RISKNZ

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

RISKPOST

RISKNZ MEMBER NEWSLETTER

SEPTEMBER 2018

WEB
risknz.org.nz

POST
PO Box 5890, Wellington 6140

EMAIL
adminofficer@risknz.org.nz

RISKPOST DISCLAIMER

RiskPost is the newsletter of RiskNZ Incorporated. RiskPost welcomes contributions from members of RiskNZ. Any such contributions do not necessarily represent the views of RiskNZ as a whole, although from time to time RiskPost will publish items setting out the views of RiskNZ on a particular topic.

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

A WORD FROM THE CHAIR

NIGEL TOMS – *Chair, RiskNZ*

Welcome to the third edition of RiskPost for 2018. September 2018 is a busy month for RiskNZ including:

- The Practitioners Day titled Practice to Performance - Risk Management in Action on 12 September 2018. At the time of writing, tickets are almost sold out, however, there is the opportunity to join some or all of the sessions by webinar, so please take the opportunity if time allows. More information can be found on page 25.
- On 20 September 2018 the inaugural Auckland breakfast session featuring a presentation by Nick Hill, Chief Executive of ATEED. See the update on Breakfast Networking Forums on pages 6 – 8 for more information.

IN THIS EDITION...

A WORD FROM THE CHAIR CONTINUED...

In the last RiskPost I gave my thoughts on Tesla and its challenges and the possible risk management approach they might employ with their continuing financial trading losses. Just after RiskPost was published I saw an article about a battery fire that had damaged a new Tesla and waited to see if there would be more similar stories followed by debate about product recalls which would be very damaging. However, this appears to have been a one off and Tesla remained unaffected.

Tesla's share price began to rise, moving from a low of $267 approximately 6 months ago to $379 in early August 2018. What could possibly stop the share price rising further?

Well for reasons that are beyond me, Elon Musk then tweeted that he was THINKING about taking Tesla private and has already sourced the $70 to $80 Billion required to achieve this aim!! The market understandably did not react well to this announcement with reports of investigation by the US Securities and Exchange Commission, and the share price dipping below the USD 300 level in late August. My only thought about this announcement was 'if you are going to do this, get on with it, don't talk about it', continuing market uncertainty in this regard will likely give unfavourable results.

While the Tesla story continues to intrigue, this latest strange episode is really a distraction. The real story is around financial performance and moving the company into profit. This is still a very real challenge for Tesla and has the potential to threaten Tesla's survival if not managed well.

Last week I was privileged to attend a presentation by Dr Deborah Pretty from Pentland Analytics titled Understand Reputational Risk in the Cyber Age – The Impact on Shareholder Value. The presentation covered the resilience of organisations when responding to the eventuation of a significant risk which has the potential to damage the organisations reputation.

Her analysis shows that there is a 50/50 split between winners and losers, with winners increasing share value by up to 20% and in contrast, losers decreasing share value by up to 30%. The key characteristics of the winners who quickly recovered their share value and then thrived include:

1. Investing heavily in preparedness including challenging simulations.
2. Strong Chief Executive stepping up to lead the response.
3. Accurate well co-ordinated communications.
4. Instant response – no delays, long debates with lawyers, slowing the response are likely to result in the organisation ending on the losing side.
5. Showing true remorse where errors have been made, followed by credible action and commitment to meaningful change.

As a comparison consider:

- Samsung and their decisive action when faced with battery fires affecting their newly issued Galaxy Note 7 phones in August / September 2016. They ceased production and completed an expensive full product recall which was favourably viewed and the company and associated share price has continued to prosper.

- VW who were forced by the US Environmental Protection Agency to reveal that they had deliberately programmed their diesel vehicles to defeat the emissions tests. While the CEO resigned 5 days after the event, the public perception continued to view VW as a company that were unapologetic for these actions and the share price fell heavily. Their woes continue with perceived poor handling of the defective seat belt issue earlier this year.

An understanding of an organisations key risks and continuing work to increase associated organisational resilience is an increasingly important area to ensure survival when major challenges which can significantly impact brand and reputation arise.

FROM THE EDITOR

SALLY PULLEY - *RiskNZ Deputy Chair*

A big thank you to all who have contributed to this Edition, which contains a range of articles combined with updates on RiskNZ activities and membership.

We have particular pleasure in introducing you to our new EO, Sathya Mithra Ashok, on page 25, and we provide updates on breakfast meeting forums and the RiskNZ Practitioner's Day.

Kristin Hoskin continues her series of updates on what is happening in the 'standards space'.

News items on the ISO website note that ISO 31000:2018 '*places a greater focus on creating and protecting value as the key driver of risk management and features other related principles such as continual improvement, the inclusion of stakeholders, being customized to the organization and consideration of human and cultural factors …'*
and that *'It also includes some substantial improvements, such as the importance of human and cultural factors in achieving an organization's objectives and an emphasis on embedding risk management within the decision-making process …'*.
Our RiskPost contributors echo these themes:

- Mike Wood facilitated the latest Wellington breakfast meeting, and has provided a Practice Note on the extension of quantitative risk analysis methodology to assist in making decisions between different options.
- Sarah Stephens contributes two articles on the topic of Cyber Risk, including commentary on common misconceptions.
- Sue Trezise identifies two thought provoking online reads - the 2018 Edelman Trust Barometer and the strategic governance of risk. Both of these are worth a long online read.
- Kerry Grass shares some tips in her second article on Anti-Money Laundering (AML) compliance.
- Silvia Zanini looks at the thorny issues of project failure and organisational culture; and
- Ben Stevens provides a thoughtful discussion of business models, disruptive waves and the pace of change. This follows-on from Ben's presentation on business model disruption at our 2017 Conference.

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

A BRIEF UPDATE – FROM RISK MANAGEMENT TO RESILIENCE

Nigel Toms' presentation in April titled *'From Risk Management to Resilience'* raised a number of questions from the audience. Nigel subsequently contributed an article to the May edition of RiskPost, which was accompanied by a call for comments and questions from our readers.

The University of Auckland's Focus Group on Organisational Resilience has provided a forum for ongoing discussion of organisational resilience and the capability of business to cope with uncertainty. We hope to provide a further update after the Focus Group meeting of 27th August.

CALL FOR CONTRIBUTIONS

The next editions of RiskPost will be published in November 2018 and February 2019.

RiskPost is designed to provide topical and thought-provoking material, as well as updates on things related to risk. Please contact me with ideas for articles or content that you would like to see included.

If you see an interesting article in a magazine or on a website, that would be of wider interest to RiskNZ members, please let me know. RiskNZ will seek the rights to republish, or provide links to the content, on the website and in RiskPost.

Please send me an email at *editor@risknz.org.nz*

RISKNZ STANDARDS UPDATE

KRISTIN HOSKIN - *RiskNZ Management Board Member*

OB-007 met 16-17 August in Brisbane and by teleconference. Work continues on development of HB436 Risk Management Guidelines (a companion to ISO 31000). The majority of the meeting was spent reviewing and refining content for this handbook.

As a point of note Standards New Zealand has opted out of issue of a joint standard of 31000 with Standards Australia, although OB-007 Committee voted 95.25% in favour of an AS/NZS adoption. The reason stated by Standards New Zealand was "because no benefit to New Zealand users in identically adopting the standard was identified during consultation".

