RiskPost

Issue 15 No. 2 July 2015

Contents

RiskNZ gratefully acknowledges
the support of our premier sponsor

JLT

This page is intentionally left blank

Headline News: New Premier Sponsor

Tim Jago

Executive Officer, RiskNZ
tim@risknz.org.nz

RiskNZ is delighted to announce that leading global risk and insurance services provider JLT is coming on board as a premiere sponsor, with a three year agreement that will see RiskNZ assisted to grow its capacity and capability to support and lead the risk management sector in New Zealand.

In confirming the sponsorship agreement, RiskNZ chairman Geraint Bermingham highlighted the many synergies that exist between the two organisations. “RiskNZ and JLT both hold respected positions at the forefront of the risk sector; both have increasing reach in to every corner of business and society, and JLT’s business services are fully aligned to RiskNZ’s vision that New Zealand prospers because risk is well managed”.

For its part JLT’s New Zealand CEO, Matthew Riddle, is heralding the sponsorship as an opportunity for his team to collaborate with the risk management sector to put in place a range of programmes and activities that build capacity and capability. “At a time of fast evolution in the risk management space RiskNZ is showing commitment to providing thought leadership, and enabling risk management professionals to develop and stay abreast of emerging best practice. From a JLT business development perspective it is inherently sensible for us to be getting right alongside NZ’s leading risk management professionals”.

The sponsorship value remains confidential to JLT and the RiskNZ Board. However, the financial investment by JLT sees it assuming the title of Premiere Sponsor. Built on a platform of collaboration and high engagement, the sponsorship will see JLT and RiskNZ working together to deliver an enhanced programme of member focussed services as well as new activities intended to elevate the risk management sector in the eyes of Government, big business and the SME and NFP/NGO sectors.

The culmination of several months of discussions, the sponsorship roll-out commences immediately. JLT’s brand will now be omnipresent alongside RiskNZ and many key RiskNZ programmes will now be presented with a JLT–RiskNZ banner. The JLT team will be involving themselves in RiskNZ outreach activities such as the increasingly popular lunchtime seminar series and professional development days, and RiskNZ is able to draw on JLT’s nationwide corporate resources.

Deborah Fisher, Divisional Manager Client & Business Relationships, will manage JLT’s side of the sponsorship with RiskNZ’s interests fronted by Tim Jago. Celebrating the signing of the sponsorship agreement, Deborah Fisher commented “We are genuinely excited to be joining with RiskNZ and to share in their vision for the future of RiskNZ as a peak sector body and their plans to grow societal understanding of contemporary risk management best practice. They (RiskNZ) truly understand that their plans can best be delivered through partnerships, and we look forward to being one of those partners, and also working with RiskNZ to create a powerful family of sponsors that together can do some truly great things”.

Editorial

Miles Crawford

Editor, RiskPost

editor@risknz.org.nz

In my last editorial I talked about how the rebranded RiskNZ has emerged as an upbeat, progressive organisation compared to its somewhat staid predecessor, and how exciting it was to be a RiskNZ member at this time. JLT coming on board as the new premier sponsor only adds to this excitement, and is not only a huge success for the RiskNZ, but also enhances our organisation's brand and standing within the risk management community.

I think this theme of excitement or enthusiasm was also present at this year's AGM. I felt that over all, members were happy with the direction that RiskNZ was taking and were keen to see the business plan put into effect. But more about that in 'A Note from the Secretary' later in this issue.

Now that the AGM is out of the way it is time to focus all of our attention on the upcoming RiskNZ: 2015 Risk Management Development Day on Tuesday 13 October. For those of you still deciding on whether you will attend or not, I highly recommend that you do. Personally, I have learned so much from attending past RiskNZ seminars – from the basics of risk management, to how human nature and risk work together, to in-depth discussions on how risk management is used in practice. Registration is now open and for more information please follow this link http://www.risknz.org.nz/newevents/risknz-2015-risk-management-development-day/

