THE RISK MAGAZINE

Vol 5 April 2019

RMIA
RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

RISK IN 2019

Risk and Risk Culture in our Contemporary World

In this edition...

About the RMIA

The Risk Management Institute of Australasia (RMIA) is the professional industry association for Risk Managers in the Asia Pacific Region. Members of the RMIA are involved in every sector of the community and economy.

The RMIA has over 30 years' experience in representing the practise of risk management. We facilitate linkages between members and offer continuing professional development opportunities via our Annual Conference, Best Practise Guides, Special Interest Groups, Chapter Networking Events and Education Programs.

Partners & Sponsors

riskware
Enterprise Risk Intelligence Software

Swiss Re
Corporate Solutions

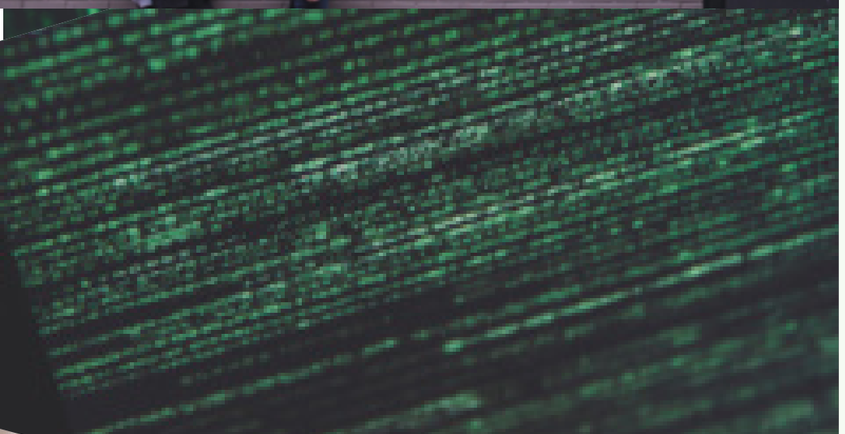
KPMG

PROTECHT.
LEADERSHIP IN RISK SOLUTIONS

SAI GLOBAL

LexisNexis

GROSVENOR engineering group
innovative | intelligent | sustainable



In This Issue

Risk Management Institute of Australasia
Suite 602A 97 Pacific Highway
North Sydney, NSW 2060
02 9095 2500

Editor
Andrew Lynch & Louise Rogers
marketing@rmia.org.au
02 9095 2501

A Note From the CEO

2019 has certainly had an exciting start for RMIA. We can see the momentum building already with solid membership growth and a record number of early bird bookings for the Conference in Melbourne (Nov 13-15).

We started the year with the highly successful Women in Risk Event Series in Sydney, Canberra and Brisbane to record attendances. Two of the events were Sold Out and had some incredible speakers share their insights and experiences in the industry.

Planning is well under way for the RMIA Keynote Tour in August with the first date announced for the 8th of August in Sydney. The Risk Manager of the Year (RMOY) Tour kicksoff in May and will be travelling to Sydney, Melbourne, Brisbane and will finish off in Perth mid June.

The Chapters are now busy working on their Odyssey's and other events.

The RMIA AGM will be held on the 22 May, ready to look forward to a new period of growth of the RMIA.

Thank you to the contributors for your submissions and we encourage others to participate in future editions!

Andrew Lynch
General Manager

In 2019, will the Risk Team finally accept responsibility for Corporate Success and Failure?

By: Mark Brown VP and Senior Risk Practitioner **Sword GRC**

"Look, if you only had one shot, or one opportunity to seize everything you ever wanted, in one moment. Would you capture it, or just let it slip?" Eminem 2002

It sounds like a risk, right? One opportunity and one moment. As risk managers we don't like risks unless we can influence the underlying likelihood or impact of that risk. Whereas entrepreneurs love them – after all that is how they make their fortunes!

As risk managers we want to analyse, assess and plan for what the business does about risks, to help manage the future performance of the business. However, we need to present that analysis to directors in such a way that it helps them to understand potential future performance volatility. Often, we mask the value of what we do in helping the board comprehend future performance, because in most cases each GRC functional head produces their own report on safety, compliance, projects, quality, IT, financial control and so on.

While it is understandable that everyone wants to demonstrate the value they are adding to the business, these separate reports do not help the board understand the consolidated view of this information in risk/reward terms as measured by the risk appetite of the business.

Rather they are being forced to consider the investment case in each function rather than a single investment decision against the corporate goals and objectives of the business within a common economic model.

For example, do we invest in a new product that may deliver an additional 5% of cashflows over the next 10 years or invest the same amount in reducing the likelihood for a major risk(s) that could impact business performance by more than 10%. Both decisions have uncertainty involved and you can't do both.

Funding is limited, so the investment case therefore needs to be made on a like for like basis. A Risk/Reward basis. To do this all risk information needs to be consolidated and mapped to the goals and objectives of the business as defined in both the ISO 31000 and COSOS ERM frameworks

If the directors are not making these investment decisions on this risk/reward basis then they will be in immediate conflict with their shareholders who are applying their own investment criteria in which companies to invest in (based on the "Efficient Frontier" first introduced in 1952 by Harry Markowitz but still a fundamental technique in corporate finance).

To do this the board needs access to consolidated risk/reward investment case information that they can make decisions on, in a common format, using consistent assessment methods and well-articulated information.

The difficulty in doing this is when the different GRC functions are assessing their risks in different ways. For instance:

- **Health & Safety: Hazards are often assessed on a Likelihood** * Detectability * Business Impact basis using Unmitigated and Mitigated RPN Risk levels

- **Cyber Risk: Often assessed on an Asset** * Threat * Vulnerability * Business Impact basis using Inherent, Current and Planned Risk levels

- Compliance Risk: Often assessed on a Severity * Frequency basis, but often just 'Risk' using Current and Planned levels

- Supply Chain Risk: Mostly assessed on simply 'Risk' using a Current level only

- Project Risk: Both qualitative and quantitative assessments on Probability * Impact basis including Schedule impact and management reserve based on a Pre and Post mitigation basis

- Pharma Product Risk: Assessed on a Probability *Severity * Detectability basis using an Inherent and Managed Risk levels

And then the crazy ones. Here is the risk assessment model for one EH&S risk assessment we have worked with !

$$\left(\left(\frac{(P x E)}{25}\right) x\, 5\right) x \left(Hm(40\%) + Cr(40\%) + Rp(20\%)\right) = Total\ Risk\ Score$$

So, with these differences in assessing risks across the business the challenge is how are these different risk types consolidated into a single view of risk to enable company directors to make the best risk/reward investment decisions across multiple investment cases?

Who is going to stand up and seize the opportunity to consolidate this into a single set of risk information for the board? That one shot, that one opportunity? Or will you let the opportunity slip? Is there a hero out there?

As a GRC professional maybe it is you that can make this revelation and deliver this value within your organisation. The methodology is easy in comparison to the organisational challenges you will face, but the reward is certainly there for the leaders.

Mark Brown, VP and Senior Risk Practitioner at Sword GRC will be presenting the practicalities of a single view of risk at the RMIA conference in Melbourne in November.

Photographer: Benjamin Cruz

Photographer: Daria Shevtsova

Climate Change Risks to Australian Businesses

By: Ben Scheltus Continuity Matters Pty Ltd

The starting point for this article is Section 180 of the Corporations Act 2001. The s180 specifically addresses how directors and officers of a company should make business judgments in good faith and inform themselves appropriately.

The information that directors could easily access has been supplied by the World Economic Forum's Global Risks Report (GRR). For three years in a row, the GRR has called out the risks we collectively face from climate change. In the 2019 report published in February, climate change and environmental risks dominate the "high likelihood" and "high impact" quadrant of the global risk matrix. The report goes into great detail explaining the multi-faceted nature of this risk and our diminishing ability to mitigate its impacts.

Alison Martin, Group Chief Risk Officer, Zurich Insurance Group, said: "2018 was sadly a year of historic wildfires, continued heavy flooding and increasing greenhouse gas emissions. It is no surprise that in 2019, environmental risks once again dominate the list of major concerns. So, too, does the growing likelihood of environmental policy failure or a lack of timely policy implementation. To effectively respond to climate change requires a significant increase in infrastructure to adapt to this new environment and transition to a low-carbon economy. By 2040, the investment gap in global infrastructure is forecast to reach $18 trillion against a projected requirement of $97 trillion. Against this backdrop, we strongly recommend that businesses develop a climate resilience adaptation strategy and act on it now."

Figure 1: Davos, Switzerland

This article will take a high level view of this risk through the lens of business continuity. The challenge is that climate change risk has the potential of disrupting the operations of many different types of businesses and a serious disruption in one sector could impact others. For example, a serious disruption to power generation in Victoria recently resulted in large scale load shedding of power supplies to Melbourne consumers.

The authors of the GRR have proven to be accurate in their warnings. Since the beginning of the year, businesses all over the world have been impacted by severe weather, fires, polar vortices and floods. Australia has been no exception. The full impact of the extraordinary floods in Townsville is still being calculated.

If your business has a high reliance on power, the efficient movement of goods through ports, availability of quality water and temperate weather – then you need to start planning for the impact of the risks presented by climate change.

Many years ago Australia signed an International Energy Agency agreement to hold 90 days' use of energy (oil) inventory, but it has consistently failed to honour its commitment. The conclusion of Australian Parliament Report in 2015 on Australia's transport energy resilience and sustainability, estimated that we had 20 days of automotive gasoline, 17 days of aviation fuel and 16 days of diesel oil.

The latest IEA data shows we currently have 55 days of inventory, by far the lowest of other comparable countries. Australia has reduced its crude oil refining capacity and it is likely it will continue to shutdown existing refinery capacity. The Parliament Committee report concluded that by 2030, we will have 20 days inventory, no refineries and 100% imported fuel dependency.

Even a short disruption to Australia's importation of crude oil products would have a significant impact on national productivity, supply chains and civil society.

A disruption to our ports could equally impact our exports. We are heavily dependent on the revenues earned through the export of minerals, LPG and grains. The GRR found that "Half of all internationally traded grain must pass through at least one of 14 major chokepoints and over 10% depends on a maritime chokepoint to which there is no viable alternative route."

The GRR devoted a chapter solely to the outlook of cities and the impact of sea level rise. Rapidly growing cities are making more people vulnerable to rising sea levels. Two-thirds of the global population is expected to live in cities by 2050. Already an estimated 800 million people in more than 570 coastal cities are vulnerable to a sea-level rise of 0.5 metres by 2050. Cities are carrying the burden of population growth and this trend magnifies the risk. Not only are there more people at risk in a given area - but there is also more costly infrastructure at risk.

Figure 2: Sunny day flooding, Miami October 2016

In 2012, the impact of hurricane Sandy on New York devastated many communities and resulted in extensve repairs to the city's infrastructure. Miami now regularly experiences "sunny day flooding" due to sea level rise; for many years the residents in Byron Bay have lost part of their properties to the sea and Pacific Islanders face an existential threat from sea level rise.

Mark Carney, the Governor of the Bank of England was concerned about the exposure of the UK insurance industry to the risks presented by climate change. Under the leadership of Michael Bloomberg, the Task Force on Climate related Financial Disclosures was established in 2016.

It develops voluntary, consistent climate-related financial risk disclosures for use by companies in providing information to investors, lenders, insurers, and other stakeholders.

TCFD | TASK FORCE ON CLIMATE-RELATED FINANCIAL DISCLOSURES

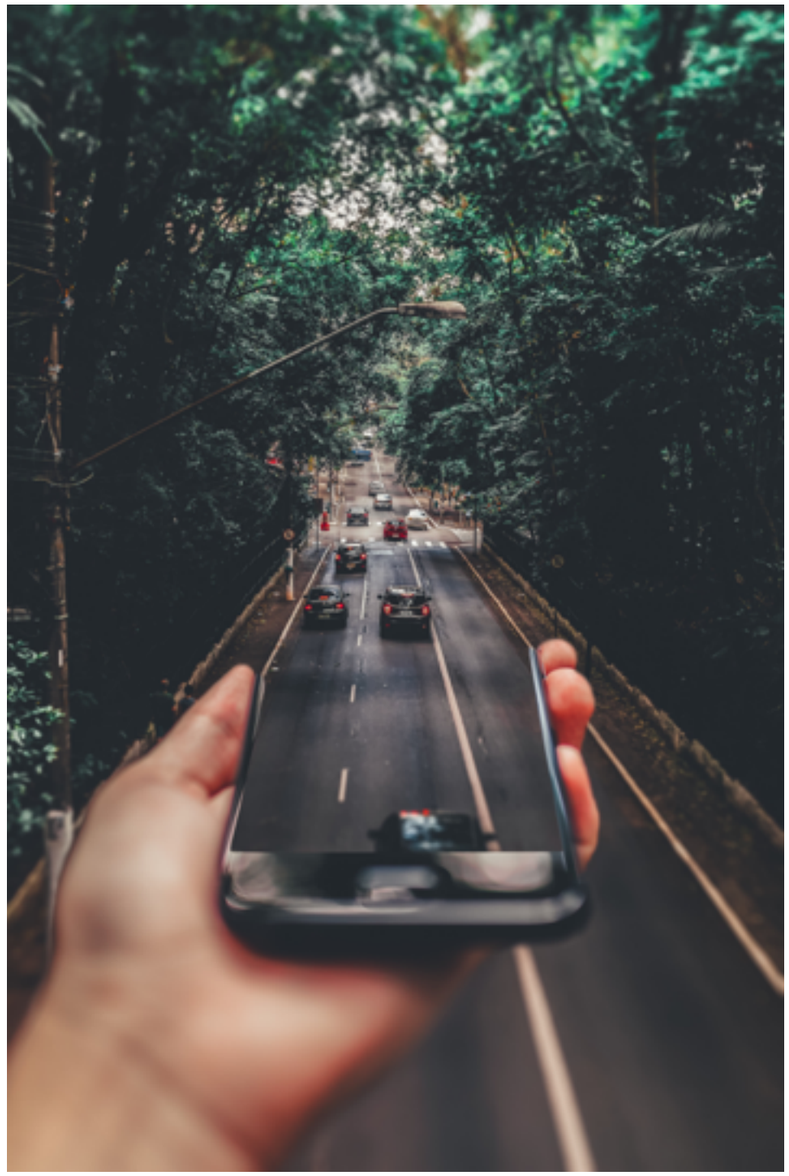
The Task Force considers the physical, liability and transition risks associated with climate change and what constitutes effective financial disclosures across industries. The Task Force has had a fundamental impact on the way financial institutions report their exposure and manage their risks. BHP has used the approach in their 2017/18 Annual Report.

Importantly, the approach addresses direct physical risks and the risk to business due to the transition that is required to mitigate the risk. For example, the Australian power generation industry is undergoing substantial change because of the need to de-carbonise the production of electricity. Similar disruption can be expected in the transport industry – with electric driverless vehicles. The approach promoted by the Task Force is quite generic and is applicable across all industry sectors.

Tackling this global problem requires strong collaboration between Governments. Unfortunately, the US Government has reneged on the Paris Accord, the UK is completely distracted by Brexit and some EU countries are experiencing serious internal disruptions. At best, Australian Governments have a spotted record in the area of climate change policy. China is moving forward aggressively and appears to be cementing its position as the world's primary supplier of renewable energy products.

We can only hope that Governments will collectively agree to reduce emissions to keep global temperatures below 2oC. As we have found this summer, parts of Australia have already experienced warming above this target. The BoM reported that January 2019 was warmest on record for Australia and warmest or second-warmest for each State and Territory. Many records were broken across the country.

If you have developed a business continuity strategy for your business, you may need to go back and review your plans in light of the multi-faceted risks presented by climate change.



Photographer: Matheus Bertelli

Tips on setting your Business Interption Insurance Maximum Indemnity Period

By: Peter Newall Senior Claims Manager **Swiss Re**

Time can pass quickly when recovering from a disaster...beware the Maximum Indemnity Period

Business Interruption policies are unique in that they require both a sum insured and a Maximum Indemnity Period (MIP). Through our conversations with risk and insurance professionals, it is evident that accurately establishing the Business Interruption value with an adequate sum insured and an appropriate Maximum Indemnity Period is a constant challenge.