The draft of AS ISO 31000 will be sent for publication imminently as comments close on 20 August. The adoption by Australia is an Identical Adoption, so only the preface will differ from the ISO version. The AS ISO preface makes a point of elements that are in contrast to practice or understanding in Australia. Standards New Zealand have indicated that while opting out of the publication of a joint standard, this does not necessarily preclude the handbook, HB436, becoming a joint publication. OB-007 continues to work on the handbook assuming joint adoption, but Standards New Zealand may decide not to opt in. If this occurs the handbook will be a Standards Australia publication.

In other related Standards work, Standards Australia MB-025 is about to formally begin the review of HB167 Security Risk Management Handbook. RiskNZ has indicated support of this review and working group. Standards NZ has opted into adoption of ISO 45001 as a joint AS/NZS adoption. AS/NZS 45001:2018 Occupational health and safety management systems - Requirements with guidance for use is currently out for public consultation (closes 28 August).

Comments received when Standards NZ initially provided opportunity for public comment have been forwarded and do not need to be resubmitted. If you missed that comment period, there is still time to submit comments through the Standards Australia public comment portal. Search for AS ISO 45001.

For further information on activities RiskNZ are party to on Standards please contact Kristin Hoskin *kristin@risknz.org.nz*

THE BREAKFAST NETWORKING FORUMS IN WELLINGTON, CHRISTCHURCH AND AUCKLAND

The Breakfast Networking Forums are an opportunity for RiskNZ members to meet and talk about risk management outside of workplace meetings or conferences and seminars. Meetings are relaxed and collegial, have a definite practical focus, and enable experienced and newbie risk practitioners to share thoughts and experiences. All attendees are encouraged to get involved in the conversation. There is no such thing as a stupid question - and believe me, this Editor has asked a lot of questions over the past few years!

Breakfast Networking has its roots in Wellington, and has been so successful that in 2018 it has been introduced to Christchurch and Auckland.

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

Contact details are:
Miles in Wellington at *miles@risknz.org.nz*
Kristin in Christchurch at *kristin@risknz.org.nz*
Darroch in Auckland at *darroch@risknz.org.nz*

THE NEXT CHRISTCHURCH BREAKFAST: PLAYING THE ODDS

Kristin Hoskin has introduced the networking breakfasts to Christchurch, and the next Breakfast Forum will probably be held in the first week of November.

We are still looking for a host. If any Christchurch members would like to host the breakfast please contact Kristin *kristin@risknz.org.nz*

The theme of the breakfast will be a discussion on how we use quantitative assessments in our risk management. All attendees are invited to share what they use quantitative inputs for. The peer voted best example shared will receive a copy of Challenging the Future as a prize. Hopefully attendees will come away better placed to pick winning horses for Cup Week as well as gaining new ideas for improving their risk management at work.

Once we have a host, details for registering for the breakfast will be posted on the RiskNZ website and on LinkedIn.

WELLINGTON BREAKFAST MEETINGS

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

Mike Wood facilitated the latest meeting of 25 July. Mike led a conversation on the use of the quantitative risk assessment to evaluate options on a risk-adjusted basis using some current examples that he has been involved in, such as the response options for the mycoplasma bovis outbreak.

The conversation was held under the Chatham House Rule. It was obvious by how the meeting ran over time that all attendees found the round-the-table discussions very informative and interesting.

Mike has authored a Practice Note on the quantitative risk analysis of options. - see page 7 for more information.

PRACTICE NOTE: QUANTITATIVE RISK ANALYSIS AS AN INPUT TO OPTIONS DECISION-MAKING

MIKE WOOD – *Broadleaf Capital International*

Risk practitioners will be familiar with the use of quantitative risk analysis to determine an appropriate contingency sum for a project or programme. The process involves the preparation of a model structure to link risks to the cost estimate, development of uncertainty distributions for the material costs or cost drivers, combining these with the deterministic costs in the model, and using Monte Carlo simulation to establish a probability distribution of the overall cost as the uncertainties drive variations in the cost. The contingency sum may then be estimated as the difference between the deterministic base cost and a point chosen on the distribution that reflects your appetite for needing to seek additional funds (the higher the percentile that is chosen, the less likely it is that the contingency sum will be exceeded).

An extension of the methodology is to apply it to assist in decision-making between different options for a project or any other type of future scenario where costs or revenue cannot be assessed precisely. A typical scenario is a choice between a "safe" but more expensive option and other options which may appear to be less expensive from a deterministic perspective, but which are subject to greater levels of uncertainty in respect of cost, duration, or achievement of the desired deliverables that impact on the anticipated benefits and so could actually cost more than the safe option. By applying the above process to each option and then comparing the costs of the options at the chosen percentile (typically the 85th or 90th percentile, which takes into account most of the uncertainty that has been modelled), a "risk adjusted" cost of each option can be used to select a preferred option which takes account of the risk and how risk averse (or otherwise) you want to be. NPV cost modelling is often used if the cost impact of the uncertainties is likely to occur some years after the initial expenditure. NPV calculations can be integrated with cost risk modelling to enable a choice to be made, for example, between a high up-front cost option and others that have a lower up-front cost but might have higher and increasingly uncertain costs in future years. This "whole-of-life- cost" modelling is the standard approach in such situations.

Applications of this approach include option selection and the establishment of acceptable funding levels for:

- equipment procurements and selecting from tenders with different headline prices and risk profiles;
- responding to major risks such as biosecurity breaches;
- technology selection for IT projects;
- designs for infrastructure projects;
- deciding whether to invest in systems to protect against business interruption.

Like any quantitative risk modelling, it assumes that the risks associated with each of the options have been at least identified and preferably analysed using a qualitative risk assessment process – quantitative techniques are of little use if the project is "flying blind"! However, given appropriate input information about the uncertainties, it is a very good tool to differentiate between the values of options at particular levels of risk, or to indicate at which level of risk one option becomes preferred over another. This gives the decision makers objective data on which to make a decision.

MIKE WOOD

Mike is a highly experienced risk management practitioner and senior manager. He is a past Chairman of the New Zealand Society for Risk Management (before the name change to RiskNZ). Mike's consultancy work with Broadleaf Capital International centres on the provision of advice, training and consultancy services in qualitative and quantitative project risk management, and risk management framework development and deployment.

THE INAUGURAL AUCKLAND BREAKFAST NETWORKING SESSION

Join us at RiskNZ's inaugural Auckland Breakfast Networking session on Thursday 20th September to hear Nick Hill, Chief Executive of Auckland Tourism, Events and Economic Development (ATEED) talk about:

'the future of Auckland's economic development, tourism and major events'

ATEED is a council-controlled organisation (CCO) established to lift Auckland's economic well-being and enhance the region's performance as the growth engine of New Zealand's economy. ATEED is tasked with developing tourism, delivering events and improving the economic performance of the region and international awareness of Auckland as a desirable place to visit, live, work, invest and do business.

ATEED champions a co-ordinated approach to all aspects of business sector development, working with central government and private sector organisations to maximise benefits for Auckland. This role is vital to Auckland's success.