Finally, I encourage you to plunge into this issue of RiskPost. As always, the articles in this issue cover a wide breadth of risk subject matter which I hope sates the appetites of members. However, my mantra is 'More is Better', so please feel free to contribute an article on your favourite risk subject, or just comment on someone else's through 'Letters to the Editor'. All articles and letters to the editor can be emailed to editor@risknz.org.nz

Chairman's Corner

Geraint Bermingham

Chairman, RiskNZ
Improving the knowledge and practice of risk management in New Zealand
chair@risknz.org.nz

Firstly, thanks to everyone who came along to the AGM this year. This was the first AGM since the significant changes to the constitution were approved and of course the name change to RiskNZ. Also, the new web site and the many associated service enhancements have been, and continue to be implemented. As such it was a great opportunity for members to be part of a discussion about these many changes as well as to debate the Annual Report and Business Plan for 2015-16.

Implementing the changes of the last 12 months has taken considerable effort on the part of the Management Board - but it has been exciting. There is no doubt that the use of the notably more contemporary name, RiskNZ, has opened up avenues and is well received when members of the committee are in discussions with other organisations and potential sponsors.

It is worth reminding ourselves of the rationale for the name change. It ensures that rather than responding to a risk agenda, we, as a professional body are seen to take a proactive role and participate in the setting the risk agenda in New Zealand. The changes also reinforce the position of RiskNZ as the peak sector and professional body bringing together those people and organisations managing risk.

Tim Jago made the point during the debate that, in his many discussions with other similar organisations, the one common theme is that all are having to challenge themselves, to re-define their role and to find new and fresh solutions on how to deliver value within to the context of the vastly changed, and now continually changing, needs of their membership. The key lesson for me is that the greatest risk of all is to resist, as opposed to embrace, change.

Just as this is true for professional societies, so it is for all organisations - and ourselves as risk professionals. In whatever field of endeavour, the ability of an organisation to understand and manipulate risk in the now continually changing organisational context, is without a doubt critical to success. This puts the risk professional in a key position - as an agent of success.

Just as RiskNZ is repositioning to change the perception of the profession, so we all as risk professionals need to ensure that we too are seen as responsive, progressive and as agents of success. We need to ensure that our expertise in the management of risk is truly valued, and that senior decision makers come to expect and demand that risk professionals are involved in all key decision making processes.

Enjoy the ride!

Executive Officer's musings...

Tim Jago

Executive Officer, RiskNZ
tim@risknz.org.nz

It's been a busy couple of months for the RiskNZ Board and a number of members who have volunteered their time to assist with progressing a number of projects, some of which are mentioned below. There is a very rewarding level of energy evident in the organisation and this is proving very beneficial as we strive to deliver added value to our members. The Board's practice of devolving some portfolio responsibilities to 'ministers outside cabinet' has seen a measurable increase in capacity and capability, with the number of programmes and services being developed or delivered concurrently exceeding that of previous years.

Conference 2016

Having explored a range of options your Board has now resolved that there should again be a RiskNZ conference in 2016. Exactly how the conference will be delivered is the subject of some further exploration, including discussions with kindred organisations to see if a joint conference of some description is feasible. The Board will determine in August the specific dates and Wellington venue for Conference 2016 to ensure members have plenty of advanced notice for planning and budgeting purposes. Thanks to Sally Pulley, Loata Stewart and Rachel Allan for their quick work in recent weeks to present the Board with a number of reports and costings to underpin key decisions.

Update: October 13 2015 Development Seminars

The inaugural RiskNZ practioners' development day is rapidly taking shape, with arrangements confirmed for concurrent seminars to be delivered in Wellington, Christchurch and Auckland, linked via the internet so that 3 keynote addresses are shared by all in real-time. The overarching theme for the day is 'The National Risk Profile', and each of the three venues has its own specific focus. The intention is that the October 13 seminars set the scene and lead in to Conference 2016.

- Wellington (Whakarewa Function Centre) – Whole of Government Approaches to Risk Management
- Christchurch (Christchurch City Council Civic Centre) – Applied Learnings from Major Risk Events
- Auckland (Beca Auditorium) – The External Face of Risk Management

We have been successful in already securing the support of several notable speakers including the Assistant Auditor General, Christchurch Mayor Lianne Dalziel and the project leader for the Government's soon to be rolled out PSR (Protective Security Requirements) Strategy. The number and quality of presentations proposed by members is also very satisfying – the challenge now is to accommodate and align many of these to the three streams.