In this article, we show how your Earnings Statement can be impacted when a Maximum Indemnity Period expires and list some of the tips to help you ensure your organization is not underinsured and can fully recover following a loss.

To start with, it's important to specify what we mean by a Maximum Indemnity Period. The MIP in a Business Interruption Insurance policy is a limited post-incident period for which an insurer will indemnify its client for financial loss.

A RIMS survey in 2017 on Business Interruption insurance highlighted the Maximum Indemnity Periods selected by risk professional s (pictured below).

Maximum Indemnity Periods may extend to 60 months. However, what is important is that once the period has elapsed, any further loss of profit is no longer insured. Therefore calculating a correct sum insured for the worst and most likely losses is critical to helping your business reestablish itself post-loss.

What can go wrong? Business Interruption auto supply chain disruption. Unfortunately, all too frequently we see claims where an inadequate MIP has been set. Inadequate Maximum Indemnity Periods leave a gap where the replacement of assets and the business recovery period extend beyond the MIP stated in the policy.

The following example highlights the need for robust loss scenario and business continuity planning prior to selecting the Maximum Indemnity Period.

Background

A client operated an auto parts manufacturing business in an industrial park in Thailand. During the 2011 floods the entire industrial park was flooded, which caused extensive damage to the Insured's property, including their production machines.

While the client had previously conducted Maximum Foreseeable Loss scenario modelling, they had assumed that the replacement of the production machines was not on the critical path and that these could be readi-ly replaced more rapidly than building damage could be repaired. Consequently, the Maximum Indemnity Period was six months in the Business Interruption insurance policy.

Challenge

Following the loss, the client approached the machine manufacturer for a quotation and projected lead time for the fabrication, installation and commissioning of the replacement machines. Unfortunately, owing to the widespread nature of the flooding, many competitors and other manufacturers in similar industries also had similar needs and got in first. As such the client was obliged to wait six months longer than the usual three month lead time for the replacement machines to be delivered.

Impact

Manufacturing ground to a standstill as a result of the flooding and the revenue stream stopped. The building and other services were reinstated within the six month Maximum Indemnity Period, but the production ma-chines did not arrive on site until three months after the Maximum Indemnity Period had expired resulting in an uninsured Business Interruption loss over three months after the reinstatement of the buildings.

The Business Interruption loss during the Maximum Indemnity Period amounted to some USD6 million. However, an uninsured loss of some USD3 million was incurred outside the Maximum Indemnity as the busi-ness was restored.

A further blow was encountered when competitors were able to reinstate faster and attract market share away from the client, thereby seriously impeding the resumption of normal business operations and previous mar-ket position.

Key learnings

• The Maximum Indemnity Period selection must be considered carefully and the critical path analysed thoroughly. Thought should be applied to critical supplies and the reality of where your organisation lies within your key suppliers' priorities.

• Maximum Foreseeable Loss modelling should be undertaken for all businesses prior to setting the Maximum Indemnity Period. Don't just think about fire, also consider the ramifications of how a Natural Catastrophe (NatCat) event, such as flood, cyclone or earthquake could impact your premises and the surrounding area.

• Scenario modelling should also be considered prior to setting the Maximum Indemnity Period. This should also address elements of the critical path of reinstatement and repair of assets and the assumptions utilised in the model should be stress tested for potential external impacts.

• Wide area damage can result in delays due to increased demand for loss adjustors, contractors, specialized equipment etc and larger companies may get preferential treatment due to spending power.

Reinstatement is only one part of the puzzle

As illustrated in the above case study unforeseen circumstances can lead to uninsured losses. In other claims situations we've seen clients being able to recover and repair machinery and buildings quickly, but being unable to recover lost business. This may be due to contract cancellations or perhaps even a lag in post-loss demand.

Business Interruption Insurance policies are specifically designed to encompass this and provide financial assistance that a business would need to return to its previous pre-loss state. This can include overtime wag-es for employees, additional promotional expense incurred to win back contracts as well as accelerating the installation of new equipment.

As a result, Business Interruption MIPs must take into account not only the time for reinstatement, but also the time taken to restore the business to its pre-loss state, which is often overlooked.

Tips on setting your Maximum Indemnity Period (MIP)

Determining the appropriate MIP is a significant challenge that requires a full understanding of the business operations and its interdependencies and must be done in consultation with relevant business departments. As well as internal factors, external influences must also be understood and analysed, for example customer supply, denial of access, wide area damage effects, infrastructure damage and many more.

From our conversations with PARIMA members, the default MIP seems to be 12 months, however, 18 month and 24 month Maximum Indemnity Periods are not uncommon. Never-the-less, we found that there was an underlying concern amongst members over the difficulty in combining asset replacement timelines with the business sensitivities, impact and recovery.

In addition, several advised that the MIP was an historic selection that had been in place for many years, being simply renewed on a rolling basis. Even lessons learned from previous losses tended to be overlooked.

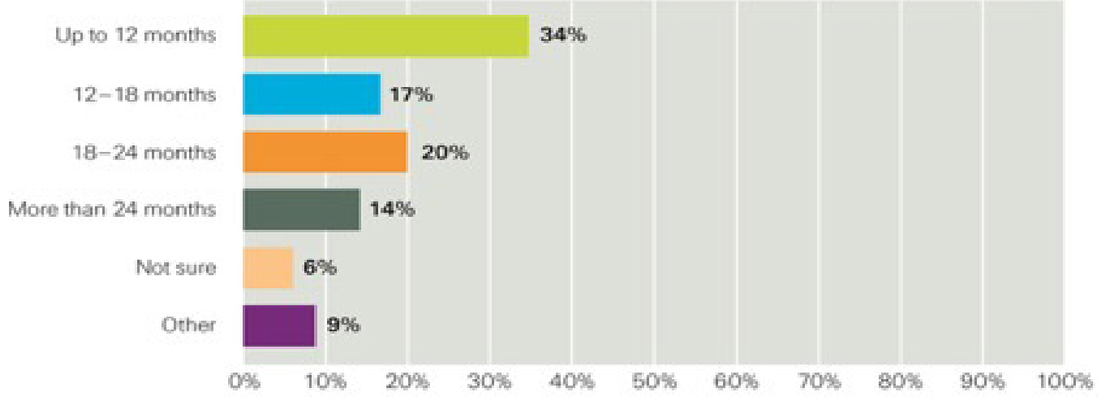
Swiss Re Corporate Solutions strongly advocates that corporate risk and insurance professionals consider working with brokers, insurers and loss adjusters with Business Continuity experience, to run in-depth sce-nario planning when assessing their indemnity period. Although the default selection tends to be 12 months, like many international insurers, we are able to offer an MIP of 36 months and 48 months for petrochemical and complex property risks. However, some factors to think about when calculating your MIP and running a pre-loss analysis exercise include:

• Critical involvement of senior business management and technical department heads with the risk man-agement department.

• The company's exposure to man-made risks such as fire and explosion as well as Natural Catastrophes (including those of your suppliers).

• Any Health and Safety considerations such as potential civil authority intervention and any environmental investigations, for example incidents involving fatalities.

• Supply chain vulnerabilities – criticality; who; where; inventory levels.



• Critical infrastructural damage to power, water, roads, ports, airports, bridges etc that prevents business operation.

•Possible loss mitigation measures and backup facility access and availability in the case of a breakdown.

•Existing production machinery configuration and bottlenecks. Parallel production techniques can reduce vulnerabilities to malfunctions and breakdown.

• Probable repair/response times for critical machines, installations and buildings.

• Lead times for spare parts or replacement machines.

• Dependency on computers process control, certain interrelated operational factors and special environmental conditions, such as clean rooms or temperature-controlled climates.

• Read your Business Interruption Insurance policy (nobody ever does in enough detail) and note limits, deductibles and indemnity periods as well as insured perils and exclusions.

•Review scenario and potential loss assumptions against the Business Interruption policy to identify gaps.

Note: The list above is not intended to be exhaustive. It will vary by industry and unique exposures, however it does serve as a good starting point when determining your MIP.

Getting it right

Business Interruption Insurance policies do make a huge difference to whether an organization can fully recover after a serious loss. Fundamental to this, is setting an adequate MIP. In order to do this it is impera-tive that risk management has proper Business Continuity Plans, clearly

identifying the exposures and how the organization will respond to those events, be it a fire, flood, cyclone or other NatCat, a breakdown of ma-chinery, terrorist or cyber-attack or any other form of disruption. Without this thorough planning and atten-tion to detail it is unlikely that the MIP can be properly assessed and set.

In my experience of Business Interruption claims over the last 40 years (I know you're thinking surely not looking at my profile picture) I've seen management being overly optimistic about post loss recovery. This is where risk professionals can help demonstrate what can go wrong and help you avoid the traps that can im-pact Business Interruption Insurance claims.

As with the case study above, even the best laid plans can go awry and time can fly by as a result of unfore-seen circumstances – all of which can impact your recovery.

Reducing the Financial Burden of Security

How SMBs can build their defences

By: Matt Bunker Co-Founder & Managing Director **ARX Risk**

Photograhy: Burst

The number of security breaches occurring throughout larger enterprise and SMB continue to rise. What's concerning is that these breaches still occur regardless of the millions of dollars that some larger enterprise spend on the latest IDS / IPS, DLP, SIEM, firewalls etc. The breaches we hear about are generally reported due to either the sheer scale of the breach and/or who the corporation is, but the ones we don't hear about are the breaches happening in small to medium business (SMB) every day. Larger corporations generally have the resources and time to undergo a period of review, change their branding and offer free services to their customers to make up for the financial and reputational damage. In essence having the marketing resources to turn a negative into a positive.

SMBs don't have the same level of resources and capacity that larger corporations have, therefore, the effects of a breach can be amplified to the point of catastrophic consequences. There is a good quote in the 2018 CISCO Threat Report that said "Small to medium business are dynamic – the backbone of innovation and the poster child of hard work. They run even faster and work even harder than enterprise peers and they are exposed to the same cyber threats". Whilst they are exposed to the same cyber threats it is in fact on a bigger scale. It probably wouldn't surprise you to know that 58% of all cyber attacks are against SMB and that the majority of those breaches are actually less likely to be technical issues as they are to be one or a combination of a human, process and strategy issue.

The predictions aren't any better. According to Allianz the current global standalone cyber insurance market is at around $2bn - $3bn in premiums, and could reach $20bn by 2025. It is estimated by 2021 cyber-crime will cost the global economy $6 trillion. Ransomware damages alone are on track to hit $11.5 billion in 2019, at which point it is estimated that a business will fall victim to a Ransomware attack every 14 seconds. Globally, the average cost of a cyber breach to a SMB is $2.2 million. Furthermore, the number of IoTs outweigh the human population, therefore, significantly increasing our threat surface without increasing our protective measures. So, with all the statistics and fear surrounding breaches why are they still occurring on such a significant scale? Especially, when we are seeing incredible developments in AI based AV software, firewall and detection technology etc. It really boils down to three key areas for SMBs:

NIMO – Not in my Organisation

SMB often feel they are not worth the attention or are somewhat less of an attractive target than larger corporations and, therefore, don't need to adhere to the warnings. Not only do the statistics prove that assumption incorrect but it's that exact attitude that the threats are looking to exploit. The scary thing is that it may not even be a tangible threat that breaches your company's defences, such as a network of bots acting to harvest the computing power for bitcoin mining or run DDoS attacks against another organisation. The issue with a NIMO attitude means that the solution to a breach is reactive, and when you are time and resource poor it's too late. Research conducted by the Economist Intelligence Unit highlights that a proactive security strategy reduces the likelihood of a breach by 53%.

Understanding the threat

This goes hand in hand with NIMO. Whilst SMB feel they are a less attractive target and not worthy of the attention, the threat thinks the exact opposite. There are two things that SMB need to understand when developing their threat assessment. The first is they offer easy gains to criminals, who are less likely to be pursued by authorities than if they had breached a larger well-known corporation. The second and most important aspect is that SMB are a means to an end. A stepping stone so to speak that enables the threats to land the bigger targets or as I discussed early, covertly harvested your computing power to conduct a DDoS attack on another organisation.

Cost

Establishing a secure framework to protect critical business assets is largely seen as expensive and outside the scope of SMB knowledge, skills and expertise. It has been mentioned that there have been and continues to be incredible advances in threat prevention and detection technologies, but they do not come cheap. The costs rise quickly especially when added to data storage, hardware, software, maintenance, IT support requirements etc. It is understandable that operational, marketing and growth costs etc. are given

priority. However, breaches are less likely to be a technical issue than they are to be a human, process or strategy issue. That's because organisations are failing to identify the root causes to their issues and largely think that they need to apply expensive technology-based solutions. The cost and benefit of conducting staff awareness training, instigating a change in strategy and culture (leadership) or developing interactive procedures outweighs expensive standalone technologies.

The threat landscape is only going to become more complex. Advances in bandwidth and mobile technology is making it far easier for employees to transfer data on the move, therefore, creating more attack opportunities. The proliferation of IoTs has also significantly increased the attack vectors. People are becoming more transient looking for better opportunities, pay and promotions. Gone are the days where an employee remains with the same company for years on end. The end state is the loss / transfer / theft of your company's valuable IP / sensitive information to the competition, all because the controls (cost effective and easy to implement) were not in place to protect it.

Especially concerning is the lack of understanding about our "real lives" versus our "digital profiles". People see themselves as separate to their digital personas and are protective of that as personal space. However, they are far from separate and the connection between the personal profile to the work profile is interconnected, making it easy for threats to exploit and move laterally from one to the other.

Equally concerning is when you hear about SMB breaches, because the root causes are on the whole relatively easy to fix. What's harder to change, is the mindset and culture. It is not an overnight process but one that needs to be implemented from the top with good leadership and driven from the bottom by a workforce with a strong security culture.

ARX has asked a number of CEOs and executives the same question – "How do you make the decision makers value the money they haven't had to spend". Because, when a breach occurs it is not just about the cost of first order effects. It's the damage to reputation, lost revenue, loss of trust, breach of privacy laws, lost investment in IP, delays in production / capability milestones, failed mergers and acquisitions, legal fees and the list goes on. It is the cost of the second and third order effects that mount up, compound and drive SMB's under. The best answer I got was, CEOs walk a tight rope each day, where it becomes a balancing act and gravitational fight between governance, finance, human resources, security and operational requirements. So, it is easy to see from this analogy that priorities often fall elsewhere and the thing that actually hasn't happened yet, gets put to the back of the line.

Here's the thing that gets misunderstood by SMB and for that matter larger enterprise. Improvements or enhancing your security framework don't need to be financially burdensome or require employing the most advanced, thus expensive, technologies. Examining what the root causes are to the issues, developing sound strategy and changing human processes are the most effective measures. Yes, it requires hard work and time, but the payoffs of being proactive can reduce the financial effects of a reactive approach significantly.

The first step in ARX Risk's proactive approach is to understand the threat environment, specific to your operational market, this will allow you to focus resources and efforts in the right areas. We call this economy of effort. To often organisations apply a scattered approach to applying security controls, mostly technology, without properly assessing where the vulnerabilities actually are. This leads to inefficiencies and unnecessary over spend.

The second step is to understand exactly what you need to protect by asking the following four questions:

What do I need to protect?

Why do I need to protect it?

When do I need to protect it?

Where do I need to protect it?

Essentially, this step is about defining what your critical business assets are. At ARX Risk we define critical business assets as: Infrastructure (technical and non-technical); Personnel and Intellectual Property (this includes sensitive information). It is important to remember that critical assets are not necessarily fixed. Therefore, the security framework you have in place needs to be fluid and flexible, capable of creating a mobile security bubble that extends beyond the organisation's walls but has connective tissue with the organisation. A good example is how our Military and Intelligence Services protect our national interests. Operations to defend those interests don't just stop at our borders. Our Military and Intelligence Services work tirelessly beyond our borders to protect what's within them.

The third step is to test your threat assessment against your existing security controls to determine if you are actually protecting your critical assets. The following is a set of principles that we recommend you use when testing your existing framework:

You're only as secure as your weakest link

Just as the 2018 CISCO Threat Report highlighted, SMBs run even faster and work even harder than their enterprise peers. Often to achieve that level and competitive advantage they utilise third parties to support their operational outputs (MSP, contractors, supply chain facilitation etc). Understanding how others are treating your information and access, within their own organisations, to your information is probably one of the most important aspects of building the right security framework.