Bookings will be essential as we need to have adequate seating and catering.

For more information and registration details please go to the *RiskNZ website*.

The provisional schedule is:
7am to 7:30 am - Networking over light breakfast
7:30am to 8am - Presentation
8am to 8:45am - Networking

Note: If you have any special dietary requirements, please let us know when you book for the event.

NICK HILL - *Chief Executive, ATEED*

Nick Hill joined Auckland Tourism, Events & Economic Development in the role of Chief Executive in August 2017.

Nick has extensive experience across the private and public sector. This includes the Chief Executive role with the Commerce Commission, and leading the formation of Sport and Recreation New Zealand (SPARC, now known as Sport New Zealand).

He also has significant experience in the energy sector, having worked 10 years with ECNZ and Fletcher Energy in New Zealand, and with Santos in Australia.

Before joining ATEED, Nick was a Partner of specialist New Zealand public policy and management consulting firm Martin Jenkins – which he joined in 2011 to establish the firm's Auckland practice.

RISK MANAGERS WANT TO TRANSFER CYBER RISK

SARAH STEPHENS – *Head of Cyber, JLT Global*

Risk managers have expressed a strong desire to transfer cyber exposures to insurers, amid growing concern for technology related risks, according to a survey of Airmic members carried out in partnership with JLT in the UK.

Cyber and IT-related risks have emerged as the top concerns for Airmic members, according to its survey. Cyber risk was ranked among the top three concerns by 39% of respondents, second only to reputation at 41%. However, risk managers expect cyber will overtake reputation and take the top spot within the next three years.

Airmic says that one of the common challenges facing all companies is how to embrace fast-evolving digital technology. The threat of competitors using new technology and business models to gain market share is another rapidly emerging concern, chosen by 21% - with 30% expecting it to feature in three years' time.

UNDER-PREPARED

Many risk managers feel that their organisations are ill-prepared to confront cyber risk. Only one-third are confident that their main cyber risks have been identified and quantified, while less than half (44%) are confident that their organisation has prepared for a cyber-incident and only 25% say that their data assets have been mapped and protected.

According to Airmic, this lack of preparedness is a concern. Only 22% strongly agree that the board has sufficient knowledge and understanding of cyber risks. When it comes to third-party cyber risks, the picture is darker still, with only 15% strongly agreeing that these are being managed in their organisations.

REACHING OUT

The Airmic survey also showed a growing desire to engage with insurers on cyber risk. Three-quarters of risk managers, surveyed by Airmic, buy standalone cyber insurance. Transferring risk through insurance is favoured for a number of risks whose origins sit outside the direct control of the company, and which are therefore harder to mitigate directly, according to Airmic.

Cyber business interruption is the third most desirable risk to transfer, after natural catastrophes and terrorism.

Some 45% of those surveyed say transferring data breach risk to the insurance market was their preferred mitigation approach, compared with 41% who would prefer to reduce their exposure. For cyber business interruption, 49% would prefer to transfer the risk, while just 33% would look to reduce exposure.

MORE ASSISTANCE

According to Airmic, there are a number of areas where risk managers would like help from insurers. Asked where they would like to see insurers develop services in response to data breaches, 58% of respondents show an overwhelming preference for support with responding to the data loss, while 48% would like insurers to increase their offering around cyber business interruption.

Airmic also says cyber insurance has matured in recent years and that risk managers are no longer concerned about capacity, cover and limits. However, consistency of cyber definitions and coverage remains an issue.

The Airmic findings echo a recent regional survey by JLT in Asia, which found increasing demand for cyber insurance in Asia Pacific. JLT reported a 95% increase in the number of policies and an 80% increase in premiums in 2017, driven by increased awareness of cyber risk and a number of high profile data breaches in the region. Some 80% of cyber policies sold by JLT in 2017 were standalone, while 20% were blended cyber and professional indemnity cover.

Similar to the Airmic survey, JLT identified in Asia an increased interest in cyber business interruption. 90% of clients with limits over USD 5 million now purchase business interruption cover, as they realise that much of their day-to-day business operations are reliant on potentially vulnerable IT infrastructure and interconnectivity issues.

CYBER RISK MANAGEMENT AND INSURANCE FAQS

SARAH STEPHENS – *Head of Cyber, JLT Global*

WHAT ARE CYBER RISKS?

Cyber risk emanates from both online and offline sources. For example, a hacker gaining physical access to upload malware on to an online ticketing system, a lost mobile device containing confidential information or a stolen lever arch file. Although the reliance on electronic communication and connected technology driven processes in today's world exposes companies to cyber risk, the data privacy elements of the risk are just as prevalent offline.

Cyber incidents can be perpetrated by numerous actors with a variety of motivations. Generally speaking, they can fit into four categories:

- The most prevalent and feared is the malicious external actor, who could be a criminal, a politically motivated group of hacktivists seeking to cause disruption or terrorists seeking to use technology to create physical consequences.

- Malicious actors also exist within companies and may either be disenchanted individuals with highly technical knowledge or access, or simply call centre or clerical employees who are approached by a criminal who induces them to steal data, introduce malicious code, or just provide physical access.

- Employees also cause cyber incidents through human error. For example, by clicking on the link in a phishing email, leaving a laptop in the airport, connecting to unsecure Wi-Fi networks or failing to check the security credentials of an unfamiliar individual on a work site.

- The vast web of vendors and outsourcers that companies rely upon. Many companies enforce strict security and data privacy regulations on perceived high-risk vendors such as data processors, but fail to consider that even the low-risk vendors pose cyber risk.

WHAT IS CYBER INSURANCE?

Cyber Liability Insurance is designed to mitigate both the first and third-party costs that you may incur due to a cyber-attack. First-party costs are those that your business may incur directly as a result of a cyber-incident, whereas third-party costs are those that you may be liable to pay others.

WHY DO COMPANIES NEED CYBER INSURANCE?

Most industries have become inextricably reliant on technology and data. On the one hand, this represents an opportunity to improve efficiency and profitability, while on the other hand it brings with it a host of emerging risks. Cyber exposures are real, ever-increasing and global in nature.

Cyber incidents can affect any company in a variety of ways. Data is often the target of a cyberattack, whether it's personally identifiable information of employees or customers; confidential information of other businesses shared under a confidentiality agreement; or the company's own confidential data such as trade secrets, business protocols or customer lists. Media content published in cyberspace also falls in scope and can result in allegations of defamation or intellectual property infringement. Social media use by companies and their employees expands the risk to include reputation and security issues. Finally, technology (both information technology and operational technology) is inextricable from the daily operations of most companies today. Technology can fail or fall victim to a cyber-attack, causing business interruption or liability consequences.

HOW CAN COMPANIES QUANTIFY THEIR CYBER RISKS?

Despite increased awareness about cyber risk, relatively few organisations have actually identified their cyber exposures and even fewer have attempted to quantify them.

For most companies exploring cyber insurance for the first time, exposure analysis and gathering underwriting information for a dynamic risk such as cyber can be daunting. Often, the insured isn't left with any clearer understanding of how their exposure has changed from year to year or in comparison to their peers.