Online registrations are now open. Go to the RiskNZ website
http://www.risknz.org.nz/newevents/risknz-2015-risk-management-development-day/

Continuing Professional Development

The Board has put some definition around what an initial RiskNZ CPD framework will look like and we are now gearing up for two major pieces of work:

1. A review of potential CPD resources available from kindred organisations and searching out other options and determining what work is required to contextualise these resources and make them NZ fit for purpose.
2. A procurement model for obtaining registrations of interest from potential training providers.

As a first step we are inviting members to offer their volunteer services to sit on a CPD Resource Development task group led by Nigel Toms to 1) identify and review potential CPD resources, then 2) input to a process of making these resources NZ fit for purpose. If you are interested in being involved in this pivotal project please contact Nigel Toms nigel@risknz.org.nz and copy in Tim Jago tim@risknz.org.nz

(Note: to avoid any actual or perceived conflict of interest any person or organisation intending to register as a potential CPD training provider will not be considered for the CPD Resource Development Task Group)

Constitution Review

The Board recently agreed the terms of reference for the task group that will be reviewing the RiskNZ constitution. The Government has now released its proposal for a new Incorporated Societies Act and this gives us a clear steer on those additional elements that will need to be inserted to our constitution, as well as those elements that will require amending and updating. I will be communicating with the task group members very shortly with a view to convening a teleconference.

The IRM UK

The IRM have been extremely helpful to RiskNZ over the past year as we have explored avenues for enhancing the value proposition we present to members. I will again be meeting with them in London in mid-September (bringing me back to reality after 10 days of exploring the French canal systems) where the focus of our discussions will be on CPD collaboration, and gaining insights to the risk issues considered most important by our contemporaries in other jurisdictions – information we will use to help shape Conference 2016.

A Note from the Secretary

Ross Wells

Secretary, RiskNZ
ross@risknz.org.nz

The 15th Annual General Meeting of the Society took place on Wednesday 20 May 2015 at 5.30 pm by audio conference between venues in Auckland, Wellington, and Christchurch.

With 25 Members present for the meeting, of whom 22 were Voting Members (Individual or named Corporate Members), the quorum of 15 Voting Members was met. Apologies from 34 Members were recorded.

After the 2014-15 AGM Minutes were discussed and agreed, the Chair introduced the Annual Report for 2014-15, and the Treasurer spoke to the Audited Financial Accounts. A number of long-standing energetic and valued Board Members had stood down at the end of their terms, including Adrian Sparrow, Anne Walker and Rebecca Moody, and the report acknowledged their contributions. Members asked some detailed questions of the Chair, and also expressed appreciation of the improvements to the web site and the Annual Report.

Discussion moved on to the Annual Business Plan and Budget for 2015-16, with more detailed questioning of the plans, the budget and the proposed fees level. One change noted in the Business Plan was the Board's conscious effort to engage members in the delivery of the business plan in areas where previously Board members were allocated roles. Miles Crawford is now the RiskPost Editor, Anne Walker, although off the Board, leads on the Surveys portfolio, and a number of the portfolio teams include members from outside the Board. This trend will continue with initiatives to engage Members in organising the Conference 2016 and the one-Day Seminar series in October.

Members were keen to question the Treasurer on the financial standing of the Society moving forward, and were pleased to hear that the auditors had given an unqualified opinion on the previous year's accounts, that the operational deficit did not in his view pose a risk to the organisation, and that the net asset position was strong. The meeting agreed the fees level for the 2015-16 financial year. The formal part of the AGM concluded at 7:15 pm.

The Board has subsequently agreed the interim Minutes of the AGM, which will come back to the 2016 AGM for finalisation. The interim Minutes have been posted on the website and can be viewed through this link: http://www.risknz.org.nz/members1/agm/

On a personal note, I was struck by the differences between the last three AGMs. Whereas the 2013 AGM had challenged the Board to display some urgency and step up the profile of the Society, the 2014 meeting been full of intense debate, focusing not so much on the future direction the Board had identified, but on the proposals on how to move quickly in that direction. My impression was that the 2015 AGM showed greater unity of purpose between the Board and Members, with continuing challenge on details and tactics, but considerable agreement on the strategic direction for RiskNZ, and on the 2015-16 business plan to maintain momentum.

