assets, regulatory environments, global markets, customers and the bottom line.

Effectively managing risk in this setting requires a greater understanding of uncertainty, and a shift from reactive to proactive risk management – there's never been a greater need to engineer a more desired future. Decision-makers need more comprehensive approaches that combine the active management of specific risks with the enhancement of generic resilience.

There are things businesses can do right now to strengthen resilience. How does your organisation consider the following?

Strengthening Resilience: What businesses can do

1. Understand your risk: be aware of your goals, your context, and any hazards or disruptions you could experience. Understand how your assets (people and capital) might be impacted, and the strengths/ resources you have available to manage those disruptions and keep your business on track.
2. Make resilience a strategic objective and embed it in plans and strategies – the continuity and ultimately the prosperity of your business (and the wellbeing your people and customers) depends on it.
3. Invest in organisational resilience by a) reducing and managing the factors that are contributing your risk, b) investing in robust business continuity planning, and c) considering and building your *adaptive capacity* – i.e. your ability to cope with the unexpected.
4. Benefit today, benefit tomorrow: embed risk mitigation, preparedness or contingency solutions that have everyday benefits for your organisation and/or community
5. Consider your social impact: consider how you can contribute to the resilience of your community – in its broadest sense. – Your staff (and maybe your customers) are part of that community, so as well as helping your community, you will also be reducing the risks to your organisation of being disrupted.
6. Keep the long-term in mind: consider the longer-term changes in your environment, for example, the impact of climate change, and how you can position your organisation to see these changes as an opportunity.
7. Collaborate with others and build your network: find others with similar risk and resilience challenges, and collaborate with them – we are stronger together, and you have much to contribute and gain.
8. Learn about response and recovery: understand how response and recovery will work in your district or area of interest, and build your own capacity to respond to and recover from disruption.

How you can help build our nation's resilience to disasters

The National Disaster Resilience Strategy is just the first step in building our resilience to disasters. The real work begins as we seek to embed its messages in our organisations and communities, take action to reduce and manage our risks, and build our adaptive capacity to deal with any kind of disruption that might occur in the future.

Other than refining the document ahead of its anticipated release at the beginning of April, there is a need to develop supporting guidance, tools, and other resources to help communities, businesses, and organisations take the messages and themes of the Strategy and turn them into real action. For this, we need your help! These resources need to be written in language and with context that makes sense to different readers: what appeals to a small business owner will be different to that of a big corporate, or a non-profit, or a government department. You can help develop and shape these resources.

Next year we will be inviting you to participate in small focus groups, workshops, and working groups to develop up a series of short guides and info-sheets. We would love to hear from anyone who is already embarking on their own organisational resilience journey, or those keen to take a leading role in 'translating' the Strategy for use by business. If you have any thoughts generally for effectively spreading the message and implementing the Strategy: all ideas welcome!

In the meantime, please do consider the resilience of your own organisation, and how it contributes, or could contribute, to the resilience of your community, city, district, or the nation as a whole: as they say, "we all have a role in a disaster resilience nation".

Expressions of interest, or for further information, please contact: *nationalstrategy@dpmc.govt.nz*

JO HORROCKS

Jo is a Principal Advisor Emergency Management for the Ministry of Civil Defence & Emergency Management

JANE ROLLIN

Jane is a Senior Regional Emergency Management Advisor for the Ministry of Civil Defence & Emergency Management.

Jane is also a Management Board member of RiskNZ

SAI GLOBAL BLOG: THE WOES OF AIRLINE TRAVEL: LOST LUGGAGE, POOR FOOD AND NOW, DATA BREACHES!

LEE EDGE – *Senior Risk Advisor, SAI Global*

When the first commercial airline took flight, piloted by Tony Jannus, in 1914, 3,000 people gathered at the pier in St. Petersburg, Florida to watch in awe. The flight only lasted 23 minutes and it's fair to assume that Abram C. Pheil, who was a passenger on board, probably wasn't worried about his luggage being lost, subpar food, or that his personal data would be threatened.

Fast-forward to 2018 and passenger planes are not the only thing in the clouds. We have become increasingly reliant on the convenience that internet connectivity brings. Unfortunately, demand for speed and ease of online booking has come at a price for some airline passengers and the carriers they trusted with their personal data.