Put yourself in the shoes of the threat then ask yourself: Why would I go after one SMB when I can go after the MSP that supports 80 SMB? The Australian Cyber Security Centre has released some good examples of questions organisations should be asking of their MSP. These also apply for other interested parties that have potential access to your critical assets.

Integration of controls

At ARX we refer to this as the "one is none" principle. Its Murphy's Law that when you need something to work it won't. That's why contingency planning is critical to operational success. Technology alone will not protect your critical assets. The technology must be integrated with human and physical controls. Otherwise it is just a standalone procedure that can be exploited by the threats.

Interactive within the workforce

The policies, procedures and controls you have in place must be interactive, so that people thoroughly understand all aspects of why they are employed and what they are trying to achieve. Where applicable, those in technical positions need to know how a control is engineered, its vulnerabilities and the procedures required to operate it. It becomes much easier to implement a policy and procedure when your workforce understands why it is important.

Interoperability

Whatever controls or procedures are in place, they should be interoperable with the organisation's operational processes so as not to impede its agility. Additionally, they must be focused in the right areas – economy of effort.

Failure breeds success

Training to failure will build your organisational resilience. Only when you know how and why something is broken can you know how to fix it. Testing your procedures, policies and controls through realistic and purpose designed training will allow you to identify where the improves and fixes are required. This continuous improvement philosophy in championing your organisation's security framework will significantly improve the chances of success when you are faced with challenges.

Culture is king

Fundamentally this is the most important principle. The right security culture within an organisation is developed through sound leadership but maintained by the employees. Handing over responsibility to the employees to drive that culture will give them a sense of ownership. That ownership and responsibility is what creates the willingness to address issues when they happen or become more situationally aware, because they are protecting something that has a tangible effect to their job security.

Summary

There is no doubt that the threat landscape will continue to become more complex by the day. In order to effectively mitigate the threat, it is important that organisations and leaders re-evaluate how their defences are laid out and whether there is an insular reliance on technology over a defence in depth approach that encompasses the full spectrum of security controls. Specifically, there are some key takeaways for SMB to reduce the likelihood of their exposure and exploitation.

•Your organisation is not immune. You need to think that you are more likely to be breached. The statistics prove it.

•Remember a "breach" is not just outsider hackers – internal mistakes are also 50% of security breaches.

•Before you can effectively implement technology-based solutions, you need to understand the threats, what you are protecting and what your overall strategy / mission is.

•Establishing a security framework does not need to be a financial burden. Leaders who own problems and employees with the right culture is the best form of defence.

•If you don't know how third parties are protecting your information then you are not protecting your information.

•Be proactive not reactive.

Ultimately CEOs and executives need to ask themselves - Have we taken the appropriate measures to mitigate the threats? If you haven't and a breach occurs, what confidence will the board of directors and shareholders have in your ability to prevent future breaches, how much will your reputation and personal brand be damaged?

In the next edition we will take a deeper look at the principles to help SMBs protect their critical assets.

Scandal, Business Transformation and the Risk Professional: 2019 and Beyond

By: Darren O'Connel Manager, Governance & Risk **Blue Mountains City Council**

The Australian financial services industry limped out of 2018 battered, bruised but not completely beaten down. It faces 2019 with an urgent need to rebuild and transform its business as it fights to salvage its reputation. While the Financial Services Royal Commission (RC) was a high profile examination into questionable practices, many other organisations, both in the public and private sectors, also ran afoul of basic standards of governance. They too are currently paying a hefty price in terms of bottom line hits and reputational damage.

As the RC observed, culture and governance practices in the financial services industry were deficient which, more broadly, enables bad behaviour to come into existence and flourish unchecked. Not all of the examples of misconduct cited in the commissioner's final report were illegal per se but many were the result of employees, managers and directors failing to follow their organisation's established governance norms (e.g. code of conduct). The corollary, of course, is why weren't the risk professionals more effective in identifying transgressions, raising them to the top of the organisation, or if stymied vertically, shunt them horizontally to the oversight committee?

The hiring patterns of 2018 provide a clue. It was evident shortly after the RC commenced that the financial services industry perceived that culture and governance capability and effectiveness would be embarrassingly exposed. Proactively, many firms began addressing their capability deficiency by hiring risk professionals in ever increasing numbers. As noted by the Australian Financial Review in June 2018, the uptick in demand was difficult to satisfy as the current talent pool was not particularly deep. Indeed, as I noticed during the second half of 2018, the number of risk management jobs advertised on Seek jumped significantly and the once strict employment qualification of "X" number of year's industry experience was gradually relaxed in order to attract more candidates. The demand also led to an increase in remuneration for risk professionals who were given mandates to improve governance culture and practice.

As organisations in every industry, sector and size came to terms with the scandals that have plagued them, it has become evident after much soul searching (and root cause analysis) that existing corporate structures and business models weren't conducive to an ethical workplace. Consequently, they are now embarking on large-scale business transformation projects. In the financial services industry, we've already seen ANZ, CBA and NAB divest their wealth management business as they came to (belatedly) understand the inherent conflict of interest between product providers and sellers . In government administration, the NSW Department of industry restructured part of itself following the 2017 water licenses scandal and it is likely that the Blue Mountains City Council will be forced to change its operating model due to the ongoing drama with asbestos breaches .

What does business transformation mean to the mandate of risk professionals? It's an exciting time and there are many avenues now available to pursue. Firstly, there is an opportunity to get a "seat at the table" in order to reinvigorate the organisation's commitment to an ethical workplace and sound governance practices. For example, prior to the water licenses scandal, the governance function at the NSW Department of Industry was tacked onto a diametrically opposite function and buried deep down inside a shared services division. Perusing the organisational structure suggested the department had no governance function at all. Post scandal, the team was hived off to the Office of the Secretary and given a clear mandate. In early 2019, NAB was actively recruiting for risk professionals (industry experience? Nice to have) to help manage the sale of its MLC business and they were cited at the very heart of the project.

Secondly, with the appropriate seniority now recognised, the governance and risk professional is able to provide expert strategic advice to the C-suite decision makers about the threats and opportunities not just to business transformation but also to the achievement of wider strategic objectives. Being accountable to the top of the organisation will provide the moral impetus to embed risk management practices into business-as-usual activities thereby driving greater accountability from staff.

Thirdly, there will be a greater focus on the effectiveness of independent boards and committees. Indeed, the RC noted that the CBA's audit committee, when presented with a third 'red' rated audit report, did not adequately challenge management about the ongoing negative audit findings . In NSW, councils are required to constitute an Audit, Risk & Improvement Committee (ARIC) whose chair now reports to the councillors rather than to the operational head of the organisation, an prior arrangement wholly at variance to the notion of independent assurance. Risk professionals should cultivate a strong working relationship with its organisation's oversight committee. When "bad news" cannot be elevated to the head of the organisation, they can bypass the hierarchy by using the auspices of the committee. Depending upon the composition, experience and commitment of the committee, there is a real opportunity for the risk professional to coach the committee to help it fulfil its charter to the highest of standards. An efficient secretariat (comprised of risk professionals) can assist the committee overcome such failings as identified by the RC.

There are undoubtedly other fruitful areas where risk professionals can add real value for an organisation recovering from a scandal and transforming its business model. Few can deny the magnitude of change coming to the financial services industries and other organisations but at least the dawning realisation that risk professionals are no longer an irritating expense item but have the skills and solutions necessary to help manage the change is a cause for optimism during 2019 and beyond.

1. Commonwealth of Australia. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry: Volume 1. January 2019. P. 12. https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

2. Tadros, E. 2018. "Risk management experts in high demand, especially in financial services". June 5, 2018. https://www.afr.com/business/accounting/risk-management-experts-in-high-demand-especially-in-financial-services-20180605-h10ys9

3. Letts, S. "National Australia Bank to sell MLC as another bank flees wealth management". May 3, 2018. https://www.abc.net.au/news/2018-05-03/nab-offloading-mlc-$2.5b-half-year-profit/9720782

4. Visetin, L. Blue Mountains council facing suspension over alleged asbestos breaches". December 13, 2017. https://www.smh.com.au/national/nsw/blue-mountains-council-facing-suspension-over-alleged-asbestos-breaches-20171213-h03n0d.htm5. Commonwealth of Australia. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry: Volume 1. January 2019. P. 397. https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

Three Privacy Risks to Avoid in 2019

By: Kobby Agyei Privacy Specialist **Salinger Privacy**

In this golden age of globalisation, information is key. Not only does it power the operational and strategic decision making of organisations but more importantly, when personal in nature, can be used to derive powerful insights that can steer an organisation to the cusp of innovation, brand supremacy and financial dominance. Still, with great reward comes great risk, and in a progressively scrutinised regulatory environment, privacy risk should be at the forefront of every risk manager's mind.

However, privacy is often incorrectly thought of as being synonymous with information security. While data breaches generally dominate news headlines, in fact privacy risk is significantly broader than just the loss of personal information. Implementing information security controls alone won't deal with most privacy risks.

Privacy risks fall into two broad categories: the risk of non-compliance with privacy law, and the risk of not meeting customer expectations about how their personal information will be handled. Both considerations can arise at any stage in the life-cycle of handling personal information, from the initial decisions taken about what data to collect, through to setting internal business rules about what the data can be used for or to whom it can be disclosed, all the way to the eventual de-identification or destruction of data.

With this in mind, three key privacy risks that should be avoided are outlined below.

I. Failure to implement Privacy by Design

Privacy risk should always to be considered in an organisation's initial project plan, and controls incorporated into the final design, prior to implementation. Known as 'Privacy by Design', the obligation to build privacy protections in at the design stage of projects now forms part of privacy legal obligations in many jurisdictions worldwide.

One example where privacy risk may not have been duly considered in project planning was AAMI's online platform feature for quoting. The feature made the physical security details of residential properties (such as whether there were deadlocks or alarms installed) publicly available, as online users were not required to verify their identity (i.e. whether they lived at the residence) in order to view those details. Consequently, although built as a time saving feature for customers, the grave privacy implications of disclosing that level of information was unlikely to have been considered. Following complaints from the public and privacy professionals, AAMI immediately removed the feature.

II. Failure to consider re-identification risk

De-identification of personal information when performed properly allows an organisation to draw powerful insights from datasets while simultaneously protecting the privacy of individuals. However, the process of de-identification can be complex, and simply stripping away personal identifiers from a dataset may not be sufficient; particularly if the data can be linked with other datasets or disclosure is made to a third party with the ability to re-identify that data.

This was evident in the Department of Health's (DoH) publication of Medicare Benefits Schedule and Pharmaceutical Benefits Schedule data on approximately 2.5 million Australians. Following the publication, researchers at the University of Melbourne were able to re-identify data belonging to several high-profile individuals primarily through a cross matching exercise with other publicly available datasets. The DoH was subsequently found by the Office of the Australian Information Commissioner (OAIC) to be in breach of three Australian Privacy Principles.

III. Failure to be Transparent

Privacy law not only sets rules about the collection, use and disclosure of personal information, but also creates enforceable rights of transparency, along with access and correction.

An organisation's obligation to be transparent in its handling of personal information is a fundamental requirement underpinning other privacy rights. Having a clear, concise and easy to read privacy policy, collection notice and consent capturing process are three effective controls to ensure compliance with your legal obligations, as well as meeting customer expectations.

A failure of transparency was evident in the case of HealthEngine, a health service booking platform that disclosed medical information about its users to a law firm – who then direct marketed legal services back to those individuals. While HealthEngine argued that users had 'consented' to the disclosure via its Collection Notice, that Notice seemed contradictory to its Privacy Policy. Additionally, the ability for a user to make a booking was contingent upon the user accepting HealthEngine's Terms, Privacy Policy and Collection Notice, which is contrary to the requirement that any consent be voluntary and specific. The public outcry over HealthEngine's practices, and demands for it to be investigated by the OAIC, illustrate the importance of only handling personal information in a way consistent with customer expectations, and of unambiguously communicating those plans to customers.

Conclusion

The risks discussed above are just three examples from a wide range of privacy risks which organisations face when handling personal information. In an increasingly strict regulatory environment, it is important that risk managers implement processes to identify and treat privacy risks accordingly, because the financial, legal and reputational consequences of not doing so are greater than ever. Risk managers should incorporate consideration of privacy risks – as distinct from information security risks - as a standard step within an effective risk management processes.

i Grubb B, 'AAMI Suncorp Suspend Online Insurance Quote Feature Over Burglary Fears', Sydney Morning Herald, December 2017 <https://www.smh.com.au/technology/aami-suncorp-suspend-online-insurance-quote-feature-over-burglary-fears-20171204-gzyo1c.html>

ii Salinger Privacy, Demystifying De-identification, 2018, <https://www.salingerprivacy.com.au/downloads/demystifying-deid/>

iii Office of the Australian Information Commissioner, 'Publication of MBS/PBS data - Commissioner Initiated Investigation Report', March 2018 <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data>

iv Maluga P, 'Healthengine May Be in Breach of Privacy Law In Sharing Patient Data', The Conversation, June 2018, <http://theconversation.com/healthengine-may-be-in-breach-of-privacy-law-in-sharing-patient-data-98942>

It's Time to Measure Up

By: Ian Randall Senior Consultant **Noggin**

Risk management today appears to be at a similar state of maturity as literacy was in 15th century Europe. In both cases, technology and globalisation were about to become major driving forces for change. First literacy: paper making was invented in 105 A.D. by Cai Lun, a Chinese eunuch in the Eastern Han Dynasty. The secret of making paper then took almost a millennium to reach Europe in the 11th century, traveling through Korea, Japan, India, Africa, and finally into Spain, via the Arabs. The printing press was also invented in China during the first millennium A.D., followed by movable type. However, the printing press would not make it to Europe until Johannes Gutenberg's adaptation of the technology in 1440. These technological innovations coupled with the Enlightenment coincide with the explosive growth of literacy in Europe, starting in the mid-15th century.

In the same way that technological innovation enabled a sudden growth in literacy, propelling further leaps in innovation and knowledge, technology today is driving fundamental change in Risk Management. Where once, risk management was the sole domain of experts (analogous to abbey monks' hand scribing copies of the bible in Latin), the field is rapidly democratising, becoming open to everyday people and more relevant to organisations. Despite the progress, risk management still remains a dark science to many. The changes needed to bring risk management into the mainstream are only now emerging.

Integrated Risk Management

One such change is Integrated Risk Management (IRM), so termed by Gartner. In scope, IRM covers all business units and compliance functions, extending further to key business partners, suppliers, as well as outsourced entities. IRM solutions cover a range of use cases:

1. Digital Risk Management (DRM)
2. Vendor Risk Management (VRM)
3. Business Continuity Management (BCM)
4. Audit Management (AM)
5. Corporate Compliance and Oversight (CCO)
6. Enterprise Legal Management (ELM)

Integrated Risk Management not only encompasses many traditional governance risk and compliance (GRC) business requirements, but it also incorporates incident management, risk mitigation action planning, KRI monitoring and reporting, and risk qualifications and analytics. But while IRM recognises that risk management must work together with business continuity management, incident management, and with internal and external stakeholders, it does fail to incorporate crisis and emergency management involving collaboration and coordination with external organisations and critical infrastructure supply chains (unless they impact critical IT systems). Also, except for external suppliers and direct contractors, IRM is for the most part inward looking, highly focussed on IT system risks.

Global Threats from Friends and Foes

The nature of risks themselves are changing, though, as highlighted by the Worldwide Threat Assessment put out by the US Intelligence Community recently. The Assessment states that threats to individual organisations, industries, and even entire nations are becoming increasingly global. Nations such as Russia, China, and North Korea have undertaken actions directed at influencing our election results, often fomenting racial and social strife. In turn, their actions have impacted government policies and priorities in the West. External actors from these regimes have also used aggressive, often unethical economic tactics to compete with western nations.

For instance, North Korea's cybercrime operations alone include an attempt to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank. Private companies like Sony have also been hacked by North Korean sponsored agents, who stole private customer details in retaliation against Sony's plan to release a movie deemed disrespectful to Kim Jong-un.