Our Data Organiser tool efficiently facilitates cyber risk information gathering, illustrates your organisation's comparative cyber risk exposure and benchmarks you against peers with respect to exposure and maturity. Insureds can then evaluate changes in exposure and maturity from one year to the next, which can be used both for an underwriting submission and to provide insights for information security and other risk mitigation investments.

HOW CAN COMPANIES BETTER MANAGE CYBER RISK?

We suggest doing the following to proactively manage your cyber risks:

- Understand the top risks to your company and communicate to the management the risks that are and are not insurable. If not insurable, then identify alternative options.
- Understand your contracts with your customers. What risks is your company assuming? What types of insurance do you need to maintain?
- Know and meet regularly with your information/IT team and understand incidents or near misses.
- Review your risks with your insurance broker and insurer continually. Insurance coverage is negotiable.

DOES CYBER INSURANCE PAY OUT?

Although the lack of actuarial data and the difficulty of putting a price on a risk with so many moving parts has led many to question the worth of cyber insurance, the sharp rise in cyber-crime has propelled big businesses to seriously consider how the insurance industry can help them mitigate business risks associated with a data breach.

With insurers paying millions of dollars annually for cyber claims cyber insurance has certainly demonstrated its worth to companies with data privacy and network security risks. As with every line of coverage, however, there are potential pitfalls that insureds might face but can avoid.

For instance, in 2017 a federal court found that a US restaurant chain could not recover payment card industry (PCI) fines, penalties and assessments incurred under a master service agreement with its credit card processor. Specifically, the court ruled that an exclusion for contractual damages barred recovery. The restaurant's insurer, however, paid USD 1.7 million in other costs that resulted from the data breach which affected 60,000 customers. Currently, many carriers provide terms that expressly cover PCI fines and penalties and will carve back the contractual exclusion to avoid any conflict. So, the total quantum of loss would have been recoverable if the insured had a well drafted policy.

Cyber insurance is a rapidly changing market. Insureds should work with their brokers to ensure that policy terms follow recent challenges to and developments in coverage. Fundamentally, however, it remains a buyer's market and companies should be reassured that cyber policies deliver real risk transfer and value.

WHAT DOES A CYBER POLICY TYPICALLY NOT COVER?

As the threat of hacking and cyber-attacks on databases of all organisations has grown, so has the uptake of cyber insurance policies. However, when buying a policy, it's important to know exactly what's covered and what's excluded.

Things excluded in a cyber-policy:

War, invasion and insurrection

Most commercial property and liability policies exclude damage resulting from these events as well as terrorism.

Patent, software and copyright infringement

This is typically covered by intellectual property insurance forms and not by a cyber-policy. However, some broadly written cyber policies will cover defence costs associated with copyright infringement claims if they result from the actions of a non-management employee or an outside third party.

Bodily injury and property damage

This coverage, which is standard under a commercial general liability policy, is typically excluded in cyber insurance as a person cannot be physically injured by having their data exposed when your business' database is infiltrated.

Failure to take required security measures

When applying for a cyber-policy, the application will include a number of questions regarding the steps you've taken to safeguard your data. If it is later discovered that you have failed to implement these security measures an insurer might deny the claim.

Employment-related claims

These are mostly covered by an employment practices liability insurance policy and are thus excluded from a cyber-liability policy. However, if your employees' personal information was compromised, your policy would likely cover employment-related privacy violations.

DO MY CURRENT INSURANCES COVER ME FOR A CYBER BREACH OR ATTACK?

Many professional indemnity policies will provide some insurance cover in the event of a cyber-breach, but there may be significant gaps, which include the following:

- Cover for loss of employee and partner information
- Breach investigation expenses, including specialist independent legal advice, forensics and IT security expertise
- Costs incurred by the firm to notify affected individuals, offer appropriate credit and ID monitoring services and hire appropriate public relations expertise
- Cyber extortion expenses incurred to end a credible extortion threat
- Reimbursement of data and computer programme restoration expenses and consequential loss of revenue resulting from a network interruption

COMMON MISCONCEPTIONS

"I am not a target for hackers."
Technology and cybersecurity are becoming increasingly sophisticated, yet human error remains the main cause of cyber incidents. Whether it's an employee leaving a password out in the open or sending sensitive documents to unintended recipients, business owners could be left exposed by employee missteps.
"We do not sell goods or services online so we are not exposed to cyber risk."
If your company captures or stores customer and vendor data, you have cyber risk. Cyber policies are designed to address the risk of utilising technology, computers and internet connectivity while conducting daily business which includes capturing, storing and using data every day.

"We use vendors for all our IT services."
According to data regulations, the company that collects data and records from clients is held responsible if a data breach occurs. Legal liability cannot be transferred by contract; therefore, if a point of sales device is compromised, the obligation to notify impacted parties will fall on the business owner and not the vendor who processes or stores payment information.
Indemnification agreements typically limit recourse to the value of the contract. However, an average data breach involving personal financial records could cost a firm thousands of pounds, well in excess of the value of many vendor contracts.

"We have top notch security in place."
There is no such thing as perfect security. Agencies including the UK Government and the Ministry of Defence have been hacked by inside and outside parties, proving that no security solution is impenetrable. Cyber insurance augments even top-notch security solutions.

"Our general liability policy will cover the loss."
General liability policies currently lack the flexibility to address new and emerging cyber perils. In fact, the majority of general liability policies specifically exclude cyber.

"I don't collect a lot of data."
Every business with employees and vendors collects and stores private information such as addresses, health information, marital status, bank account information, payment history and human resources records. Additionally, if you sell goods or services, every financial transaction carries protected information such as credit card and bank transfer information. The mishandling of such information can lead to a liability or public relations challenge.

"But my biggest risk is my reputation, and this can't cover that..."
Your reputation is entwined with your ability to deal with a cyber-incident. Evidence shows that a swift reaction to mitigate the impacts of a data breach will minimise the immediate costs, and potentially reduce the exposure to subsequent slow-burn costs, which include reputational damage and loss of competitive edge.

SARAH STEPHENS

Sarah Stephens is the Head of Cyber for JLT Global.

Prior to joining JLT in 2015, Sarah spent 12 years with Aon in a variety of roles. Most recently Sarah was Aon's Head of Cyber & Commercial E&O for the Europe, Middle East, and Africa (EMEA) Region, working with colleagues across business groups and clients in the region to identify, analyse, and drive awareness of cyber risks, exposures, and both insurance and non-insurance solutions.

ONLINE READING - TWO THOUGHT PROVOKING PIECES

SUE TREZISE – *Sue-lutions Ltd*

The 2018 Edelman Trust Barometer

With reputation management being a key focus in both the public and private sector, the 2018 Edelman Trust Barometer provides interesting reading. The study underlying the report was undertaken in times marked by the rise of disinformation and a questioning of what and who to believe. Reputation and trust go hand in hand and the report notes that global trust remains on average at a distruster level showing a greater polarisation of trust across and within countries.

Based on the question 'how much do you trust the institution to do what is right?', the general population (those over the age of 18) consider NGOs (53%) and business (52%) are more trusted than government (43%) and media (43%). By country the global average is 48% with China (74%), Indonesia (71%) and India (68%) being the most trusted. At the other end of the scale are South Africa (38%), Japan (37%) and Russia (36%). Trust decline in the USA has fallen from 52% to 43% which the authors note is the steepest ever measured. While New Zealand doesn't feature in its own right, it is interesting to consider which country we would be most aligned to in this context. The Netherlands and Mexico sit at 54%, Brazil and South Korea at 44%, with Australia and France at 40%.