Assessing your cyber risk profile: the business case for cyber assessments and their organisational benefits.

Tom Walton,

Sales and Marketing Director for Network Box Australasia

Tom is a passionate communicator and cyber-security specialist on a mission to assist New Zealand businesses better understand and manage their cyber risk. Currently, Tom is the Sales and Marketing Director for Network Box, a Managed Security Services Provider who protect New Zealand and Australian business from both inbound internet based threats and outbound data leakage, loss or theft. Having recently presented to the New Zealand Risk Society on cyber governance best practice, Tom has been asked to further the discussion regarding an organisation's next steps to reduce their cyber-security business risk.

Is your organisation doing all it can to protect itself from cyber-attack?

If your answer to this question is "yes", great! But how do you know?

If your answer is "no" or "I don't know", how do you establish which aspects of your organisation require review to identify vulnerabilities and strengthen your defences?

Potentially the worst response to this question is "I'll just wait for a cyber-attack to happen and see if my organisation is affected".

It goes without saying that your organisation has already been subject to a cyber-attack of some degree.

If your organisation is connected in any way to the internet, then it is vulnerable to cyber-attack. With internet based technologies developing at a rapid speed and cyber-attacks constantly evolving and increasing in sophistication, the cyber business risk does not stay idle but changes significantly over time. As such, an organisation must continuously assess its business risk from cyber threats.

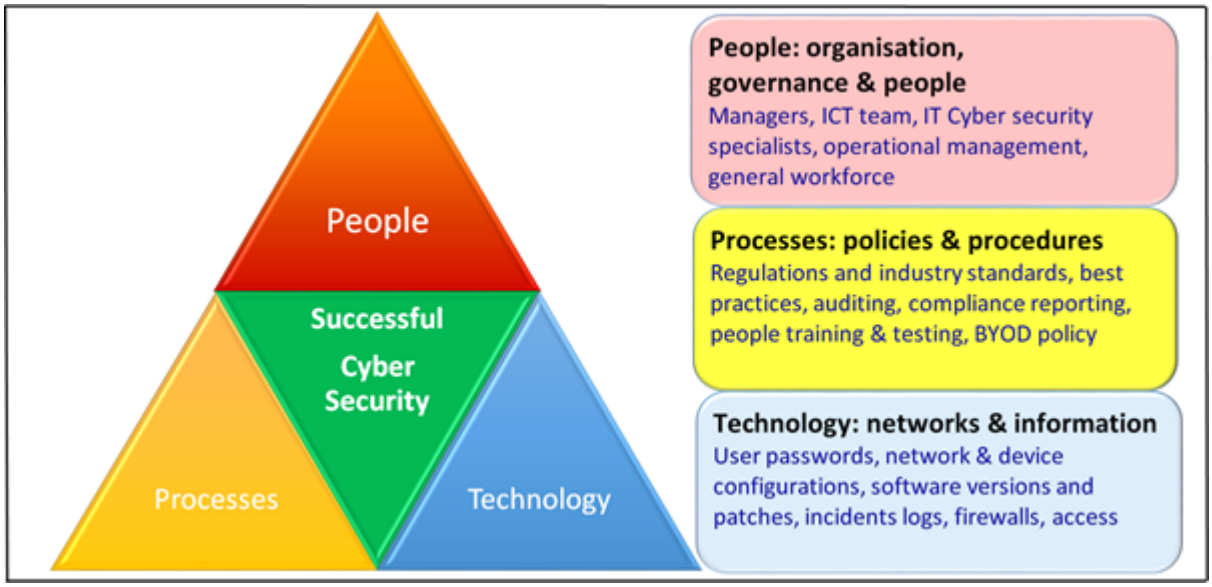
More and more often stakeholders (board members, customers, the media and regulators) are demanding evidence of organisation-wide cyber risk management. An organisation must do everything within its power to reduce the risk of a cyber breach and keep private and sensitive data secure.