Globalisation of Risks

So while global trade has brought many benefits, it has also introduced new threats that must be managed: consider one of the documents disseminated by Wikileaks in 2010. Wikileaks released the details of a US diplomatic cable, "Critical Foreign Dependencies Initiative" (CDFI) which documented the location of all key assets and infrastructure that if disrupted would critically impact the US entire economy. Most of this infrastructure is neither owned or operated by the government instead by private companies, bound together by a global supply and distribution network. The CDFI cable included the details of all major foreign port hubs, the specific locations of undersea fibre-optic telecommunication cables connecting the US to the rest of the world, critical sea lanes, and oil and gas supply pipelines, as well as key mines, dams, and pharmaceutical facilities that supply the US economy from all major foreign sources. The US and UK Governments reacted strongly to the release of this information, arguing that its public release provided a "shopping-list" for terrorist organisations around the world to target key resources that could cripple the US economy.

Another potential attacker: the "frenemy" who comes in the guise of an employee, customer, or supplier. According to a PwC Global Survey published in July 2018, 60 percent of economic cyber-crime in Australia was committed by this class of attacker.

The Threat To Critical Infrastructure

As highlighted by the Wikileaks CDFI diplomatic cable release, all countries are now dependent upon complex networks of supply chains and interdependent utility infrastructures such as power, water and fuel, as well as vulnerable transport networks and telecommunication data channels. While many organisations have already identified key suppliers, customers, and distribution partners in their Business Continuity Management plans and Contractor Management systems, few organisations could survive a long-term outage to one of these key dependencies.

Take for example the remote island nation of Tonga, about 1,100 miles northeast of New Zealand. On January 20th, Tonga lost the main underwater fibre-optic cable that connects its citizens to the internet. For 11 days, the 100,000 residents of Tonga lost international and inter-island phone calls, emails, and credit card payments. The question: how would your organisation and the country deal with such an event? Another example comes way of Puerto Rico, still reeling from the Hurricanes Maria and Irma in 2017.

After Hurricane Maria, specifically, it took 11 months to restore the full electricity grid to the island. By then, it was too late for the 8,000 small businesses which closed in the aftermath of the storm, and too late for the hundreds of Puerto Ricans with treatable ailments like bedsores and kidney problems who died without power for dialysis, refrigeration for medications, and other forms of medical care. Both these examples are poignant reminders of our society's vulnerability when its critical infrastructure is disrupted beyond a few hours or days. And for this reason, governments

around the world such as Australia, New Zealand, Canada, United Kingdom, and the United States have been busy implementing Critical Infrastructure legislation and Protective Security Frameworks to address vulnerabilities. Risk management, in turn, must adapt itself to this broader national and international supply chain focus. This focus will also take risk management into the realms of crisis management, emergency management, and continuity of operation.

Technology Changes

When you talk to risk management professionals, they are called risks, when you talk to emergency service and safety people, they are called hazards, and when you talk to people in the defence and intelligence sector, they are called threats.. Regardless of what they are called, though, we are on the cusp of technology revolution that will have a profound impact on risk management.

Examples include:

Risk and Control Libraries which foster consistency and industry best practice in risk management across the entire enterprise.

Wizards that walk people through a simple and intuitive process that hides the complexities of risk management and minimises the training needed for general staff.

NewSQL databases that provide the scalability of NoSQL systems but retain the key benefits of online transaction processing (OLTP) and the familiarity of the SQL interface for technical staff.

Predictive/Prescriptive Analytics tools that identify patterns, themes and trends that might not be immediately apparent to a risk manager.

Data visualisation tools which facilitate "evidence-based decision making" and provide what-if modelling capabilities that allow staff to evaluate and predict in near-real time the potential impact of new risk management initiatives.

Data-driven risk assessment tools based in machine learning and big data analytics that help staff to identify vulnerabilities and gaps and to plan appropriate operational level controls and measures. Improvements in the simplicity and ease of use of software that runs on personal computers, on the cloud and any type of mobile device, which provides the flexibility for non-technical users to tailor the system to meet their unique requirements.

Hyper-integrated systems that tightly integrate risk management with incident management, compliance management and all the other management systems into a single platform. A platform that integrates risk management with plans that contain actions and provide us with the ability to monitor the implementation of those actions in real time.

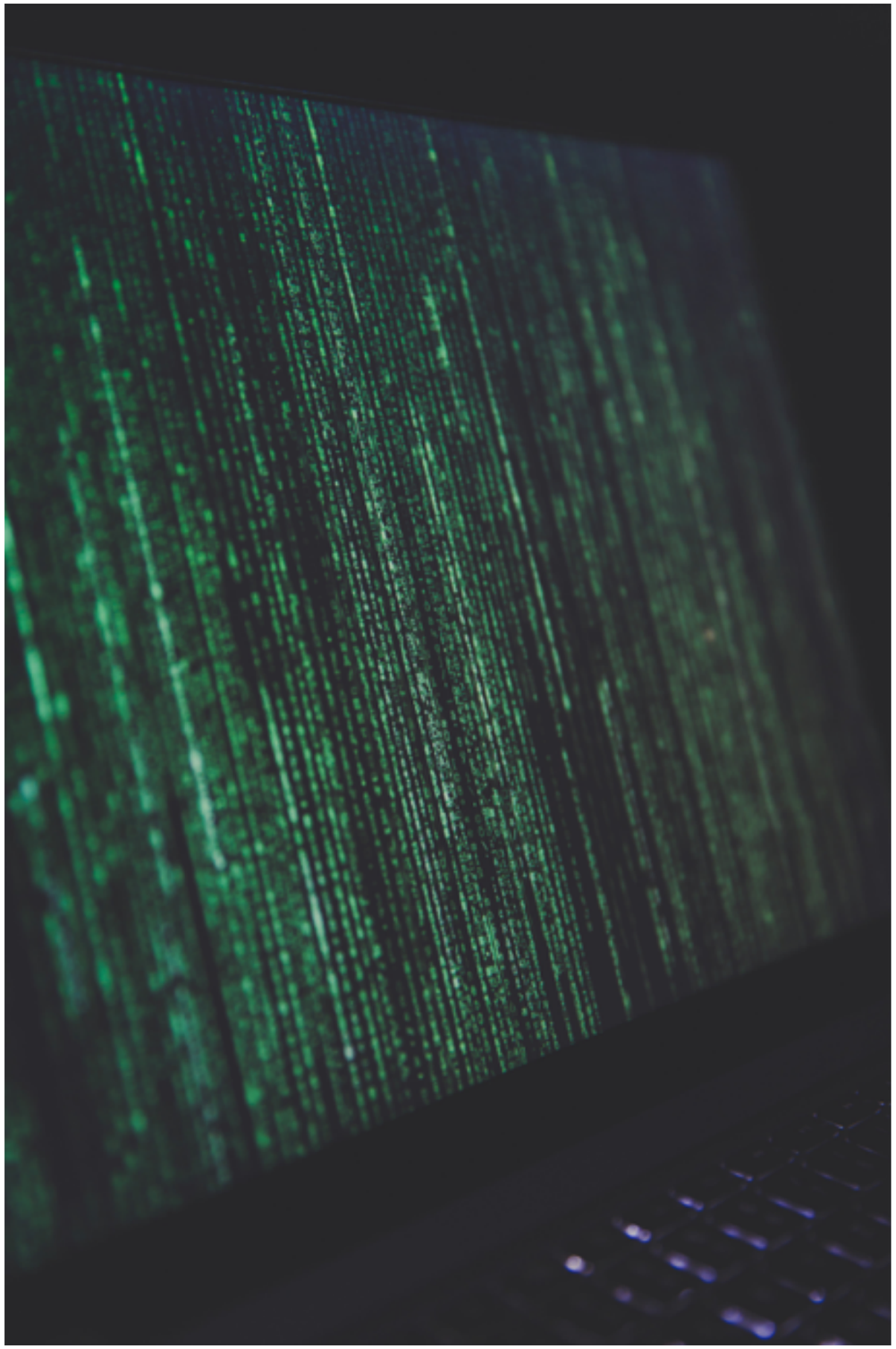
Conclusion

The scope of risk management is changing due to globalisation, which has created a complex web of interdependencies that all organisations must now master in order to be fully resilient.

What is required: organisations must become more collaborative within themselves as well as reach out to fellow businesses and public sector agencies, many of which will be half a world away.

And while technology is creating new risks, especially in the digital and cyber spheres, new innovations will also improve the ability of risk managers to deal more efficiently with risk management challenges as they emerge.

Like the monks in their 15th century monasteries, we are collectively on the cusp of a profound paradigm shift which will improve how risk management is performed. It's hard to predict how all of these changes will pan out, but to paraphrase Bette Davis, "Fasten your seatbelts, we may be in for a bumpy ride."



Photographer: Markus Spiske

Are you a Risk Leader?

By: Anthony Browne Enterprise Risk and Compliance Manager **Melbourne Water**

The concept of risk has evolved of the last 400 years and risk taking is now one of the prime catalysts that drives our modern society (Bernstein, 1996). Today societies and organisations now have a vast array of highly sophisticated methods for identifying, assessing and managing risk. Despite all the theories, tools and techniques, there are many recent examples where major risks have failed to be managed including:

• Global financial crisis in 2007 due to unforeseen financial risks from housing price collapse.
• the Deepwater Horizon oil spill in 2010 caused by unmanaged safety risks.
• the Fukushima Daiichi Nuclear Power Plant in 2011 was not adequately protected from the earthquake and tsunami risk.

Hubbard (2009) has argued these types of events are examples of The Failure of Risk Management. I contend these are not examples of the failure of risk management but failures of Risk Leadership. Just as most car accidents are due driver error most risk failures are due how leaders use risk management not the discipline of risk management itself.

While there is a wealth of information on risk management and leadership as separate disciplines, there is limited information on risk leadership.

During my 20 years in observing risk management practices across public and private companies I have found three key characteristics of risk leaders.

1)Risk leaders think differently

Risk is defined in the International risk standard (ISO 31000) as "the effect of uncertainty on objectives". Yet the four letter word RISK has different meanings to different people.

An example is the work of Thomson (1990) who classifies people perceptions of risk into five categories based on the degree of group cohesiveness and respect for formal hierarchy as follows:

• Atomised Individuals - risks are out of our control and are a matter of luck
• Hermits - risks are acceptable as long as they do not involve the coercion of others.
• Bureaucrats - risks are acceptable as long as institutions have the routines to control them.
• Egalitarians - risks should be avoided unless they are inevitable to protect the public good.
• Entrepreneurs - risks offer opportunities and should be accepted in exchange for benefits.

While five cultural categories have received some criticism (Breakwell, 2007) and I personally find that labelling groups as "Atomised" or "Hermits" to be unnecessarily derogatory, I contend that Risk Leaders need to be entrepreneurial in their understanding and approach to risk.

This idea goes as far back as 1893 in Hawley's Risk Theory of Profit in which "assuming risk gives the entrepreneur a claim to a reward".

This is supported by the concepts described in Taleb's (2012) book, Antifragile: Things that gain from disorder which identifies that positive outcomes can be gained from minimising downside uncertainty and maximising upside uncertainty.

Yet most think of risk as only downside. Risk Leaders think differently. Risk Leaders think about risks as entrepreneurial opportunities for gain.

2) Risk leaders act differently

Managing risk in an entrepreneurial way takes courage. It takes courage to act differently to other. It takes courage to take a risk. Significant psychological research over the last 50 years has shown that people are strongly influenced by others when it come to taking risk. Peer pressure has been shown to have a strong influence on risky behaviours such as smoking (Kobus, 2003), Alcohol (Borsari & Carey 2001) and juvenile crime (Bayer, Pintoff and Pozen, 2004). While these are examples of taking the wrong risks, the same can be applied to not taking risk in order conform to authority or majority.

Neuroscientist Lieberman (2013) has shown that the parts of the brain that experience physical pain are the same as the regions that experience psychological pain. This research helps to explain why disobeying or thinking differently to authority figures and majority opinion can be so difficult.

Helfinstein et al (2014) has been able to identify networks of brain regions where activity patterns are a reliable prediction of risky behaviour. The identified regions are the same parts of the brain that are responsible for control, working memory and attention. This research suggests that Risk Leaders use cognitive control processes to perform appropriate risk taking.

The word risk derives from the early Italian word risicare, which means "to dare". Risk leaders dare to be different in order act in an entrepreneurial way. It is only by harnessing the bee do we get to taste the sweetness of honey.

3) Risk leaders communicate differently

While a risk leaders think and act differently, without followers there can be no leader. Risk leaders need to master the techniques for communicating risk effectively in order to influence others. Morgan et al (2002) developed four step mental model approach to assist in developing risk communications as follows:

1. *Normative research* to identify what information is necessary;
2. Descriptive research to characterise what people currently believe, and the affect of these beliefs;
3. *Prescriptive research* to examine what people still need to learn;
4. *Evaluation research* to test whether communications are effective, in terms of actually facilitating more informed decisions.

What I particularly like about this approach is that it seeks to understand peoples existing beliefs before seeking to communicate on risk. Changing people believes can create an uncomfortable feeling of "cognitive dissonance" when evidence is inconsistent with existing beliefs. Psychologist Festinger (1956) argued that the only way to overcome this discomfort is to somehow make the belief and the evidence consistent.

Risk Leaders are masters at communicating risk in way that takes people from where they are to where the need to be.

Self reflection

Do you think about both upside and downside risks?

Do you have the courage to act different?

Have you mastered risk communication?

Then you are well on your way to being a risk leader.

Changing the Focus on Risk Culture in 2019

By: Nerida Irving-Dusting Director **Hall Advisory**

The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (hereafter Royal Commission), which ran for the better part of 2018, has resulted in a number of recommendations for change in the financial services industry. These recommendations are focused on better protection of consumer rights and meeting community expectations,and have also raised awareness of significant conduct issues that have eroded consumer trust. Following the Royal Commission findings released in February 2019, financial institutions are now faced with the task of navigating the potential myriad of regulatory and legislative changes, while attempting to demonstrate to customers that their expectations regarding culture and conduct have been heeded.

Considering this focus for 2019 and beyond, financial institutions will no doubt be considering how to navigate through the uncertainty. When it comes to risk culture, there are 3 clear areas to focus on.

1)Adopt a Risk Culture Framework

The rapid evolution of risk culture diagnostics has been propelled both by regulatory intervention and by organisations wanting to be at the forefront of change and demonstrate their commitment to putting customers first. This momentum for change has somewhat outpaced the fundamental step of defining what risk culture means to the organisation and establishing a risk culture framework to operate within.

The real challenge of assessing risk culture lies in understanding and interpreting the results sufficiently well to use them to drive change. A useful assessment must necessarily start with a framework which considers a range of inputs including:

•tone from the top (embedding the 'should we do it' question1);

•organisation-wide understanding and capability;

•communication processes; and

•incentive programs.

2) Assess Risk Culture

While regulatory requirements for assessing risk culture have been in existence for a number of years,2 ongoing uncertainty over how institutions can best demonstrate their risk culture has led to a slower progression of diagnostic techniques in some organisations. Findings from the Royal Commission encouraging the Australian Prudential Regulation Authority (APRA) to build out its supervisory program for culture and assess cultural drivers of misconduct in entities3 will ultimately encourage more supervisory oversight. As it currently stands, this finding provides no more certainty on regulatory expectations for complexity or frequency of assessments.

Many financial institutions have sought to address APRA's CPS 220 Risk Management requirements by extending pre-existing employee culture surveys to cover specific elements of risk culture and conduct. The seriousness of cultural failings within organisations has, however, demonstrated a need to increase the rigour and regularity of these assessments. To achieve this, organisations can consider:

•employing standalone risk culture surveys;

•supplementing survey approaches with the use of research-backed scales;

•conducting independent interviews; or

•supplementing assessments with artificial intelligence software to identify sub-cultures across the business, or to monitor the tone of communications.

In any case, the approach taken should be appropriate to the size and complexity of the organisation and relatable to employees. In the case of risk culture, the simultaneous use of multiple data sources can often be beneficial and reveal a more accurate picture of the culture and sub-cultures existing within an organisation.