According to the report, trust in a company ranked more highly than 'high quality products and services' or 'business decisions reflecting company values'; making building trust the number one job for CEOs. Reputation and trust go hand in hand and this finding further validates the importance of managing these as key risk areas. For risk specialists this means providing senior management and executives with risk information and insight that maintains the confidence of staff and stakeholders.

Meanwhile, the report identifies that one upside of trust (and truth) being 'elusive' is people having a renewed faith in credentialed voices of authority, signified by in a rise in the credibility of experts.

In response to the question 'if you heard about a company from each person, how credible would the information be?', technical and academic experts were rated in the very/extremely credible category by over 60% (increasing by +3% and +1% respectively). The credibility rating of CEOs, Boards of Directors, and government officials have all shown positive change (+6-7%) with journalists improving the most (+12%). The credibility rating of information 'a person like yourself' - often a source of news and information on social media - has fallen to an all-time low. The credibility gain for the voices of expertise is encouraging (and reassuring) news for risk specialists. This is an opportune time to further embed risk practices as an essential element of organisational trust and reputation.

Source: *https://www.edelman.com/trust-barometer*

Strategic governance of risk: Lessons learnt from public sector audit

In a recent address to the Institute of Internal Auditors-Australia, Grant Hehir (Auditor-General for Australia) noted that the importance of effective risk management has been highlighted in many reviews of organisational failure. The reviews identified the importance of having not just good risk processes, but also strong governance and clear accountability to establish effective risk culture.

Other suggested key indicators of an effective risk culture include:

- the board and its sub-committees engaging with risk through establishing risk appetite and tolerance, along with active oversight and challenge of management responses to emerging risks;
- clear responsibilities and accountabilities for risk and an effective performance framework linked to risk outcomes;
- monitoring implementation of risk treatments, changes in risk ratings, and emerging risks;
- proactive, not just reactive, approaches to risk;
- learning from your own and others' mistakes;
- fit-for-purpose management arrangements, which are consistently communicated; and
- adequate resourcing with a focus on building staff capability.

Of particular note is the comment "Good risk managers produce innovative outcomes, because their entity's risk tolerance allows for failure, remediation and learning where the decision making in the risk management process was sound".

The accompanying paper (to the speech) is an interesting read and is available here: *https://www.anao.gov.au/work/speech/strategic-governance-risk-lessons-learnt-public-sector-audit*

SUE TREZISE

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

SUELUTIONS Ltd
An independent and practical approach

HOW AN 'INFORMED CULTURE' CAN HELP PROJECT SUCCESS

SILVIA ZANINI – *New Zealand Post*

Project success rate in NZ
A KPMG's 2017 project management survey (188 respondents) found that 21% of projects are "consistently delivering on their benefits" (Barlow, et al., 2017).

Which means that 79% pf projects are not.

Why are projects failing?
Looking at 'project failure' through the lens of organisational and safety culture, sheds light into why companies fail to learn from past experiences, why 'abnormal' behaviours become accepted, and what it takes to ensure that companies are successful. These lessons can be transferred to other fields, including project management and project governance.

Organisational culture is defined differently based on what people's ideas are.

- one school of thought sees organisational culture in the context of change and of achieving a company strategy, culture is driven from the top and can be imposed on an organisation. One culture applies to the whole company. Culture is something that an organisation 'has' (Reason, 1997).

- another school of thought thinks that the above description is very optimistic. Company-wide change programs, driven from the top, usually fail. Instead, successful change programs start at a local level and are led by local leaders. Culture is built from the bottom up, created by members of a group - not imposed, not uniform across the entire organisation, but is made by the sub-cultures existing within a company. Culture is something an organisation 'is' (Smircich, 1983).

I tend to think that the second school of thought is on the money – but I think that many organisations adopt the first approach.

Projects may fail to deliver due to:

- No effective reporting: disincentives to reporting include the extra work, a natural desire to forget what happened, lack of trust and fear of punishment, not forgetting scepticism, as if nothing ever changes after reporting, why report at all?

- No accountability: no clear demarcations between acceptable and unacceptable actions. Or maybe the demarcations are there, but the fact that they are not enforced result in abnormal behaviour becoming normal (see below)

- No learning post failures: this includes observing, reflecting, creating, and acting – with acting on the information being the most difficult element to implement (as there is always something more pressing to do)

- No flexibility in the organisation: the best people might not be used when needed, the organisation is not able to adapt to changing demands, teams are not able to work autonomously

- There often is also an element of 'making the abnormal normal': this happens when people within an organisation become so accustomed to a deviant behaviour that they do not consider it deviant: the people that adopt this deviant behaviour do not do it deliberately, they are not trying to deceive or to break the rules, the fact that the abnormalities never result in negative consequences, result in them becoming the accepted norm. This is what happened in the 1986 Space Shuttle Challenger disaster: prior to the disaster, in several instances, the O-rings that were found to be the technical cause of the explosion suffered damage due to a design flaw, but because the recurrent problem had no negative consequences, the design flaw and recurrent damage became normal, catching everyone by surprise when the component failure resulted in disaster. NASA didn't learn from this experience and in 2003 another disaster, the Space Shuttle Columbia, occurred (Vaughan, 1996).

An 'informed' culture
Culture change happens when an organisation's core assumptions are changed: it is difficult and time consuming. Organisational change results from organisational learning as opposed to being achieved quickly by "management decree". For organisational learning to occur the culture of an organisation must be one of trust and openness, in which people feel encouraged and protected to disclose and report information, in turns allowing the organisation to learn.

Such a culture is a just culture (Reason, 1997). A just culture is different from a no-blame culture, where no matter what one does, nothing is sanctioned - therefore creating an "environment of impunity" with no incentive to act sensibly. A just culture provides clarity of the boundaries between acceptable (honest mistakes) and unacceptable (culpable) behaviours, of who sets these boundaries and how they are set.

A just culture is one of four key components of an **informed culture**, which plays a major role in successful organisations:

- effective reporting, including data on faults, errors and near-misses
- a just culture, encouraging employees to report and providing clear, known, boundaries between acceptable and unacceptable behaviours
- a learning culture, able to act on information and implement change
- a flexible culture, able to morph from a hierarchical to a decentralised structure when required.

An additional vital component is that of senior management support: without senior management support in both actions and words (Pidgeon, 1998) an informed culture does not stand a chance to occur.

Implementing the above in an organisation will help to create the 'right' culture and result in organisational success.

Finally: what is your context?

People don't (usually) come to work to do a bad job. Often they make poor choices due to their context: what is the underlying message they receive, are there conflicting messages between what people in their organisation say and how they act, are teams all working toward the same goal, or is there an element of looking after their own patch? For example: ramp workers at airports have very tight turnaround times – which are often unrealistic; often accidents happen as procedures are not followed, but in reality the underlying message ramp-workers receive is that 'on time performance' is a must, resulting in the need to break or bend the rules to ensure the planes leave on time, with managers tolerating this behaviour and only complaining when an accident happens or the on time performance is not met.