An independent cyber assessment provides peace of mind to executives and board members, and will appease stakeholders that your organisation is in the best position to manage cyber-security incidents. Any weaknesses in your defences will be identified and prioritised, providing clear direction for strengthening your cyber-security management. From here, action can be taken to mitigate any weaknesses and reduce the risk of cyber-security incidents.

Following an assessment, many organisations find they have indeed fallen victim to a successful cyber breach, of which they were blissfully unaware.

It is not enough in today's constantly evolving cyber threat landscape to rely on technology to prevent cyber-attacks. A more holistic and organisational wide view is required to ensure adequate protection across the plethora of attack surfaces that exist today. The speed of technological advances and the rate at which these are being adopted by businesses expose increasing vulnerabilities. To stay ahead

of, or even keep up with cyber risk, your organisation must continuously assess its cyber risk strategy and cyber incident management plans. To ensure you are adequately addressing the issue, people, processes and technology aspects should be considered.



The organisational costs of responding to and recovering from a cyber breach include both the immediate IT and operational costs and the more long-term costs to business reputation and profitability. These far exceed the costs of assessing your current situation and taking action to reduce your cyber risk.

Understanding your current cyber risk profile is the first step towards increasing your cyber defences.

When you can understand your cyber strengths and weaknesses you are in the best position to identify areas for improvement, greatly reducing your cyber-security risk.

Many organisations get caught up in simply trying to prevent a cyber breach from happening. Unfortunately, this is not enough to successfully manage cyber-security incidents. A more holistic approach is called for.

Many frameworks exist for assessing your organisation's cyber risk profile. It is important to remember, however, to look beyond your organisation's technologies and consider the people and processes involved, regardless of the framework you use.

A useful standard assessment framework is the NIST Cyber Framework. The National Institute of Standards and Technology has set out five capabilities; identify, protect, detect, respond and recover. This strategic approach assesses an organisation's maturity in terms of their ability to plan for and manage cyber-security incidents. It is important to consider and assess the effectiveness of an organisation's people, processes and technology across each of these capabilities. This approach provides a comprehensive view of an organisation's preparedness to managing cyber incidents.

But what do these capabilities cover and how do they relate to your organisation?

Identify:
Develop an understanding of how to manage cyber-security risks to your organisation's systems, assets, data and capabilities. Identify your organisation's critical business assets, the crown jewels as it were, which could include intellectual property, trade secrets and critical systems. From here

identify the possible risks to these assets from a cyber-security view point, and the organisation's risk appetite if these were compromised.

Protect:
Controls and safeguards are necessary to protect critical business infrastructure services from cyber-security threats. This includes the ability of an organisation to deter, limit or contain a cyber-security incident. Although technology plays a large part within this capability, it should not be the sole focus. Account must be taken of policies regarding the access to and handling of data, and information security awareness and training.

Detect:
Continuous monitoring to identify the occurrence of a cyber-security incident. This capability should provide proactive and real-time monitoring and alerts of cyber-security related events. This ensures timely discovery of cyber-security incidents to be able to mitigate accordingly. If you are not comfortable you have the skills, expertise and time to consistently monitor your IT networks and keep up-to-date with cyber threats, partner with people who can do it on your behalf.

Respond:
The activities required to take action to minimise and contain the impact of a detected cyber-security incident. This capability includes response planning and the analysis of events. It is important this capability includes communication plans for affected stakeholders including board members and shareholders, customers, the media, and regulatory bodies.

Recover:
Business continuity plans to maintain resilience and restore capabilities or services following a cyber breach. This capability must support timely recovery to normal business operations in order to reduce the impact of a cyber-security incident. From here an organisation will have the ability to suggest future improvements to cyber incident management plans.

It is important to address organisational capabilities across each of these concurrent and continuous functions. The effectiveness of all five of these functions is required to provide comprehensive planning and management of your cyber risk profile.