3) Regularly Monitor

As internal culture is susceptible to change over time resulting from organisational growth and employee movements, it is critical to follow-up initial risk culture assessments with regular monitoring. Periodically monitoring changes in risk culture encourages a lasting impact and helps to translate objectives into meaningful information that can be communicated throughout the organisation. This has been reinforced in Recommendation 5.6 of the Royal Commission, which suggests that all financial institutions regularly assess culture and governance and determine whether implemented changes have been effective.4

Organisations typically already have the tools available to conduct this type of monitoring and should start by taking a closer look at existing Key Risk Indicators and Key Performance Indicators. Often existing metrics have both intentional or unintentional influences on risk culture (in a reactive sense) and can be reinvented for more proactive use to drive cultural changes. Given the difficulty of measuring culture in any strict quantitative way, chosen metrics should not be looked at strictly in isolation; correlations should also be considered. Ideally organisation will also institute some form of quarterly or regular dashboard reporting of risk culture indicators for oversight by Management and Board, and we can expect to see varying approaches to this adopted across different organisations.

Although the specifics of looming regulatory change may currently be uncertain, it is guaranteed to propel the progress of risk culture management for the foreseeable future as financial institutions strive to demonstrate that lessons have been learnt. Financial institutions that are not actively or publicly acknowledging the issues of misconduct and seeking to demonstrate improvements in culture may get left behind as the industry repositions to rebuild consumer trust.

1 Prudential Inquiry into the Commonwealth Bank of Australia (CBA) Final Report, April 2018, page 55, Recommendation 21 https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf
2 Prudential Standard CPS 220 Risk Management, April 2018, paragraph 9(b) https://www.legislation.gov.au/Details/F2017L00973
3 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 1, February 2019, page 37, Recommendation 5.7 – Supervision of culture and governance https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf
4 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 1, February 2019, page 36, Recommendation 5.6 – Changing culture and governance https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf

Why do Accountants and other Professionals need Better Risk Management Competencies?

By: Alex Sidorenko Director **International Risk Services**

Risk management competencies can significantly improve decision making in any profession. The bad news is that these competencies don't come to us naturally. They have to be developed.

Even if you don't operate in a high risk, uncertain environment I recommend at least considering more than 60 years of research into what scientists call heuristics and biases, cognitive psychology and psychometric paradigm, collectively called risk perception.

The History of Risk Perception

The study of risk perception arose out of the observation that experts and lay people often disagreed about how risky various technologies and natural hazards were.

The mid 1960s saw the rapid rise of nuclear technologies and the promise for clean and safe energy. However, public perception shifted against this new technology. Fears of both longitudinal dangers to the environment and immediate disasters creating radioactive wastelands turned the public against this new technology. The scientific and governmental communities asked why public perception was against the use of nuclear energy when all the scientific experts were declaring how safe it really was. The problem, from the perspectives of the experts, was a difference between scientific facts and an exaggerated public perception of the dangers.

Research began to try to understand how people process information and make decisions under uncertainty. Early works found that people use cognitive heuristics in sorting and simplifying information which lead to biases in comprehension. Later work built on this foundation and identified numerous factors responsible for influencing individual perceptions of risk, including dread, newness, stigma, and other factors.

Research also showed that risk perceptions are influenced by the emotional state of the perceiver. According to valence theory, positive emotions lead to optimistic risk perceptions whereas negative emotions influence a more pessimistic view of risk.

The earliest psychometric research was done by psychologists Daniel Kahneman (who later went on to win a Nobel prize in economics with Vernon Smith "for having integrated insights from psychological research into economic science, especially concerning human judgment and decision-making under uncertainty") and Amos Tversky, who performed a series of gambling experiments to see how people evaluated probabilities. Their major finding was that people use a number of heuristics to evaluate information. **These heuristics are usually useful shortcuts for thinking, but they may lead to inaccurate judgments in complex business situations of high uncertainty – in which case they become cognitive biases.**

Cognitive Biases are just the Beginning

Beside the cognitive biases inherent in how people think and behave under uncertainty, there are more pragmatic factors that influence how we make decisions, including poor motivation and remuneration structures, conflict of interest, ethics, corruption, poor compliance regimes, lack of internal controls and so on. All of this makes any type of significant decision-making based on purely expert opinions and perceptions highly subjective and unreliable.

Risk management can provide clarity and assurance to decision makers anywhere within the organization, not just the risk management team .

Risk management provides a set of tools to help management see risks, understand their significance to each decision and determine the best course of action with these risks in mind. Now risk management may seem simple enough in theory, yet many employees outside of the risk team still don't have the necessary skills and competencies to apply it successfully in practice.

Here are some practical ideas to bring risk management competencies to life, regardless of where you are in the organization (based on the free risk management book "Guide to effective risk management):

A. Risk management competences should become an important attribute when hiring new personnel

HR teams should include risk management requirements in all relevant position descriptions when hiring new personnel for the organization. The level of detail will of course depend on the risks associated with each role. Any finance, accounting or investment individual should possess a basic understanding of risk.

B. Risk-based decision-making in induction training for new employees

New hires come from a variety of educational and experience backgrounds and most importantly, each new employee has their own perception of what is an acceptable risk. It is important for risk managers to cooperate with the HR team or any other business unit responsible for training, to jointly carry out training on the basics of risk-based decision-making for all new employees.

C. Risk awareness sessions for senior management and the Board

Executives and Board members play a vital role in driving the risk management agenda. Nowadays many executives and Board members have a basic understanding of risk management. Auditors, risk management professional associations and regulators have been quite influential in shaping the Board's perception of risk management. It is important to make risk management training less about risk assessments and more about risk-based decisions making, planning, budgeting and investment management. The paradox is that risk management training shouldn't teach management how to manage risks, instead it should show them how to do their jobs with risks in mind.

D. Advanced training for "risk-champions"

Additional risk management training may need to be provided for the risk management team and business units responsible for internal control, audit, finance, strategy and others. In-depth risk management training should include: risk psychology and risk perception basics, integrating risk management into culture, basic knowledge of ISO 31000, risk management and decision making foundations, integration of risk management into core business processes and decisions.

E. Use passive learning techniques

Make risk management information available to employees, contractors and visitors. Place the Risk Management Policy on the intranet and the corporate website. Record and publish risk management training or awareness sessions videos on the dedicated risk management intranet page. Invite guest speakers (risk managers from other companies) to speak at the Audit Committee or Risk Management Committee and give all employees the opportunity to participate. I have used this in the past and it worked very well.

F. Make risk management part of everyone's responsibilities

It helps to include risk management roles and responsibilities into existing job descriptions, policies, procedures and Committee charters. The common approach of capturing risk management information in a single risk management framework document doesn't work well.

G. Integrate risk management into day-to-day work

My experience shows that updating existing policies and procedures to include aspects of risk management works much better than creating separate risk procedures or methodology documents.

Risk management is a valuable tool to help employees make business decisions under uncertainty. It works equally well with strategic, investment, financial, project or operational decisions. However consistent application of risk management requires good knowledge of risk management standards, risk phycology and quantitative analysis. Should you wish to discuss risk management matters further, feel free to reach out me via Linkedin.

Alex Sidorenko is an expert with over 13 years of strategic, innovation, risk and performance management experience across Australia, Russia, Poland and Kazakhstan. In 2014 Alex was named the Risk Manager of the Year by the Russian Risk Management Association. Alex works as a Director at the International Risk Services, a Valletta based risk management consulting and training company. Alex worked as a Head of Risk Management at RUSNANO, one of the largest private equity funds in Russia, specializing in technology investment. Alex won an award for best ERM implementation at RUSNANO in 2014. Alex recently published his second risk management book called "Guide to effective risk management 3.0" which is available for free at www.risk-academy.ru/en

Photography: Federation of American Scientists

Examining the Link between Enterprise Risk Management and Organizational Financial Performance in Australia

By: Dr. Jolene Morse Head of Risk Models and Support **Bendigo & Adelaide Bank**

Background
Every organisation whether they are profit, non-profit, or government provides value for its stakeholders and given the rapid pace of change in the global business environment, organisations need to leverage every opportunity available to them whilst navigating an increasingly complex risk landscape. To assist in managing this complexity, Enterprise Risk Management (ERM) is becoming increasingly important. ERM is a rigorous and coordinated approach to managing the risks of an organisation from a strategic perspective. The conceptual benefits of ERM include better strategic and operational decision making, reducing the organisations risk premium and a reduction in earnings volatility. However, despite the increased focus on the relationship between ERM and organisational financial performance, research in this area has produced inconsistent findings.

Research
To date research examining the relationship between ERM and organisational financial performance has reported mixed outcomes and has been limited to primarily the US and UK. However, a recent study focused on Australian businesses and identified and tested the link between ERM and organisational performance. An explanatory sequential mixed methods design was utilised for this research, in which both quantitative and qualitative methods were used to collect data from Australian organisations using an online survey, followed by face to face interviews. The organisations that participated in the research represented 23 industries, including government agencies and not-for-profit organisations, and the majority of participants primarily operated exclusively within Australia, however there were a small proportion of respondents that also had operations in other regions such as New Zealand and Asia.

What does this research mean for risk in 2019?
1.When establishing an ERM program, it is important to consider the effect of organisation specific characteristics on the relationship between ERM and financial performance. These may differ by organisation type, nature and size amongst other factors, however this study has shown there are important implications of doing this step up-front to determine where the organisation's key risks lie and what supporting infrastructure may be required to best implement the ERM framework. Furthermore, it was found that larger organisations are more likely to have an ERM framework in place, confirming the importance of having sufficient resources available to support the program.

2.The research findings indicated that ERM may be implemented in Australia for the purposes of compliance, rather than to gain the organisational financial performance advantage. This suggests that there is an opportunity for organisations in Australia to gain much more from their ERM programs, more developed risk reporting, a greater focus on risk assessment and a more effective connection of resources to risk-based decisions.

3.The findings suggested that the survey respondents may have believed that they were deriving more value from their ERM program than was the case as they identified risk assessment activities, but not incorporating risk management in the organisation's strategic decision making. This suggests that there is an opportunity for Australian organisations to better link their risk management and the strategic planning process. It is more likely that the organisation will achieve its strategic objectives when they are strongly integrated with the ERM process. This will require the development of a complete ERM implementation, senior management support and communication and education throughout the organisation.

4.The level of ERM implementation in Australia was found to be highly variable, but generally lower than other developed countries. The low level of maturity of ERM in Australia provides many opportunities for practitioners to become early adopters of enhanced ERM programs in the Australian context. Australian organisations should utilise ERM as a coherent conceptual framework for managing risks holistically and allocate sufficient resources to its implementation to ensure that it is consistently applied across the organisation. It is also important to ensure that sufficient measures are incorporated to allow the organisation to monitor and assess the benefit that it is gaining from its ERM process. In particular, Australian organisations should not consider ERM as a compliance framework and instead consider it to be a strategic framework that will enable the organisation to treat risk as an opportunity rather than a threat and increase performance levels.

Conclusion
This research has determined that ERM can play an important role in protecting the organisation's value. The discovery that there is a relationship between ERM implementation and the organisation's ability to manage risks so as to avoid any negative effect on the organisation's value has significant implications for practice. The implication from the finding that larger organisations are more likely to have an ERM framework in place has important ramifications for ERM practitioners in small organisations, where access to resources may be limited. Cooperative practices with industry bodies or small business consortiums may be a valuable way for sharing information and resources to maximise the success of ERM implementation and its subsequent contribution to organisational financial performance. Possibly the most important finding for practice was the relationship between the success of ERM implementation and the organisational culture. This finding has far-reaching consequences for the practice of ERM implementation.

The dimensions of culture which may affect ERM implementation include senior management engagement, communication, tolerance, level of insight, level of care, speed of response, confidence, openness, challenge and cooperation. In addition, the organisation's culture should be considered in relation to the initial plan to ensure that any potential issues can be appropriately addressed and not be embedded into the program as it is implemented. A culture suitable for the successful adoption of ERM is open, transparent and productive. It must be supported by senior management, both in concept and by demonstration. The board should set expectations for how conversations about risk should occur and this should include the creation of a risk appetite statement for the organisation. Therefore, whilst the level of ERM implementation amongst the organisations represented by the survey respondents was reasonably high on several measures, the utilisation of risk management to proactively improve financial organisational performance amongst these organisations was low. Hence, this research shows that risk in 2019 provides many opportunities for Australian organisations to improve not only their risk management but also their financial performance.

Individual and Corporate Risks are Not the Same

By: Alex Sidorenko Director **International Risk Servcies**

In the first of a four-part series, Alex Sidorenko, founder and CEO of Risk-Academy, explains how the key to managing corporate
management is not about managing risks. It's about helping management make strategic, operational and investment decisions while keeping the risks in mind.

It sounds simple enough, but it's anything but. Over four columns, I will share four valuable lessons about integrating risk management principles and methodologies into day-to-day decision-making.

There is a big difference between the risks that the board is concerned about, such as corporate risks, and the risks that individual managers worry about, often their personal risks. It is quite natural for humans to consider risks that can potentially impact them personally as significant, while the risks that impact the achievement of strategic objectives as somewhat remote or distant.

The important lesson I learned is that if you want management to pay serious attention to corporate risks, you should first help them deal with their individual or personal risks. And by personal risks I mean things like maintaining their area of influence, building a solid reputation, advancing their career, not losing their job and protecting themselves from investigations or prosecution.

Another aspect that has a huge impact on the quality of decision-making – and hence the quality of risk management – is remuneration policy. Many people are driven by their financial self-interest much more than any corporate values or best practices. And this has a huge implication on the work of risk managers. To address these challenges, I aim to do the following:

•Demonstrate how proactive risk management can benefit individuals within the firm and solve their personal risks. Even basic things like creating a paper trail for key decisions and risks taken by management to protect against any future enquiries;

•Review existing remuneration policies and find out how the bonus payments are calculated to understand whether it drives any excessively risky behaviour and what periods are particularly vulnerable. For example, employees usually make much riskier decisions just before bonus entitlements are calculated;

•Work with HR to ensure existing individual objectives and KPIs adequately take risks into account. This will help to cement the message that risk management is a part of normal performance management;

•Work with strategy to ensure corporate objectives and KPIs are also set based on the outcomes of risk analysis to help make the targets more realistic and achievable;

•Include risk management roles and responsibilities into existing job descriptions, policies, procedures and committee charters to reinforce ownership and accountability.

As risk managers, we need to be prepared to the fact that some managers ignore risks and take uncalculated risks for a reason. Therefore, it's absolutely critical to understand what motivates each individual.

In my next column, I will share some practical suggestions on how to overcome cognitive biases when managing risks.

Opportunity Management: The New Way to Manage Risk

By: Ben Kelly Chief Risk Officer **Australian Taxation Office**

'With great risk comes great reward' (Thomas Jefferson) a quote we hear so often, but when we conduct our risk management processes, I often feel we forget the word 'reward' and just focus on whether the 'risk' is too big to take. What if we started asking whether the reward is too big to miss?

In my experience, this has particularly been the case in the public sector. One of the recent fundamental changes to the ATO is how we have moved to a simpler, more meaningful, positive, and objective focused view of risk – where looking for opportunity is just as important as managing the potentially negative effects of risk.

At a time where the public service is trying to do more with less, harnessing opportunities is essential. Maintaining leaves us behind; and keeping up is often not enough. We must look for the rewards, the opportunities, the innovation, and those moments where we can not only meet best practice, but create better practice.

This is where the ATO is moving our position as an organisation to focus as much on 'opportunity management' as we do on traditional 'risk management'.

So, where are we on our journey?

Over the past 18 months we have released a refreshed Enterprise Risk Management Framework (ERMF), appointed a Chief Risk Officer, established an Enterprise Risk Management Committee, embedded our new risk management processes, introduced a new enterprise risk register, and embraced the use of our new risk methodology. We've embedded the refreshed ERMF through aligning four critical components:

•culture
•governance
•informed decisions, and
•data and technology.

These components and our processes under the ERMF are designed to:

•support strong risk discussions at all levels
•improve decision making
•harness opportunities
•support a positive risk culture
•simplify risk management and cut red tape, and
•better integrate risk into strategic planning and everyday conversations.

The use of our new risk methodology has been critical in driving our shift to opportunity management. We ask ourselves four simple questions to focus our efforts:

1.What are our objectives?
2.What must go right? (what strategies are being used to meet our objectives?)
3.What may go wrong? (what are our uncertainties in achieving our objective?)
4.Are the strategies working and risks being managed effectively? (assurance)

This approach is starting to become a key element of our planning activities and risk assessments. We now consider what opportunities we can harness as part of actively avoiding the negative impacts of risk.