Employee behaviour is in some degree produced by the work environment, if senior management place great emphasis on the need to achieve benefits could it be that a reality of great benefits to be achieved by investing on a project could be constructed? Could this result in misrepresenting project benefits, in massaging the plans, in being overly optimistic?

BIBLIOGRAPHY

Barlow, G., Tubb, A. & Riley, G., 2017. Driving business performance, Wellington: KPMG.

Pidgeon, N., 1998. Safety culture: Key theoretical issues. Work & Stress, 12(3), pp. 202-216.

Reason, J., 1997. Managing the Risks of Organizational Accidents. 2016 Kindle ed ed. London and New York: Taylor and Francis.

Smircich, L., 1983. Concepts of Culture and Organizational Analysis. Administrative Science Quarterly, 28(3), pp. 339-358.

Vaughan, D., 1996. The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA. Chicago: The University of Chicago Press.

SILVIA ZANINI

(CIMA, CGMA, AMBCI)

Silvia is a risk manager at New Zealand Post, currently studying towards a Risk, Crisis and Disaster manager Msc at the University of Leicester. Silvia has extensive risk and audit experience gained in Italy, the UK and NZ.

POST IMPLEMENTATION OF ANTI-MONEY LAUNDERING COMPLIANCE

KERRY GRASS – *Anti-Money Laundering Consultants Limited*

This is Kerry's second article on Anti-Money Laundering Compliance. Kerry's initial RiskPost article: 'NZ Spreads a Wider Net to Detect Money Laundering' is published in the May 2018 Edition, which is available online in the member's area of the RiskNZ website.

From 1 July 2018 lawyers and conveyancers became known as 'reporting entities' under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act). The implementation date for accountants, book-keepers and tax agents is 1 October 2018. Real estate agents and the New Zealand Racing Board follow on 1 January 2019.

This means before each relevant implementation date, reporting entities must complete an anti-money laundering and countering financing of terrorism (AML/CFT) risk assessment. The risk assessment is required to measure the likelihood of the reporting entity facilitating ML/FT in the course of its business.

The risk assessment is then followed with the development of an AML/CFT programme. The programme establishes the policies, procedures and controls and must be aligned to the findings of the risk assessment. Where the risk assessment has identified areas of higher vulnerability for the likelihood of ML/FT occurring, the programme must address how the reporting entity will mitigate and manage those risks.

The AML/CFT programme is therefore the engine of an AML/CFT framework. It represents a broad range of components that need to be monitored and maintained on an ongoing basis. Failing to do so may result in a compliance breach.

Having spent the past 8 years as an AML/CFT consultant, I have become familiar with common failings of Phase 1 entities. In this article I will therefore share some tips to assist Phase 2 entities avoid the same pitfalls.

Training

Training is required for all employees that have a role linked to AML/CFT compliance. This includes senior managers. A senior manager is defined in the AML/CFT Act as being equivalent to a director of a company, or holding a position comparable to a director, or a person who occupies a position that has influence on the administration or management of the reporting entity. This includes CEOs, CFOs and Board members.

Training should be at the right level. This means the training delivered to senior managers may not need to be at the same level of training that was provided to staff members who are involved in the opening of accounts and/or delivery of services direct to clients.

The AML Compliance Officer is responsible for determining adequate requirements for training.

Following a training session, it is advisable to provide a written assessment which will assist to ensure the training has resulted in employees obtaining the expected level of understanding.

Refresher training should be delivered on at least an annual basis.

Client Risk Profiling

Meeting the obligations of ongoing customer due diligence and account monitoring requires the reporting entity to ensure the business relationship with the client is consistent with their risk profile (section 31(2)(a)). Therefore, failing to implement client risk profiling is likely to result in the reporting entity being unable to establish they have met their regulatory obligations. This includes managing an adequate and effective programme (section 57 of the AML/CFT Act).

Further, without client risk profiling, reporting entities will be unable to make determinations of when enhanced due diligence should be applied. Section 22(d) states enhanced due diligence must apply – 'when a reporting entity considers that the level of risk involved is such that enhanced due diligence should apply to a particular situation'.

A key aspect of client risk profiling is to understand the client's expected account activity. This should include the expected volume, value and nature of account/transaction activity. Without knowledge of the client's expected activity, it is unlikely the reporting entity will be able to detect unusual or suspicious activity. If a reporting entity is unlikely to detect unusual or suspicious activity, then the requirements of section 57 have not been met.

Client onboarding is the best opportunity to capture sufficient data to apply client risk profiling. This is because customer due diligence requires obtaining and understanding the purpose of the client's proposed business relationship. Add a few additional data inputs to this process will enable a client profile to be established.

Ongoing Monitoring

The requirements of ongoing customer due diligence and account monitoring is set out at section 31 of the AML/CFT Act. To meet this obligation the programme should include the type of client activity or behaviour that the reporting entity will be vigilant for. This is commonly referred to as 'red flags'.

It is important to ensure written records are maintained to evidence ongoing monitoring is being carried out and the determinations made. The recording of determinations should enable an auditor or AML supervisor to understand the rationale for either filing or not filing a suspicious activity report.

Record Keeping

Should a reporting entity find itself in regulatory hot water, it will only be able to establish a reasonable defence through record keeping. This is because a court will be unable to determine the existence and adequacy of any procedures established by the reporting entity to ensure compliance (section 98(2)(b)).

Further, as record keeping assists an auditor and AML supervisor to make determinations on compliance, a reporting entity should ensure their procedures and processes incorporate written records. This applies for each component of an AML/CFT programme.

General Obligations

To meet AML/CFT compliance requires a certain level of AML/CFT expertise and sufficient resources dedicated to administrative functions. By applying a consistent approach to the application of adequate policies, procedures and controls, supported with a healthy compliance culture, AML/CFT compliance is not difficult to achieve.

KERRY GRASS

Kerry Grass is an executive consultant for AML360, and has held the status of a Certified Anti-Money Laundering Specialist since 2005.

She has worked in anti-money laundering positions with government in three jurisdictions. Since 2010 she has worked in a private capacity as an AML advisory expert and in 2013 she partnered with software engineers to develop AML360.

AML 360 provides regulatory technology and outsourcing services for small and medium sized businesses. AML360 is now recognised as a leading global software vendor in anti-money laundering compliance.

Further information: *aml360.co.nz*

WHAT'S IN A BUSINESS MODEL?

BEN STEVENS – *Risk Dynamics*

RISKDASHBOARD™
where risk meets strategy

We are living in some chaotic times. What we are witnessing right now, with the internet of everything, is however no different to what people experienced at the turn of the last century. The invention and commercialisation of the light bulb sparked something of an electric revolution. Prior to the invention of the light bulb, power did not represent the utility it is today. The invention of the lightbulb lead to more and more houses being connected to the power grid. As a result, a whole industry around the manufacture and consumption of electronic devices was born. Some inventions were abhorrent (the electric chair, the Heidelberg belt); others had a profound effect on and daily life and in turn drove the creation of numerous other inventions (the fan, for example, has found application in computers, cars, refrigerators and many other inventions).