Might as well place your data on the baggage carousel

British Airways (BA) has been *making headlines* after the airline suffered a malicious breach of its website and mobile app. Around 380,000 payment cards - including the three-digit CVV security code on the back of cards - were compromised during the cyber-attack over a two-week period between 21 August and 5 September 2018. Confusion among BA customers was further compounded by news that the data was almost certainly being traded on the dark web immediately after the attack.

As recently as June - a month after the EU's new General Data Protection Regulation (GDPR) came into force - members of BA's frequent flyer programme received an email reassuring them that: "Your personal information is in safe hands with British Airways. We want you to know you can trust us to respect your privacy and keep your personal information safe."

The BA cyber-attack is not an isolated incident within the airline industry. In fact, it's just the latest in a growing list of data breaches to be reported:

- Air Canada recently confirmed a data breach - including passport details - of its mobile app between 22-24 August 2018, affecting up to 20,000 of its customers.
- In July 2018 it was revealed that a major vulnerability in Thomas Cook Airlines' booking system had exposed the names, email addresses and flight details of customers.
- In May 2018, Atlanta-based carrier Delta Airlines announced that its third-party online chat service had been impacted by a cyber incident between September and October 2017, resulting in customer payment information being compromised.
- In 2016, Korea's second largest airline, Asiana Airlines, confirmed that its website had suffered a security breach, compromising the sensitive information of thousands of its passengers, including passport information, home addresses, bank account details and phone numbers.

So, what are the implications of a cyber-attack and subsequent theft of personal data to both the airlines and their customers?

Sky's the Limit to Your Reputational Damage

Organisations receive and store vast amounts of personal data, bringing the issue of consumer trust to the fore. Established companies like BA build trust over time via proven track records. According to SAI Global's *Consumer Trust Index (CTI)*, a good reputation - even in the absence of direct experience with a company - equated to trust for 76% of consumers.

Hard-earned trust can be fragile, however, even for a company of BA's stature. Particularly when it comes to a private data breach, potentially resulting in identity theft. The CTI reveals that 43% of consumers indicated they would never return to a company if their data had been breached. Put another way, imagine two out of every five customers taking their business elsewhere because of a cyber-attack that could have been avoided.

The real reason behind increased baggage fees

BA could face a hefty fine if found negligent for its handling of the incident. Under GDPR, companies are required to take precautions to protect customer data and notify the relevant authorities of any breaches within 72 hours. If it can be demonstrated that BA didn't do enough to protect the data in question, it could face a fine of up to four per cent of its annual revenue - the airline's total revenue in 2017 was £12.2billion, meaning it could be forced to shell out around £500 million. In addition, *estimates from legal experts* suggest those impacted by the breach could claim up to £1,250 in compensation from BA.

Avoiding the reputational and financial mayday call

By implementing a robust risk management framework, an organisation will provide itself with a solid foundation for avoiding a crisis in the first place, and a better framework for managing one if and when it occurs. This helps the organisation reduce reputational and financial damage. According to the CTI, 47% of consumers agree strongly that trust can be regained by taking responsibility for the issue, ensuring it isn't repeated and providing ongoing high-quality service. Further, 44% of consumers strongly agree that taking time to understand the cause of the issue can regain their trust, and 36% strongly agreed that compensation for the issue can regain their trust.

The provision of clear information to those affected about what happened and the steps they should take to protect themselves is essential in the immediate aftermath of a data breach. Having apologized, BA was quick to explain the nature of the breach and advise concerned customers to contact their banks or credit card providers and follow their advice. Before confirming the issue had been resolved, BA had notified the police and relevant authorities. In terms of financial compensation, BA chief executive Álex Cruz was at pains to stress that "We will work with any customer affected and we will compensate any financial hardship suffered." Companies must take data security seriously to ensure ongoing viability. The most effective means of preventing reputational and financial damage is adopting a proactive approach to cybersecurity detection and response. By stopping data breaches from occurring in the first place, consumer trust in the brand will be protected. And when a cyber-attack does occur, the speed and efficiency of the response is crucial.

To talk to SAI Global about your data privacy requirements visit *www.saiglobal.com*.

SAI360

Integrated Risk Management

In today's complex business landscape, perspective is everything

WHY SAI GLOBAL

SAI Global offers customers an integrated suite of proven risk and compliance solutions to manage and assess their operational and strategic risk and compliance obligations. We bring innovation to integration; combining transparency, accountability, risk agility and ethics to improve your future business outcomes and build your organizations risk culture.

Our solutions are backed by our teams of domain and industry experts globally. We've helped thousands of customers just like you with problems just like yours all over the world for more than 90 years.