Is 'opportunity management' irresponsible?

This is a great question. 'Opportunity management' is not about blindly chasing a dream. Opportunity management, like risk management, still involves well considered activities to achieve a goal. As an organisation, we actively **identify,** positively **engage** with, and **manage** risk to make the most of opportunities, deal with threats, foster innovation, and to build a strong risk culture. The ATO is always and rightly subject to scrutiny: from our community, the media, and other government authorities. Our enterprise risk management framework is an essential part of a governance foundation to satisfy the expectations of these stakeholders.

What's an example of 'opportunity management'?

When most people think of the ATO, they think about our compliance activities. Audit is one of our controls to support people to pay the right amount of tax. By using our risk methodology, we look at the methods we use that help support people to meet their obligations. Audit is only one tool in our risk management 'toolbox'. Applying our opportunity approach, we explore different options and look for innovative ways to foster willing compliance, such as:

•Improving how and when people can access our channels to find information, lodge and report their income – and get their refunds and pay their tax
•Scoping how tax can be paid at the time income is received, and not just by the due date of a payment on a calendar.

There is a risk for us in not investing in the opportunity. And have you ever heard of someone being 'opportunity adverse'?
What is a positive risk culture?

When you hear 'risk management', you may think of lots of paperwork in the hands of risk managers who are more likely to press the 'stop' button than embrace opportunities.

Positive risk management and positive risk culture is about making sure anything that may get in the way of achieving your objectives is actively identified and managed.

We encourage our people to be innovative and responsive, to look for how we can positively manage risk and put the experience of our clients at the front of everything we do. You can see a positive risk culture in any organisation by how staff talk about risk.

If staff are innovative, learn from mistakes, look for ways to improve and develop, and are focused on opportunities – as opposed to fear of failure and worry about delivering bad news - these are all indications of a positive risk management culture. It is this culture that will enable us to influence and support willing compliance with the tax and super systems, and as an organisation to continually evolve to meet the challenges of the 21st century.

So next time you have a risk management discussion, I challenge you to ask if you have seized the chance to manage your opportunities. about making sure anything that may get in the way of achieving your objectives is actively identified and managed.

We encourage our people to be innovative and responsive, to look for how we can positively manage risk and put the experience of our clients at the front of everything we do. You can see a positive risk culture in any organisation by how staff talk about risk. If staff are innovative, learn from mistakes, look for ways to improve and develop, and are focused on opportunities – as opposed to fear of failure and worry about delivering bad news - these are all indications of a positive risk management culture.

It is this culture that will enable us to influence and support willing compliance with the tax and super systems, and as an organisation to continually evolve to meet the challenges of the 21st century. So next time you have a risk management discussion, I challenge you to ask if you have seized the chance to manage your opportunities.

Risk Culture, Risk Management and the Banking Royal Commision

By: David Abell & Helen Bird Course Director & Master of Corporate Governance **Swinburn Law School**

There is a strong sense of 'déjà vu' in Commissioner Hayne's observations about culture, risk and governance in the recently published Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry ('Banking Royal Commission'). On 27 February, 2013, Dr. John Laker, then Chairman of APRA, remarked:

'A board of a financial institution has the ultimate responsibility of setting the institution's overall strategy, determining it risk appetite and overseeing the management and control of risk within the appetite, and ensuring there is a robust decision-making process with appropriate executive talent in place. When a board does not exercise that responsibility astutely, the consequences for the institution can be severe – poor strategic decisions, excessive risk-taking, substantial losses and financial failure.'

Just 6 years later, this premonition can to pass in the form of findings of serious conduct and conduct falling below community standards of behavior by the Banking Royal Commission. Commissioner Hayne likewise observed:

'….. There can be no doubt that the primary responsibility for misconduct in the financial services industry lies with the entities concerned and those who managed and controlled those entities: their boards and senior management…….

Dr. Laker identified five key failings of financial institutions coming out of the Global Economic Crisis of 2007/2008: a lack of professionalism on boards; poor risk governance; poor flow of information to the board; poorly understood values and non-existent risk culture; and poorly designed executive remuneration arrangements. Commissioner Hayne was uncannily similar:

'The evidence before the Commission showed that too often, boards did not get the right information about emerging non-financial risks; did not do enough to seek further or better information where what they had was clearly deficient; and did not do enough with the information they had to oversee and challenge management's approach to these risks. …. financial service entities put the pursuit of profit above all else and, in particular, above the interests of their customers and above compliance with the law. When financial services entities did have regard to risks, they gave priority to financial risks, leaving their frameworks for the management of non-financial risks underdeveloped.

Two simple but critical questions

In his 2013 address, Dr Laker considered the rhetorical question of what might have been different if the institutions caught up in the GFC had properly addressed their governance and risks issues. He noted that 'One can only imagine how different the destiny of some institutions might have been' if their corporate statement of values required that financial products promoted and sold by the institution had to pass two simple tests:

•They had to meet/satisfy genuine customer need; and

•Customers would have bought the products if they had the same product knowledge as the financial institution?'

Implicit in these questions are a number of assumptions as to the culture and ethics of the institutions selling the products. First, a shared belief that the customer's needs were front and center of the institution's business. Secondly, that the institution would properly inform the customer and not attempt to sell products that advanced the interests of the institution at the expense of customers.

Prescriptive Prudential Standards

Dr Laker's speech was a curtain raiser to a period of significant policy development at APRA, with prudential standards CPS 220 (Risk Management) and CPS 510 (Corporate Governance) introduced into law in response to the Global Financial Crisis. CPS 220 first became binding for APRA regulated institutions on 1 January, 2015 and CPS 510, on 1 July 2012. Both standards have since been updated on several occasions. Both are also highly prescriptive in their requirements, requiring institutions to comply with those requirements in their entirety. For example, CPS 220 requires boards of regulated institutions to take responsibility for the institutions' risk management framework, oversight of its operations including its risk management strategy, risk culture, management information systems, business plan for managing risk and performance of supporting compliance functions. These responsibilities culminate in the requirement that the Board Chair and Chair of the Board Risk Committee must make an annual declaration about the institution's risk management to APRA.

The risks managed by boards are those regarded as 'material' in nature, namely those that could have a material impact on the institution or the interests of depositors and/or policyholders.

Specific categories include operational risk (Cl 26 (d)) and other risks (Cl 26 (e)) that, singularly or in combination with different risks, may have a material impact on the institution.

The annual declaration made by the board chair and chair of risk must state that the organisation has systems and resources in place for identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating material risks and that the risk management framework is appropriate to the institution, having regard to the size, business mix and complexity of the institution. Prudential Practice Guide CPG 220 supplements CPS 220 advocates that APRA-regulated institutions should use a '3 Lines of Defence' model for promulgating their risk management.

Climate Related Risk Disclosure - Asleep at the Wheel?

By: Tony Pooley & Rob Hogarth

Misalignment of new guidance on climate-related risk with risk standards demands swift responses from the risk profession.

Risk profession caught napping

We have been tardy in responding to emerging "climate-related risk" disclosure expectations of listed companies. Current practices by most entities differ substantially from that being demanded by the agencies creating and endorsing a new generation of climate-related pseudo-regulation on disclosure!

Pressure is mounting beyond the ASX 200 to increase the disclosure of climate-related risk for the upcoming reporting season. Unfortunately, the term as used by proponents of increased disclosure does not align with risk standards. This is hardly surprising, given the void of the risk profession's involvement in the new wave of well-intentioned guidance. CROs and Risk managers who are not yet alert to these developments need to get ready now!

Guidance with a sting in the tail

Climate change disclosure recommendations from institutional investor ESG groups, not-for-profit sustainability report standard setters and the ASX Corporate Governance Principles and Recommendations (ASX CGC Principles) are well established. They are also widely adopted amongst listed and unlisted companies and public sector agencies. *Figure 1: The climate change race*

Recently the bar has been lifted with ASIC highlighting the Corporations Act requirement for listed companies to disclose material business risks in the Operating and Financial Review (OFR) of the Directors' Report. Further, it indicated that, in its opinion, climate change is a foreseeable risk facing many listed companies and that it may be material. The Australian Accounting Standards Board (AASB) and Auditing and Assurance Standards Board (AUASB) in December 2018 released a joint bulletin setting out recommendations in relation to treatment and disclosure of climate-related risks in financial statements and related reports.

These recent developments, confirming the extension of climate risk disclosures from sustainability reports into financial statements and Directors' Reports, reference recommendations from the Task-force on Climate--related Financial risk Disclosure (TCFD). The Basel-based G20 Financial Stability Board established the TCFD in 2016 as an industry-led task force, and their 2017 report is increasingly referenced as the guide for climate risk disclosures. Unfortunately, the underlying risk concepts in the TCFD recommendations are not well aligned with risk standards creating a sting in the tail for risk managers tasked with preparing climate risk disclosures.

Guidance misalignment

The TCFD recommendations set out four core elements of recommended climate-related financial disclosure (governance, strategy, risk management and metrics & targets). Risk management disclosures recommendations relate to climate-related risk management processes, whilst metric and target recommendations include the measurement and oversight of climate-related risks and opportunities. There are three key areas of misalignment between the recent guidance use of TCFD recommendations and ISO 31000:2018, Risk management:

Figure 2: Misalignment between TCFD and ISO 31000 (see right)

These differences are not just terminology—they reveal fundamental misalignment in the conceptual bases. Recent guidance using TCFD focuses on all potential impacts within, and outside of, an organisation's objectives, with negatives regarded as risks and positives as opportunities, and applies a financial statement type basis to materiality. Further it contemplates that aspects such as physical, regulatory and cost outcomes will be separate risks owned, at least in part, by non-operational managers. ISO 31000 focuses on impacts on the objectives of the entity, both negative and positive on an after-treatment basis, with significance determined by likelihood and consequence. Further, it contemplates that aspects such as physical, regulatory and cost outcomes will be managed by operational managers because they will become causes (threats or opportunities) of a range of operational and strategic risks.

In the ISO 31000 context, if climate change impacts are already included in budgets or plans and treatments in place then the risk relates to the uncertainty around the estimation and hence may not even get on the radar of a board. In the TCFD context, if the potential impacts of climate change across a range of operational areas could be material (however defined), then disclosure is needed even if they are not significant or if actions have been taken to manage these impacts.

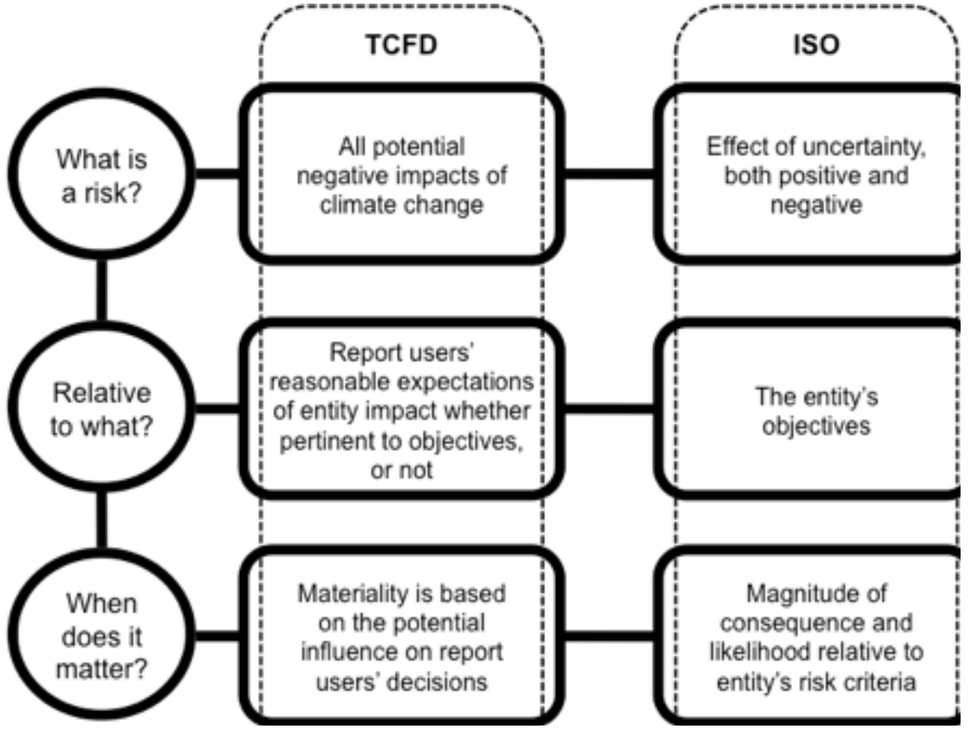
Extent of the extension

Extending risk concepts to all potential impacts beyond entity objectives and relating materiality to reports users' decisions is a major disparity from ISO 31000. The key question is how far does this extension go both in terms of climate-related risk and any other risks? The AASB and AUASB joint bulletin indicates that climate-related risk is in the mix because investors have said it should be, but cyber risk is not because that has not been put forward. Similar questions need to be resolved about the boundaries of disclosure of potential impacts of climate-related risks beyond the entity to the sector, country and the planet.

Finding a solution

Many of the top ASX companies have already made a start on climate-related risk, so if the risk profession is to be influential it will need to move swiftly. Time is short with the referencing of the TCFD recommendations in the recently released 4th edition of the ASX CGC Principles. These Principles make no reference to ISO 31000, so the ASX CGC will not have considered impending clashes. The company approach to date has been to follow the TCFD terminology to the degree possible, whilst referencing potential impacts to operating issues such as credit risk or physical asset deterioration.

Disclosures around processes to identify, assess and manage climate-related risk need to be tied back to the ISO 31000 concepts adopted by most Australian reporting entities but caution is needed not to mix apples and oranges. Most importantly, the TCFD disclosures go well beyond information otherwise available to risk managers. A team approach is needed involving wide-ranging input across most entities—preparation time will be substantial. Metric and target disclosures from the TCFD recommendations are likely to involve board interaction which should also be factored into timelines. Paradoxically, these developments are an opportunity for top risk professionals to show genuine C-Team membership credentials, because TCFD has strategic impact on every listed company and many other entities. The RMIA should urgently consider establishing their own climate-related disclosure task force, to represent the risk manager's perspective and help bring about a seamless interface between TCDF and ISO 31000 intentions.



Avoiding the Culture Clash

By: Jerry Grayson

Bio
Jerry Grayson began flying helicopters in the Royal Navy; eight years that culminated in being the most decorated pilot in peacetime. Since then Jerry has been capturing images from the air across all seven continents for movies (James Bond was his first!), sports (Olympics, Soccer World Cup …), and documentaries (An Inconvenient Truth, Planet Earth …) But in 2013 the drones arrived with a vengeance; perhaps the biggest advance in aviation since the Wright Brothers. In a clash of two cultures the proponents of manned and unmanned aviation are on a (quite literal) collision course.

Avoiding the Culture Clash

In past years my corporate and keynote speaking engagements, including one at the RMIA annual conference in 2017, have very much focussed on the classic need to address subjects such as leadership, decision making in a crisis, disaster management, resilience and teamwork. It's always a joy to recount stories from extreme flying and rescue scenarios which shine a spotlight on those various needs in the corporate environment. Even more recently the subject of disruption has become more widely requested and I've used the example of how my own career in helicopters ended abruptly with the advent of ubiquitous drones.

Drones have opened up a whole new career canvas for me, but in the last few months they have also shown their dark side with hundreds of holiday flights cancelled at Gatwick over 36 hours, followed almost immediately by a similar, albeit shorter, incident at Heathrow.

So I now find myself called upon to speak publicly about the Culture Clash that's growing between manned and unmanned aviators. More particularly my focus is on how to put a halt to that process and hopefully reverse it. Here are the main points of the conflict …

• There are two users of a single resource (the air). One group has been around for just over 100 years, wear rings on their arms to signify command and are somewhat elite as a result of training and cost. The other is a start-up (upstart?) of lesser beings but is growing exponentially. The two groups are forced to share the same airspace and it's not working out very well so far.

•Overseers, known locally in Australia as Civil Aviation Safety Authority, are trying to find the right balance between integration or separation. There is no ideal answer.

•Manned aviators believe they have grandfather rights and priority access to the air; with a certain amount of justification due to the humans aboard their flying machines.