The majority of investment should aim to be in the first three functions of this framework, since responding to and recovering from a cyber breach is far more costly than preventing it from happening. It is crucial, however, to have in place cyber management plans for the response to, and recovery from, successful cyber-security incidents. Put simply; focus on prevention but plan for everything.

The outcomes of a cyber assessment.

Completing a high-level cyber assessment, such as the NIST framework explained above, provides an organisation the ability to:

- describe their current cyber-security posture
- describe their target state for cyber-security
- identify and prioritise any gaps in the current and target cyber-security postures.

Once the opportunities for improvement are identified and prioritised an organisation is then able to assess and measure its progress towards its targeted state of cyber-security maturity. Completing an assessment provides an organisation the information necessary to communicate to stakeholders on the cybersecurity risk facing the organisation and the measures it should be taking to address the risk.

Understanding where your strengths and weaknesses lie in terms of your cyber-security management will help focus and prioritise your cyber risk strategy.

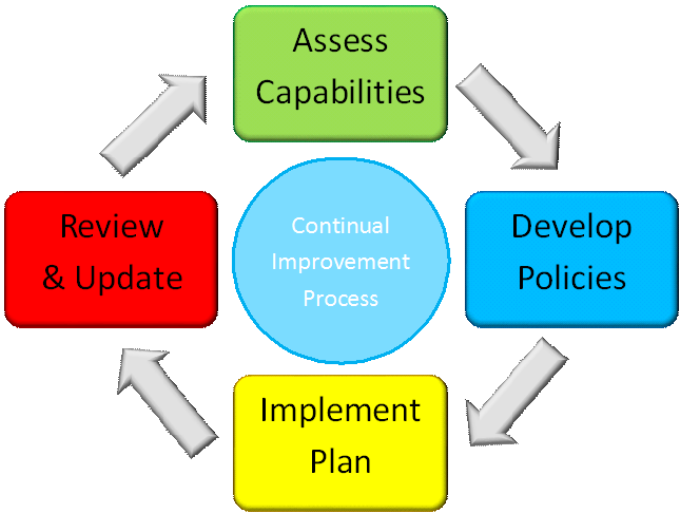
Assessing your cyber risk profile is only the first step in managing your cyber risk. The government led initiative, Connect Smart, details a four step process:

Assess your capabilities using an assessment framework such as the NIST Cyber Framework. As mentioned previously, this should review your organisation's people, processes and technology. It is important that this review is as objective as possible in order to present an impartial view of the level of preparedness to manage a cyber-security incident. It may be necessary to outsource the assessment to a third party in order to receive a truly objective review.

Develop policies to address any gaps identified in your cyber-security profile. Following an assessment it is crucial not to delay in taking remediate action if required.

Implement an action plan to put into place cyber governance policies. The capabilities identify, protect and detect focus on prevention and this is a good place to begin in the short term. Prevention is far more cost-effective than responding to and recovering from a cyber breach, however, it is crucial to still plan for everything.

Review and update your organisation's capabilities and cyber governance policies and management plans. The cyber threat landscape is dynamic and increasingly challenging. Continuous review ensures proactive rather than reactive behaviour, improving your organisation's security posture, business continuity and business assurance.



The sooner you can take action to prepare your critical business functions from cyber-attack, the greater protection your business operations and reputation will have.

Book Review: Antifragile - Nassim Nicholas Taleb

Miles Crawford

Principal Consultant, Code Red Consulting

CODE RED CONSULTING
Risk, Business Continuity, Crisis & Emergency Management

Miles has worked in risk, business continuity, and emergency management for over 12 years, in both the private and public sectors, in New Zealand and overseas. Miles' strengths lie in the way he approaches the community or organisation he's working for; with an open and approachable manner, in a clear, understandable way, and through developing measures that are realistic, fit for purpose, and owned at the right level. Along with running his business providing advice on risk, business continuity, emergency and crisis management, Miles is completing a PhD focussing on disaster risk management, and also tries to handle a young and rapidly growing family.

In *Antifragile*, Nassim Nicholas Taleb introduces the concept of antifragility, which he defines as the opposite of fragile. You might think that 'resilient' or 'robust' is the opposite of fragile but according to Taleb that's not right. A system is fragile if it is sensitive to errors. A system is resilient if it is insensitive to errors. A system is antifragile if it improves with errors.