Rest easy knowing you have all the insight to advance confidently with SAI Global as your trusted partner.

[Insight] to advance confidently

To find out more visit www.saiglobal.com

SAI GLOBAL

RISKNZ ELECTIONS 2019

NOMINATIONS ARE NOW OPEN FOR THE 2019 RISKNZ MANAGEMENT BOARD ELECTIONS!

We invite you to vote, nominate potential board members or put yourself forward in the coming election.

You have the opportunity to support the continued growth of RiskNZ by standing, nominating, and voting in the 2019 Management Board election. A diverse, skilled and effective Board is crucial for our success and now is the time to actively contribute toward excellent governance and management. This is a great opportunity to cut your teeth in a rewarding governance role.

Two-year terms mean that members elect or re-elect approximately half the Management Board each year. We will elect a Chairman and four Management Board members to take office on 1st March 2019. This is an exciting time to lead the future success of RiskNZ by selecting or becoming a member of the Management Board as it continues to implement new ideas and initiatives:

- Modernising our brand, website, reputation and value proposition to members
- Growing the membership, reach and the professional standards of the organisation
- Improving benefits through more high-quality events and seminars

Please consider this opportunity to lead the future success of RiskNZ.

The Elections Notice, Procedures and Nomination Form can all be viewed in the members only section of the website *http://www.risknz.org.nz/members1/elections-2019/*

Nomination forms are to be completed and returned to the *adminofficer@risknz.org.nz* by **5:00pm Wednesday 19 December 2018.**

RISKNZ

RISKNZ INFORMATION

THE MANAGEMENT BOARD AND OFFICERS OF RISKNZ

Chair:	Nigel Toms	Deputy Chair:	Sally Pulley
Secretary:	Jim Harknett	Executive Officer:	Sathya Mithra Ashok
Treasurer:	Gary Taylor	Administration Officer:	Joanna Beckford

Management Board Members:

Miles Crawford
Kristin Hoskin
Stephen Hunt
Jane Rollin
Brent Sutton
Darroch Todd

INFORMATION FOR CONTRIBUTORS

The next edition of RiskPost will be published late February / early March 2019.

RiskNZ strongly encourages all members to contribute items for this newsletter on practices, developments or issues in your particular area of risk management. Contributions should be sent to editor@risknz.org.nz. Articles are welcome at any time; please contact the editor if you wish to discuss an article. As a reminder, the editor will issue a call for articles for each Edition.

RiskPost provides a service for the display of notices and advertisements that are aligned with RiskNZ's objectives. Members are welcome to submit notices and advertising material to RiskNZ. Notices may describe an activity or service, or advertise a risk management vacancy. Notices should not exceed 150 words of plain text, inclusive of all contact and reference details.

Advertisements can be included in RiskPost and delivered by email to the RiskNZ membership base. RiskNZ's charges for advertising in RiskPost and by email vary dependent upon membership status, and the nature and scale of the advertisement.

For further details on RiskNZ's submissions of notices, advertising, and relevant changes, please send an email to the Administration Officer: adminofficer@risknz.org.nz, or contact the Editor.

RiskNZ
PO Box 5890
Wellington 6140

Membership of RiskNZ is open to any person of good character or an organisation engaged in or with an interest in the practice, study, teaching or application of risk management.

RiskNZ is keen to attract a wide range of Individual and Corporate members representing all the different aspects of risk management knowledge and practice. This includes those with direct involvement in the field and those with a personal or community interest.

Apply online at http://www.risknz.org.nz/join-risknz/

RISKNZ WELCOMES NEW MEMBERS

RiskNZ welcomes the following new Members for this financial year…

Individual Members:

- Ajith Fernando, Operations Risk Manager, EnviroWaste Limited
- David Turner, Principal Consultant, Tregaskis Brown Ltd
- Sarah Enslin, Risk Manager, WorkSafe NZ
- Paul Bishop, Director, Aotearoa Quantity Surveying Ltd
- Paul Quiroga, Postgraduate Student Advisor, University of Auckland
- Marc Armitage, Manager, Intelligent Risks Group
- Truong Nhu Tam Nguyen, Business Student
- David Middleton, Risk Manager, Panuku Development Auckland
- Chris Quest, Risk Specialist, Tauranga City Council
- Tanja Smets, Business Performance Manager, Antarctica NZ
- Debbie Watson, Risk Manager, Whanganui District Council