•Unmanned aviators believe they are the party of the future, again with certain justification due to financial savings and advancing technology. Is any of that beginning to resonate with you in your own context?

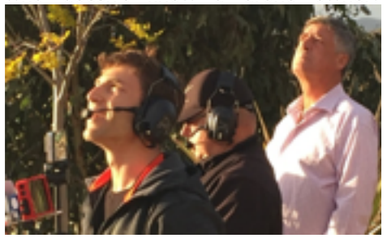
Aviation, more than any other industry, is populated by workers who are supremely alert to risk – all day, every day. It's not by accident that everybody from the captain of a plane carrying 600 passengers to the driver of the push-back tractor is constantly alert to the usual risks, the less likely risks, and the downright improbable risks. Even the team unloading your latest designer suitcase from the hold know that if they slightly bend a cargo door there are potentially several hundred lives at risk if they don't tell somebody right away.

Aviation accidents and even small incidents are put under a stringent microscope in an effort to never see the same occurrence again. It might surprise you to know that as a pilot myself I don't lay awake at night worrying about crashing and burning. What I DO process in the small hours is whether I've got away with something by the skin of my teeth and not declared it. If a fellow aviator subsequently experiences the same problem and is not so lucky then I may have many lives on my conscience

Honesty, use of checklists, mutual regard for everyone in the chain and a healthy dollop of respect for the unforgiving environment in which we work, all culminates in what we know as aviation CULTURE. Culture is a hard thing to teach, but an easy thing to accord with, and fit in with, when everybody around you has embraced it and is putting it into daily practice. On the other hand, it can't be created out of thin air, it's a long and challenging process that requires focus, leadership and full participation by all. Oh, and by the way, it comes from the top.

So allow me to now return to the subject that's top of my personal Risk Management in 2019 agenda; drones. They have been called the product that made it the fastest from the CIA to Walmart but there is more to it than the superficial joke contained in that statement. With just a couple of short stories I can make your hair curl with what it's now possible to do with drones. The subject is no longer about individual drone capabilities (which are astounding enough as it is), the real story for 2019 lies in autonomous collaboration between drones that already feature embedded forms of early AI. This is called "swarming". Commercially available off-the-shelf drones can already fly many hundreds of kms, carry out their task at the destination, or en-route, and return to base without any human interference. Now imagine them doing this as a swarm. It's not science fiction it's here and now… and it's risky when mixed with manned flying machines.

Meanwhile the aviation authorities worldwide, of which the Australian CASA is justifiably held up as being an example of "best practice", are struggling to keep up with the pace of advance. This is not through fault, they are simply overwhelmed by the technological advances and the sheer weight in numbers. Hands up anybody who doesn't know a drone owner?



Suddenly the industry that has so long prided itself on being one of the best examples of collaborative risk management has a problem on its hands that's growing daily and exponentially. Scientists and engineers are frantically throwing drones into jet engines and onto cockpit windows in an attempt to quantify the actual risk from wind tunnel experiments. Whatever their findings there is no getting past the fear of manned aviators that it's only a matter of time before they are brought out of the sky by one of these satanic things. If an airborne pilot can see a drone then, by definition, it has passed too close.

Similarly, risk managers such as the Senior Air Traffic Control Officer at Gatwick can hardly be blamed for dealing with the risk by completely closing their airports. Would you like to be facing the subsequent board of enquiry explaining how you took a balanced view which unfortunately ended up with the loss of a full airliner?

The main problem is one of silos. How often have we heard that one before, except that this time the stakes are not corporate efficiency, they are life and death. Manned aviation has had many hazards to avoid over its hundred-year life; birds, toy balloons, other aviators, masts and buildings that go up into clouds, lightning that comes down from clouds, icing on the wings, bits that fall off, burn, or just fail. So, from within the manned aviation silo a drone is just another hazard which has to be avoided at all costs, preferably at a very wide margin.

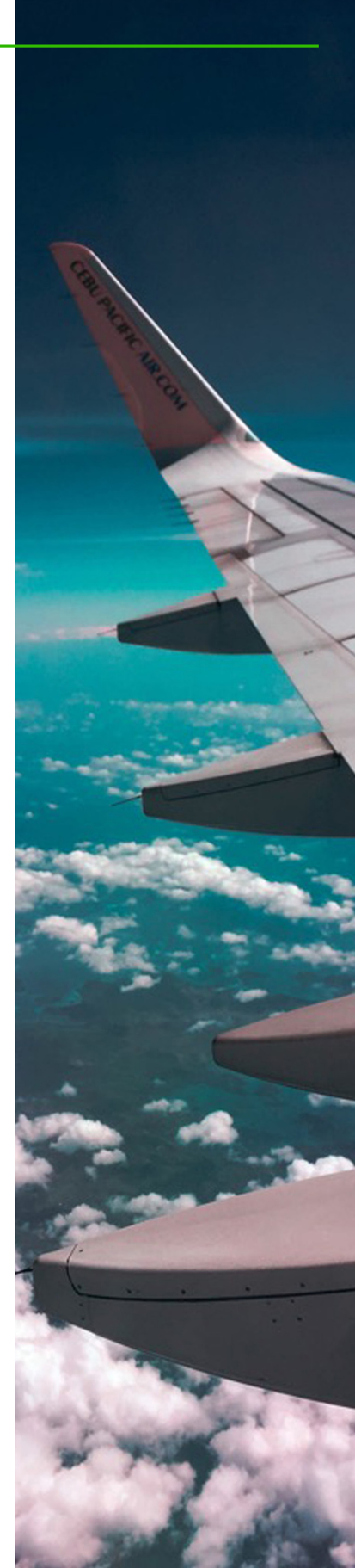
Communication is inextricably linked with education. In my own world of aviation, I'm exhorting all parties, in both silos, to communicate. This doesn't mean shouting at each other across social media and/or complaining about each other to the regulators, it means actually talking and learning something from each other. This has to take place in an atmosphere of mutual respect and a genuine desire to participate for the sake of a risk management system that works for everyone.

Over in the other silo of unmanned aviation the two bastions of communication and education are even more paramount, in fact both need actively enforcing. The manned aviator has to pass a multitude of exams before he can take charge of a flying machine, why should it be any different for the pilot of a drone if they are to share the same airspace? I fully accept that the rider of a motorcycle shouldn't have to take the same tests as a bus driver, but they do both take tests and their respective tests already take into account the need to understand the constraints and perspective of the other.

Finally we return to the word culture. If we are to share the same airspace then we need to be a part of the same culture, and we cannot expect regulators alone to instil a culture. That has to come from industry leaders, mentors and educators. And, as with all aspects of risk management, it has to come from within the individual as a result of the education that individual has received. It can also be augmented by exposure to role-models, constant communication and an awareness of the other professional's perspective.

In 2018 we watched bankers face up to the fact that many had embraced a culture that had to change if they were to avoid the risk of being taken out of the game altogether. My prediction for 2019 is that we'll see users of the sky having to equally look inward to determine whether their culture is sustainable. Let me know whether you think there are lessons to be learned between my silo of aviation and your silo, whatever that may be. Let's COMUNICATE!

To contact Jerry – www.jerryg.co – jerry@jerryg.co – 0438 059912



The Alternative to Despair - Collaboration in Risk

By: Madeleine Taylor Chief Risk Officer **YMCA Canberra**

Risk Management is a critical function for all organisations - private, public and not-for-profit. However, despite being widely recognised as critical, it is usually staffed with small teams who are allocated limited resources in favour of more obvious areas such as operations and marketing. These small teams often have wide ranging responsibilities and work with stakeholders who have little interest in engaging - believing the prevailing view that risk is a tick-box activity with little value. The teams are often using templates developed way back in time, or brought with them from prior roles, and are so focused on the churn of business as usual, and the grind of uninterested stakeholders, that there is little time or enthusiasm for improvement or innovation as the years pass by.

The result of this situation can be basic and low-value risk management in organisations, and staff who lose their passion for risk and move on.

Don't despair though - there is an alternative to this scenario.

Emerging in some organisations is an appetite for collaboration and a continuous improvement approach to risk management. These organisations will lead the way in how risk management professionals, and more broadly, functions in organisations, collaboratively develop and share their improved templates and models. This has been noted by PwC in their 2018 Risk in Review Study, and I have seen it in practice at the Department of Health in Canberra as well as my own work with YMCA Victoria and YMCA New South Wales.

At the Department of Health in Canberra, they have regular Community of Practice sessions which attract up to 50 professionals whose work involves risk in some capacity. They listen to best practice speakers, share experiences and ideas and together improve risk management practice in their organisation. Further to this, they have been working to identify other organisations in Canberra with a similar appetite for improvement and collaboration, so they can learn from each other and in turn all improve. An example of an idea that was born from this exercise, is their Risk Day planned for August 2019 which will see relevant staff attend informative sessions throughout the day on risk, visit stalls and have quality time with their risk team.

Some work I have been doing with YMCA Victoria and YMCA New South Wales, in my capacity of Chief Risk Officer of YMCA Canberra, is another example of collaboration resulting in improved practice. Over the past six months we have been meeting and slowly negotiating changes to our individual templates and models which will result in a (mostly) standard set which will not only reflect best practice in risk management, but will allow for further collaboration efforts such as consolidated training and possibly even software.

Collaboration work like what the Department of Health and YMCA are undertaking, requires risk professionals to be vulnerable and to share warts and all. It requires time and effort and the setting aside of pride to think we know best. Importantly, it requires a shared understanding from our Executive of why risk management is important, and how collaboration and a focus on improvement is critical for having mature and high-value risk management.

Think about what collaboration opportunities exist for your organisation, and reach out to your fellow risk management professionals to get something going. It could be as simple as sharing templates or talking through your common challenges and how you have each overcome them. Your risk management practice, the value you bring to your organisation, as well as your enthusiasm for risk can only benefit.

If you get stuck, there are some great resources out there including your local RMIA Committee and Risk Management LinkedIn groups

Below Source: PwC, 2018 Risk in Review Study; Base: 1,258
Q: As you envision the future of your risk management function, please supply one adjective to describe that vision.

A Key Component Missing From Your Risk Management Plan

By: Chris Gray Partner **First Light Consulting**

Areport released in 2018 by global consulting firm Deloitte, entitled 'Faster, Stronger, Fitter: Crisis Management for the Resilient Enterprise', found that seven out of the 11 key lessons documented in post-crisis environments related directly to communications.

The report noted, for example, that close to 20% of risk professionals admitted that they should have communicated more effectively with employees during a crisis, 14% acknowledged better communications with business partners would have been beneficial and 8% said their customer communications required significant improvement. A further 15% said they should have developed and executed more timely and robust communications plans.

Tellingly, a greater focus on communications planning and implementation, would have reduced many of the problems identified in post-crisis analysis.

These findings highlight a pressing reality: even the best scenario planning in the world risks being compromised to some extent if one key component of the mix is overlooked or under-prioritised: communications. Risk planning and crisis communications must work hand-in-hand at all times if an organisation is to maximise the benefits of both functions. To do otherwise can place the very survival of a business in jeopardy when dealing with a major crisis.

The role of communications in managing and dealing with risk is further amplified by a long-term study undertaken by Oxford University which shows that companies that respond poorly to a crisis lose an average 20% of market value in the proceeding months, while those that respond effectively gain 10% over the same timeframe. That's a 30% differential!

Having worked closely with many organisations in developing crisis plans, our observations support the view that the companies which recover the quickest and with the least disruption are the ones where the risk and communications teams have worked in tandem from the outset to identify, plan around and manage incidents.

One only has to look at some of the high profile crises of recent times to appreciate the role communications plays in the risk management process. A chilling example is the United Airlines incident in April 2017 where a passenger was dragged off a plane at Chicago's O'Hare Airport when the flight was overbooked. In awful scenes captured by passengers, dentist Dr David Dao is shown being pulled kicking and screaming down the aisle of the plane by airport security staff. The vision was shared across social media platforms and TV networks across the world with an estimated 200 million people viewing the footage within hours.

The airline's stock price and brand quickly went into free-fall as it mismanaged its response to the incident, initially supporting the actions of staff and then accusing the passenger of refusing to not adhere to company policy. When the airline's CEO was finally forced to apologise for the incident 24 hours later, no reference was made at all of the treatment handed out to Dr Dao.

Within days, the airline was forced to change its policies, travellers across the globe started boycotting the brand and the passenger filed a massive lawsuit. Additionally, the stock price tanked $1.5 billion (or 12%) and the CEO resigned.

Many observers have since noted that while the airline industry's overbooking policies should be reviewed, the way United's management mishandled the communications response to the incident was the fundamental reason the incident escalated into a full-blown crisis.

While United's stock price has rallied somewhat in the 24 months since the incident, the airline will forever be held up as a 'poster child' of what not to do when it comes to crisis communications with many travelers and corporate clients still refusing to fly with the airline.

The incident proves beyond a shadow of a doubt that in today's 'always-on' world, where anyone with a smart phone is effectively a reporter and a cameraman, an organisation's brand and financial health can be trashed in a heartbeat when it does not respond and communicate appropriately, even if procedures and processes were implemented according to plan.

In our experience, Boards and senior executives in Australia are only now starting to take more notice of the role communications plays in crisis management. Even seemingly minor incidents, which once could be have been dealt with at an operational basis, now require deft communications and messaging to reduce the chance of reputational damage.

The salient message here is that while risk managers can develop effective plans which tick all the boxes, communications must be incorporated into every aspect of the process. With this in mind, here are a few tips to encourage you to work with your communications team to ensure all aspects of a crisis are planned and prepared for.

Step 1: Audit the stakeholder experience
Understanding how to prepare for and manage the consequences of a negative experience is the first step towards ensuring your brand and business is prepared to survive it. Look at every aspect of your business from the perspective of customers, business partners and employees: your website, shop front, social media platforms, customer service, staff, the quality of your product including warranty and return policy. While you already have an indication of what could go wrong, where the risks are and key scenarios you could encounter, this will provide a baseline to show management how much the brand will be impacted should a crisis occur. Discuss and review the scenarios in depth with the communications team in order to ensure they have included all the possible eventualities in their planning.

Step 2: Consider your brand values
We all know that developing a robust, workable and realistic risk management plan is an investment in protecting the value of your business. Review and ensure your plan is built around the organisation's core values, company ethos and key messaging as your plans will then have a better chance of being fully aligned with your brand and hard-earned reputation.

Step 3: Test the plan
Ensure the communications team is part of any/all testing. Have mock journalists turn up with video cameras, or create fake social media posts from customers to demonstrate how the issue can spiral out of control. Review the results. Are there areas for improvement? What vulnerabilities were uncovered? Put steps in place to ensure best practice, then test again.

It is clear that the complexities and risks in business are multiplying in strength and diversity every year. A negative issue must be looked upon as an opportunity to show the human face of the brand. Having a clear brand vision and a crisis communications plan in place allows the organisation and executives to feel in control and equipped to deal with that inevitable negative occurrence.

When you think of how your plans will protect the business and impact your bottom line, make sure you also consider the broader

impact communications will have on your brand's reputation and performance.

Chris Gray is a Partner with First Light Consulting, a crisis communications advisory and training firm that provides strategic, legal and media counsel to help organisations prepare for, and respond to, a crisis or operational threat. Learn more at www.firstlightconsulting.com.au

Risk. It's Growing Digital

By: Antoine LeTard General Manager **RSA Australia & New Zealand**

It's creeping into business of every shape and size. It's sneaking into government, not for profit and society at large. Bit by bit. Byte by byte. Gigabyte by gigabyte. It's the yang of digital transformation's yin.

Organisations are extending technology deeper into their operations to improve processes, efficiencies, value and effectiveness. Inadvertently, it also raises their exposure to digital risk.

Digital risk is the unwanted, and unexpected outcome that stems from digital transformation and the adoption of digital technologies. As a result organisations are exposing themselves to risks from cyberthreats, third-party meddling, business continuity interruptions and data piracy.

There's little doubt of the significance of transforming analogue organisations to digital.

Gartner, a global research and advisory firm, reported in Harvard Business Review that digital business reached a tipping point in 2018. According to the report, 87 percent of senior business leaders say that digital transformation is now a priority and in many cases is a do-or-die imperative.

Australia's maturity in digital transformation is relatively advanced, compared to the world.