History is littered with "disruption" and companies that were not able to read the signs of the times. Western Union, who once owned the world's telegraph lines did not see the potential in Alexander Bell's new-fangled device. Nowadays, they just do money transfers.

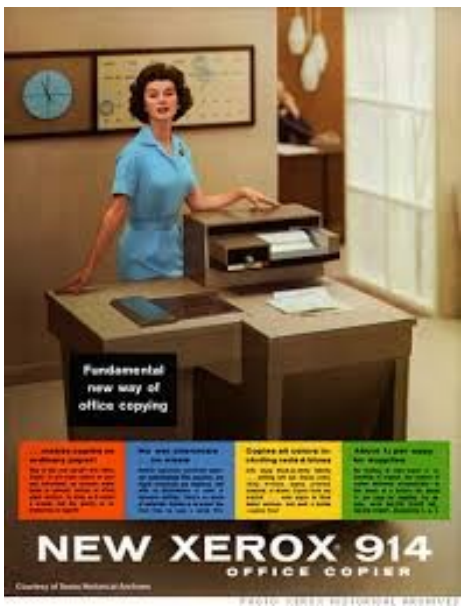
What is different to previous disruptive waves is the pace of change today. Many of the changes we experience today are driven from computational processing; they are driven by advances in microchip technology. A microchip roughly doubles in its price-performance ratio every 18 months (this is Moore's law). When the Spinning Jenny was rolled out (sparking the first industrial revolution), one Spinning Jenny replaced roughly 8 workers. It was a simple linear equation. It upset the Luddites and led to the Luddite uprising.

The microchip is to the internet of everything, what the lightbulb was to electricity.

A great analogy for today's exponential change that is often bandied around (and is not technically correct) compares the computational power of a mobile phone to the technology that was harnessed to land us on the moon in the late 60s. It's a hard one to fathom, but I wouldn't trust my iPhone to land me on the moon. It would probably be a one-way ticket. This aside, we can all agree that the current rate of change is mind-boggling and effects of multiple pieces of technology intersecting can be seen in many areas.

One effect is the decline in company life expectancy. The S&P500 life expectancy has dropped from roughly 67 years to around 17 years. Mortality is also on the rise – the fortune 500, which tracks the largest companies by market cap, at its inception in the 1960s had a churn of roughly 10-20, more recently this has jumped to between 40-50 (or effectively doubled).

People often cite Kodak and Blockbuster as great examples of disruption. However, what a lot of people do not talk about is the digital giants that have also found themselves carcasses on the verge of the information super-highway. Whatever happened to Myspace? Only 10 years ago it was bigger than Facebook. The effect that Tinder is having on traditional dating websites is also another interesting one to watch. Some might argue that pure digital models are fraught with risk. Most people agree though that traditional boundaries between business models and industries are evaporating and that we are set for a turbulent few decades ahead. Amazon is getting into banking (they started out as a book-store), while WeChat, a social network, is now one of the world's biggest payment providers (paying with cash in China is a novelty). Dyson, who make vacuum cleaners, are looking to build electric vehicles. The traditional verticals are becoming very fuzzy; the traditional risks associated with "the competition" are being totally redefined.



Many talk about disruption (or technology) as being the root cause. The reality is that technology drives disruption and that disruption drives the proliferation of business models which truly disrupt! Business model risk is one of the biggest risks facing companies today. So much so, that one of the victors in this space has even coined a new verb that may find its way into the English dictionary: "to be netflixed", aka to be disrupted – or is this because we are just tired of hearing the term "disrupted"?

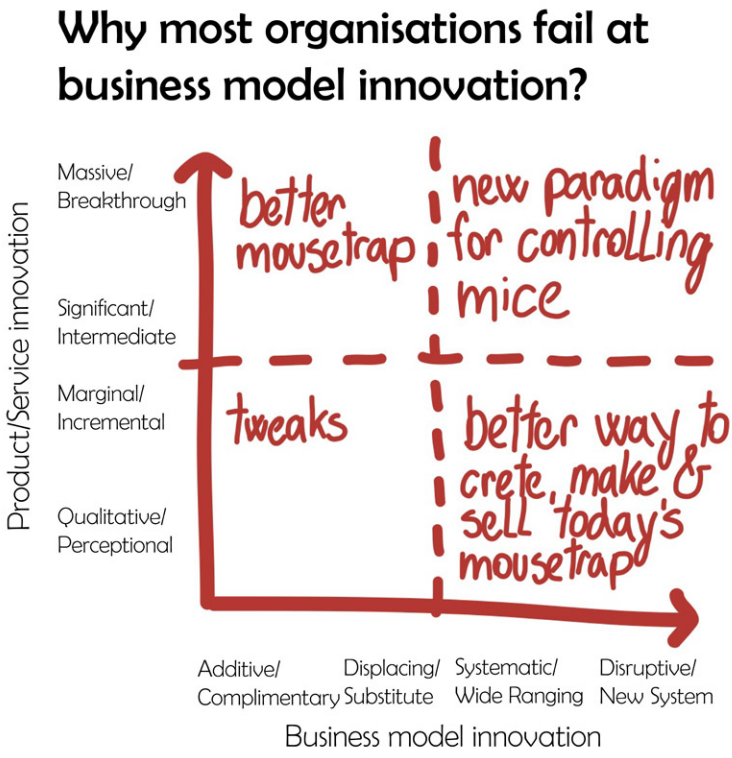
The threat of being a carcass on the verge of the information super-highway is real. It is also one of the biggest risks facing companies in the digital age. But those risks are often ignored or poorly addressed. Part of the reason for this comes back to the fuzziness of the terms - what do we really mean by business model disruption? If we cannot define it, how can we fix it? The other reason is that to combat the risk, a significant amount of risk needs to be taken onboard (often risking core products/services and their associated revenue streams). This forces a sort of reconciliation between risk and strategy. Finally, if we also overlay this with a focus over the last 20 years on operational efficiency methodologies, lean, six-sigma (or strategies that have a more measurable focus), then this lack of addressing business model disruption as a risk comes as no surprise.

It is hard to address something that's not well defined. A bit like trying to define what a company's core competency is. If it's not the leaves of the tree but the trunk, what's the trunk?

To compound matters, there are a fair few academic definitions of what a business model is. Joan Margaretta (HBR) notes that although the concept is old, it has really only become more mainstream with the advent of the personal computer and spreadsheets (Excel). This gives a clue to how we define what a business model is: monetisation plays a key role. It was iTunes that really disrupted the music industry. iTunes enabled a legitimate way to share (and monetise) content (Spotify is now really disrupting this model).

Osterwalder's "lean start-up canvass" is also being increasingly used as a methodology for defining business models. Central to the lean start-up canvass is understanding the value you provide to the end-customer (or the problem you are trying to solve). Related to this is the concept of what sandpit you are playing in. John McGee (WBS) talks about the business model being tied to the role that you occupy in the industry-wide value-chain. The approaches to defining business models are of course all related.

Many companies that are being disrupted recognise that they need to tweak, change, or reinvent their business model to survive. Saul Kaplan, the author of the business model innovation factory, charts business model innovation on two dimensions: product innovation or business model innovation.



Most companies tend to either create a better mouse trap (product innovation) or create a better way to produce or monetise that same mousetrap (business model innovation).

The music industry, in trying to combat disruption, created a whole plethora of new formats (DVD Audio, Mini-discs, SACD) etc. Kodak did something similar in the late 1990s by creating APS film roll (also hailing this as one of the biggest consumer inventions of the last decade, putting it up there with the PC). These strategies of product innovation in a disruptive environment failed.

The other crucial point here is that business model disruption has also created a huge amount of opportunity for companies.

In the early 1960s, Xerox was a very small operator with a turnover in the tens of millions. They took a huge risk, and in many respects pioneered the photocopy lease-model that exists today. Rather than selling their new 914 photocopiers for the princely sum of USD 29,500 a piece, they decided to sell them on a pay-per-sheet model. By the late 1960s, they had a market cap of 8 billion. They grew so big that to photocopy something became synonymous with "to Xerox".

Hilti, one of Europe's leading power tools manufacturers, have recently started a subscription-based model ("tools on demand"). The upside of business model disruption is there are numerous different ways now to monetise a product. There is also a plethora of alternatives to the "razor-blade" model.

Disruption on a big scale is really equivalent to a new paradigm for controlling mice (new product and new way of monetising). It can lead to the creation of entirely new markets. I would argue that Airbnb and Uber are good examples of this. Xerox's 914 was possibly also an example of this (the 914 was revolutionary, as was the method of monetisation).

Kodak were and still are regarded as one of the most innovate companies to have graced the planet. Product innovation alone is not enough in the face of disruption. To avoid being "netflixed" or becoming another carcass on the verge of the information super-highway, you need to consider taking risks with your core revenue streams and innovating your business model.

BEN STEVENS

Ben Stevens is the Chief Executive of Risk Dynamics and founder of the RiskDashboard™.

Ben has an extensive background in risk and has spent over a decade working in senior strategic risk roles across a variety of industries.

Ben developed the RiskDashboard™ as an online service after growing tired of seeing many companies use unwieldy spreadsheets to track their risks. The tool allows companies to automate the information gathering and reporting process, aiding strategic planning and ensuring key risks are identified. The RiskDashboard™ is a Silver Sponsor of the RiskNZ Practitioners Day 2018.

12 SEPTEMBER 2018 | 55 FEATHERSTON ST, WELLINGTON

PRACTITIONERS DAY 2018

PRACTICE TO PERFORMANCE: RISK MANAGEMENT IN ACTION

Curious about Practitioners Day? This year we will be holding our annual professional development event in Wellington. Practitioners Day is a one-day event with six speakers that ends with our RiskNZ Awards of Excellence ceremony.

Our objective in holding Practitioners Day is to give risk management practitioners an opportunity to boost their tools for implementing risk management with executives and key stakeholders. Each speaker will draw on practical experience-based approaches that they have used successfully (and lessons they have gained from unsuccessful efforts).

The keynote speaker, **Scott Milne** is flying in from Australia to speak on Coordinating response to an unknown event. He will be drawing on his own experiences with coordination of searches for Malaysia Air Flight 370 from when Scott was the Rescue Manager with Australian Maritime Safety Authority.

Miles Crawford, from our RiskNZ Management Board will be speaking on managing risk appetite; workshopping techniques and practical application of his research over the last few years.

With extensive experience in post-earthquake risk and landslip risk **Matt Howard** (an expert in geotechnical risk) is going to speak on post risk realisation - how to dust yourself off and get back on track.

Des Irving is the Principle Advisor Fire Risk Management Region 3 for Fire and Emergency New Zealand. Des will be sharing how Fire & Emergency as an organisation address engagement with communities regarding risk and the public.

Shaun Sellwood is a Broking Manager for JLT and has a depth of experience across all classes of insurance, where he will be speaking about Cybersecurity.

Dr Richard Vipond a Public Health Physician and Medical Officer of Health holds a number of portfolios at the public health unit at the Waikato DHB. Richard will be speaking about Risk and the media – crafting public information.

There will be opportunities for all practitioners to learn from their experiences in gaining strategic buy-in from key stakeholders to work collaboratively on minimising risks.

In the interest of boosting interaction, the day is limited to 50 people in Wellington at the venue but we are also running online access for individual sessions or the day using the Go-to-Meetings software. So, if you can't get away for the whole day, why not register to attend online from your computer?

The climax of the day will, of course be the Awards presentations. If you are in Wellington please show your support for our Awardees and attend the Award Presentation Ceremony.

REGSITER HERE NOW!!

Premier Sponsors

JLT

SAI GLOBAL

CAA CIVIL AVIATION AUTHORITY OF NEW ZEALAND

Gold Sponsors

PALADIN RISK MANAGEMENT SERVICES

NAVIGATUS CONSULTING

Silver Sponsor

RISKDASHBOARD™ where risk meets strategy

INTRODUCING OUR NEW EXECUTIVE OFFICER

Please congratulate our new EO, Sathya Mithra Ashok, who joined the RiskNZ in June 2018

SATHYA MITHRA ASHOK – *EO, RiskNZ*

Before joining RiskNZ, Sathya was Operations Manager at New Zealand Global Women. She is a current member of the board at Dress for Success (Auckland) and at AUTSA.

Sathya brings over fourteen years of experience, spanning communications, management and strategy, specifically in media organisations, small businesses, social enterprises and non-profits, across three countries and two continents.

As part of multinational organisations, she has designed and executed on growth strategies, expanded revenue opportunities and been key in rolling out plans across diverse countries.

Passionate about small businesses, micro-enterprises, social enterprises and community organisations, in her most recent roles she has supported them by providing critical input in strategy formation and implementation, and in understanding the unique nature of markets they address.

With postgraduate qualifications in mass communications and business administration from AUT, she brings with her proven ability to develop and execute on strategies, build multi-stakeholder relationships, manage resources and finances, and deliver on goals.

Sathya's contact details are:

Email *sathya@risknz.org.nz* **LinkedIn** *http://linkd.in/1tbZ6QK*

RISKNZ

RISKNZ INFORMATION

THE MANAGEMENT BOARD AND OFFICERS OF RISKNZ

Chair:	Nigel Toms	Deputy Chair:	Sally Pulley
Secretary:	Jim Harknett	Executive Officer:	Sathya Mithra Ashok
Treasurer:	Gary Taylor	Administration Officer:	Virtual Assistants NZ

Management Board Members:

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

INFORMATION FOR CONTRIBUTORS

The next editions of RiskPost will be published in November 2018 and February 2019.

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

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

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

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

RiskNZ
PO Box 5890
Wellington 6140

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

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

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

RISKNZ WELCOMES NEW MEMBERS

RiskNZ welcomes the following new Members for this financial year...

Corporate Members:

- NZI Insurance
- Hastings District Council

Individual Members:

- Christel Fouche
- Crespo Gao, Kiwihealth
- Gillian Somerville
- Scott James
- Tim Casey, Manager Risk & Compliance, Nelson Marlborough Health
- Rodney Young, Lead: Quality & Audit, Te Wānanga o Aotearoa
- Andrew Rimington, National H&S Manager, Arrow International
- Ben Lynch, Risk Consultant, Aon
- Paula Zinzan, Risk & Resilience Specialist, Trustpower