Dell Technologies' Digital Transformation Index II found that only three percent of Australian organisations are Digital Laggards, compared to nine percent globally. Forty-three percent of organisations in Australia are Digital Evaluators, compared to a global 33 percent. And Australia has seven percent of Digital Leaders, while globally there are only five percent that are in that commanding position.

These progressions in digital transformation suggest a broadening portfolio for risk managers to include digital risk management.

Digital risk management refers to processes for identifying, assessing, evaluating and monitoring, and ultimately mitigating risks associated with digital transformation. This also involves emerging technology, such as the Internet of Things (the growing network of devices including vehicles and home appliances that contain technology and connectivity to connect, interact and exchange data), big data, cloud technologies and mobile.

With digital transformation so prevalent amongst every industry, business leaders are beginning to understand that they can't protect their organisation from every risk. Therefore, managing digital risk is a business issue, not just a technology one. And to properly manage this risk, organisations must take a unified approach that has been agreed upon by all stakeholders.

By proactively managing digital risk, organisations can focus on the financial impact this has on an organisation, including lost opportunity, impact on revenue and reputational damage, just to name a few. This quantification of digital risk provides a foundation for managing risk across disparate business functions.

Digital transformation is one of the most influential forces redefining business today. From encouraging collaboration, to increasing agility and innovation. While the process of digital transformation improves business, it also inadvertently uncovers three increasingly intertwined business challenges: modernisation, malice and mandates.

These challenges are intensifying for companies with ambitious digital transformation initiatives, as pressure to innovate and grow generates new complexities and risks that organisations must manage.

Modernisation - In the pursuit of modernisation, digital technology offers organisations opportunities to transform their operations, resulting in increased speed, agility and efficiency. The explosion of information, user preferences, connected devices, digital channels and third-party applications can introduce new threats and risks. Virtual and hybrid cloud environments, and a global social network also create IT security complexity.

Malice - Technical complexity, combined with a cybersecurity talent shortage and organisational silos, can create an abundance of new opportunities for adversaries, who have more tools, resources and patience than ever before. Threat actors continue to mature with data breach and identity theft rates doubling every 15 months. As a result of IT modernisation attacks are harder to detect and have broader business impact.

Mandates - Governing bodies are trying to drive more accountability for data security and privacy by enforcing risk-based requirements versus prescriptive checklists. In Australia, the Office of the Australian Information Commissioner introduced the Notifiable Data Breach scheme to make organisations accountable for data breaches. This is where security and risk requirements are converging to shift the conversation from technology-focused security issues to a business risk and mitigation challenge. With traditional governance, risk and compliance programs proving to be inadequate, companies now require a continuous compliance strategy and more rigorous data privacy governance across borders.

The growing pace of business requires organisations to manage and coordinate cross-functionally more fluidly and agile than ever before. When it comes to digital risk, many leaders are grappling with where to start, where to go next and how to keep a sustainable and evolving strategy aligned with the business.

Managing digital risk effectively requires collaboration between security and risk management teams. Aligning security and risk provides organisations with:

1.visibility so they can be sure they have the right information and business context

2.insights to understand what is happening and determine how responses can be prioritised

3.the ability to take appropriate and timely action.

There is no single risk profile that applies to every organisation, which makes the task of digital risk management challenging. There are, however, three steps that help organisations get started. Each, ultimately familiar to risk managers.

1.Identification: Uncover where digital risk exists in the organisation.

2.Assessment: Assess how well prepared the organisation is to deal with risk in different areas of the business.

3.Planning: Identify and implement a rigorous process for managing, mitigating and avoiding digital risk that incorporates data and insights from across affected areas of the business.

As digital transformation is no longer the sole domain of IT, neither is digital risk management. Both have grown to touch all aspects of organisational development. The best way to balance the tremendous advantages of digital transformation against any digital risk is for the risk portfolio to undergo its own digital transformation, understand digital risk more thoroughly, and for IT to grow closer to risk managers.

Yin and yang.

Interview Series : Bree McLennan - The Diary of a Self-Confessed Risk Nerd

By: Simon Doherty

Welcome to the Risk Management Institute's of Australasia's (RMIA) (Victoria Chapter) interview series that showcases the people who break the traditional risk management mould. We search for people who are doing risk management differently, drawing from very different backgrounds and using skill sets in unique ways to provide real and valuable risk management insights and solutions. If you're doing something different, put your hand up and tell us - different is good, different is innovative and different could be the way of the future! Read on to start your journey with us.

Self-confessed data nerd, competitive sprinter, risk management specialist and healthy living enthusiast, Bree McLennan provides us with an insight into the symbiotic relationship between data science and risk management.

Bree walks us through her diverse background that as the story unfolds is anything but boring, and provides us with a great insight into how her exceptional cross dimensional skill set developed.

From the get-go it is evident there is an extremely efficient and analytical scientific mind that yearns to ask and answer the 'why' questions. What's also evident is a genuine humanitarian warmth that strives to utilise that diverse skill set to make individuals' lives better via her work at the Transport Accident Commission (TAC) and high-performance athletics coaching.

To back up the 'boots on the ground' experience, Bree casually mentions an extensive list of undergraduate, postgraduate and industry qualifications that must have made FEE Help weep.

The diary of a self-confessed risk nerd.

Bree please tell us about yourself?

In one headline, I'm a data science and healthy living enthusiast. On one end of the spectrum I'm a fully-fledged computing technology and data and risk nerd, and on the other end of the spectrum I'm an athlete who is passionate about athletic performance coaching. It's been my life's work to date getting these two different facets to blend with balance.

Background:

Amateur athlete, passionate runner.
Athletic performance coach. Owned and operated a small athletic performance coaching business and now currently an owner of a small family business in personal fitness training, strength and conditioning.
Broad spectrum IT industry experience ranging from technical support to systems engineering, training facilitation to technical thought leadership.
Transferred skills and experience from IT to working with business data in business intelligence.
Combined a collection of eclectic professional experiences, became a data scientist and also a risk practitioner.
(To see Bree's full list of qualifications scroll to the end. We had to cut it back because it is sooooooooo long!)

What does a data scientist do?

Since the role of a data scientist is relatively new compared to many other traditional STEM industry roles, the job description varies depending on who you ask.

My current textbook answer to this is; data scientists help businesses and people interpret and manage data. Data scientists understand the spectrum of transforming data into wisdom and they solve problems using expertise in a variety of different niches, including their own business subject matter expertise, and where appropriate they will use and apply tools and methods originating from computer science, mathematics, statistics, machine learning and artificial intelligence.

My personalised definition of what I routinely do as a data scientist is, I help TAC to identify areas where we can be managing our data better. I look for and communicate actionable opportunities originating in the data which enable us to better understand and clarify support needs for our clients, our providers, and even ourselves as staff and business units. In the spirit of science, I explore and experiment with new tools, algorithms and methods to discover new and value-add ways we can use our data to support improved decision making in our claims management space.

In the data analytics landscape the key questions I'm always seeking answers to are:

1. "What might be interesting"? Relating to automated data exploration and data discovery.

2. "What is likely to happen?" Relating to predictive analytics and forecasting.

3. "What can we do about it?" Relating to prescriptive analytics and advising on possible outcomes for scenarios.

So when data scientists and risk people get together, risk management turns from art to science?

I like to think a balance between art and science can promote an optimum result when it comes to risk practice. When it comes to assessing risks, opportunities, testing our control framework and simulating consequences, certainly a data-driven approach using modern data science methods offers a great, evidence-based and truthful starting point for a healthy risk discussion. However in our business we're a social insurer, the majority of our business is about "people" and therefore being emotionally intelligent is an occupational requirement. We acknowledge that most of the time, there are humans directly behind the numbers we crunch, the data we analyse and use in predictive exercises. Algorithms can produce biased results if used carelessly and for us the impacts of such carelessness if it were to occur would flow on to our clients, the people we exist to support and our external partners who help us provide support. All these flow on impacts would detract from our organisation's mission to be the world's best social insurer.

In the balance between art and science, as data scientists we provide scientific, data-driven decision support tools to the business. These tools aim to remove the cognitive load in routine business decision making and assist in calling out the likely decision path to follow. Experience teaches us, nothing which involves humans is ever 100% certain and science-based decision support tools while useful, are not perfect and are subject to regular review and continuous improvement to maintain their usefulness and relevance. A human being is still needed to make the ultimate business decision and the tools we create as data scientists are intended to increase the likelihood that the human being making the decision is making the most informed, best possible decision to drive the best possible outcome.

How do you work with risk owners and risk management SMEs to traverse the qualitative gap from I 'believe' this is a risk, to I 'know' it's a risk?

A few years ago in our journey of upskilling our TAC risk champion network and risk team via the Diploma of Risk Management and Business Continuity course, we came to a startling realisation that a lot of the time what we think is a business "risk" is in fact either an enterprise-wide shared causal factor, a consequence or an issue. It is not an actual "event" which if realised has the potential to "sink the ship" of the business. Learning about the true nature of "cause" and "effect" was thoroughly enlightening for all of us. At the time we realised this, our enterprise risk register had more than 200 enterprise business "risks" documented.

After our educational enlightenment we've come to realise and accept that truly there are less than 20 enterprise business risks, and these risks have many shared causal factors and consequences. These risks describe the real events that if were to occur would directly threaten our organisation's ability to operate and exist.

The benefits of detangling and simplifying our risk register made it so much easier for us to focus our energy, attention and work efforts on the big ticket items we must get right as an organisation, and stop sweating the small, noisy stuff.

These days when we receive queries about "how do I know this is a risk?", we like to remember and share what we have learned on our learning journey to date and ask more important questions like "can this be more appropriately defined as a causal factor, consequence or an issue, instead?" and "can you demonstrate the effectiveness of the controls you have, versus the real business problem you have?".

Outside of the TAC world, how do you see the application of data science, and the risk management function and risk owners working together, in for example a commercial sense - the translation of risk's potential cause or effect on the P/L or performance KPIs?

The TAC is a unique kind of business versus many other organisations, where our paradox is we are a social insurer and we do not aim to increase the number of clients we have. A perfect world for us is where no one suffers road trauma on our roads, or in a Victorian registered vehicle. We measure ourselves on the rehabilitation outcomes our clients achieve, how many lives we save and serious injuries we reduce through the "Safe System" approach of safer roads, safer vehicles, safer speeds and safer people, and by how well funded the scheme is to continue providing this noble service to the community.

As a TAC data scientist who is balancing art, science, empathy and logic, in a different business world I see the application of data science to be the same as we apply it at TAC. We apply data science when we seek to better understand the nature of our business, to have better, clearer comprehension of the data landscape which is supporting the business. The balance sheets, performance KPIs and reports may look different between business worlds, however the math, statistics and algorithms largely stay the same. The variable creating the difference here is the business purpose, business rules, and the problems the business is attempting to solve.

Data Scientists are advisers, just like risk practitioners and we want to work toward ensuring that the most optimum business decisions are being made. We must work collaboratively with risk owners, else the advice we have to share will yield no value and contribute nothing in business decision making. In a collaborative context, the data scientists support the risk owners by advising the optimum path forward while the risk owners decide, action, and drive the path to take.

On the flip side of risk there is opportunity, how can you support the identification and achievements of opportunities?

The world of science is wonderful. There are people out there who are always seeking to improve methods and the world around them for the greater good of all. There are wonderful people like this in the data science industry and I like to think some of those people work here!

As our technology and computing power improves, so does our ability to work with data. In the spirit of scientific endeavour we are always seeking out new algorithms, tools and technology we can apply to our data, sometimes we need to do this in researching options to approach business problems and sometimes we need to pioneer an entirely new approach or tool to inspire the business to keep on track with TAC's mission and continue to innovate forward. Part of the journey to be world leading is to have the courage to explore and pioneer within new and unfamiliar frontiers and iteratively apply valuable lessons from these experiences to grow and become what we seek.

Qualifications:

Bachelor of Information Technology. Majored in Information Systems & Games Design and Development
Certificate IV Training and Assessment
Information Technology Infrastructure Library (ITIL) - Industry Certification
Change Management Foundation Certification - Industry Certification
Neuro Linguistics Programming (NLP) Practitioner Certification
Recreational Running Coach Level 2 (Athletics Australia)
Certificate III Fitness Instructor, Certificate IV Personal Trainer
Certificate IV Small Business Management
Diploma of Risk Management & Business Continuity
Data Science industry certificates & online study: Machine Learning, Deep Learning, Text Mining & Natural Language Processing

RMIA Profile Series: Simon Weaver

By: Heather Wilson Marketing Consultant **Willis Towers Watson**

Having spent over 20 years in insurance broking in Asia, Simon Weaver knows there's a diverse range of approaches to risk management which reflects the different cultures and economic maturity throughout the region.

Now Head of Australasia for global advisory, broking and solutions company Willis Towers Watson, Weaver believes organisations which can demonstrate their understanding of these heterogeneous markets throughout Asia Pacific will be best placed to deliver optimal risk outcomes.

Take China as an example. "While China continues to emerge and is looking to influence the region and beyond through multi-billion dollar investment programmes such as the One Belt, One Road initiative, there is no single way for all the players involved to look at risk," Weaver says.

"Let's take an infrastructure project for rail, or a port under One Belt, One Road, as an example; how you marry up and relate to all the joint venture partners who may not have the same cultural attitudes to risk or insurance is crucial. That might apply to risk retention or risk transfer strategies, but also in devising benefits programmes for local employees in territories where the investor may be inexperienced in managing talent.

Weaver took the top role in Australasia at the start of 2019, having been head of Willis Towers Watson's Corporate Risk and Broking practice for Asia Pacific, based in Singapore. He spent much of 2018 commuting to Australia and New Zealand, relocating with his family in December.

"I'm also keen to explore some of the perspectives from the Asia region and how they might add value to our work in Australasia," he says. "While the recent Royal Commission in Banking and Financial Services has forced certain companies to look at their culture, this is a much broader imperative because the risks and challenges facing businesses today are evolving at such a rapid pace.
"Only those organisations who embrace diversity in their thinking and in their workforce will be able to devise holistic risk management strategies for their own clients."

Weaver says the 'Future of Work' is a big theme for Willis Towers Watson's Australasian business. "It's something our clients need help with; when we look at who is doing it well throughout the region, I can't help but look to how the Singapore government has led the way in retraining its workforce for the Fourth Industrial Revolution."

Through the 'SkillsFuture' program, announced in 2015, the Singapore government is investing more than $1 billion annually up to 2020 to drive a more agile workforce. A main plank of SkillsFuture is that all Singaporeans over 25 are incentivised to retrain or develop their careers with a $500 payment.

"That kind of government intervention isn't likely to happen in Australasia so developing workforces and enhancing their agility need to be addressed at organisation level. It helps businesses deal with key elements of risk – how to be adaptable and flexible in a rapidly-changing environment.

"The speed of risk and disruption is at an all-time high. Organisations and particularly their boards are needing to deal with a range of risk management themes. The future of work is just one, among globalisation, consolidation, AI, cyber and regulatory oversight. Organisations are also being impacted by cultural change and increased social awareness among all stakeholders – employees, clients, shareholders and the community at large.

"All these elements can influence on each other; our clients are looking to us to combine our perspective on risk, using analytics, global benchmarking and thought leadership, along with risk financing, risk identification and risk transfer.

"Since our merger at the start of 2016, we've developed a set of analytical risk tools that delve into the range of insurable exposures for our clients, creating actionable insights. This goes across the totality of our business; clients are looking for help across a range of risks, whether it's M&A advice, blending employee benefit schemes or consulting on the future of work.

The Weaver family has settled into Sydney. "My kids were absolutely delighted with the move and we've all felt much more at home since we got into our house in January.

"I certainly arrived here at an interesting time, particularly for the Australian market, with the release of the Royal Commission into Banking and Financial Services report. It was a significant wake-up call for all organisations looking after the end-user – the people we're trying to support and protect – to ensure they have the best interests of their customers at the heart of what they do.

"I've worked in this industry for over 30 years all told, with roles in retail insurance as well as wholesale and treaty reinsurance broking markets. Our clients rely on us to know the risk environment and how it impacts on their business and their customers. The challenges are complex, but I firmly believe we have the right combination of expertise and analytical insight to be able to deliver real value for our clients and, through that, to the people who rely on us."

RISK

THE NEW FRONTIER

RMIA ANNUAL CONFERENCE 2019