I was keen to read *Antifragile* because I knew it was a sequel or logical follow-on to Taleb's book *The Black Swan*. In *The Black Swan*, Taleb argues that despite human beings' taste for rational patterns of cause and effect, it's impossible to predict the occurrence of large, improbable and highly consequential events like World War I or the rise of the Internet. Taleb defines these occurrences as black swan events. *Antifragile* is Taleb's attempt at telling us how to deal with black swan events. He states that black swan events are increasing, "as a result of complexity, interdependence between parts, globalisation and the beastly thing called 'efficiency' that makes people now sail too close to the wind." What we can do is locate the fragility in the system and reduce it. "Not seeing a tsunami or an economic event coming is excusable," he writes; "building something fragile to them is not."

I was also keen to tuck into more of the narrative style Taleb introduced in *The Black Swan*. I liked the cheek with which Taleb took shots at authority, cloistered academics and bureaucracy. I thought his anecdotes were novel, well-illustrated, and insightful. And while the essayistic approach Taleb employed made heavy reading, it was clear-cut.

However, it seems Taleb has used his success with *The Black Swan* as licence to spiral way off the radar. Along with scornfully dismissing all with which he disagrees, such as those in the "phony professions" of journalism and academia, we find out that Taleb hates TV, soccer mums, air-conditioning, Thomas Friedman, sissies, and most economists. And while this could have been seen in his earlier books as comical rough handling of his favourite targets, the tone has now deviated into a sort of dictatorial bullying. And if it isn't bullying, it's a full blown ego-rant: Taleb refers to his amazing, wonderful travels, all the cafe's he has been in around the world, how he can dead lift 330 pounds, about being an "an intellectual who has the appearance of a bodyguard", and being the only person to truly understand the ancient philosopher Seneca's work.

This boasting would be excusable, even amusing if it all made sense, but the book suffers from a kind of attention-deficit disorder, jumping from subject to subject, continually looping back on itself, and full of contradictions. Everything is taken to link to everything else but Taleb scatters his ideas through the

book indiscriminately, he offers predictions about the future, though he keeps talking about the unreliability of predictions, he despises mere 'theorists' but still aspires to produce a theory of everything. I was left feeling that too many of his ideas came across as weak and inflexible, fragile rather than antifragile.

So, would I recommend reading *Antifragile*? - Yes.

You might think this strange considering how critical I have been so far, and you would be right. But every now and then Taleb does get around to illustrating antifragile strategies that offer up some provocative titbits that encourage us to think differently. He argues that "less is more": that, instead of introducing "thousands of pages of regulation" to institutions, we should instead be adopting basic anti-fragile principles and concepts. Such concepts are:

- The 'barbell technique' where Taleb states that it is better to run slightly behind the pack most of the time by devoting a small but significant portion of your resources to outliers. If one of them hits, the rewards will more than make up for the lower return that you had been receiving to date. This avoidance of the middle ground would avoid the "risk of total ruin" in putting 100 percent into 'medium' risk securities.
- 'Skin in the game' – an expression coined by Warren Buffett to refer to a situation where executives use their own resources to buy stock in the company they're administering. Such involved interest leads to greater levels of executive responsibility for the viability and success for ventures they control.
- 'Optionality', where if you do not know what will happen; make sure you have every option covered. Antifragile takes the idea of optionality from finance and broadens it out into a universal quantity. From engineering to medicine, to career development to politics, Taleb sees optionality everywhere.

All in all, this is a book that should be approached with caution – but it still should be approached. The book is difficult to follow, and Taleb seems to have divorced himself from the real world, blithely expecting us to ride along with him on his antisocial mystery tour. However his concepts are interesting, they build on his previous work, and continue to add perspective to how we deal with 'uncertainty'.

So go on, give *Antifragility a* crack.

Revisiting the Use of Predicate Logic in the Construction of Risk Statements

Barnaby Pace

Risk Manager, Hamilton City Council

One of the most important aspects of any risk assessment is the risk itself and how it is presented. What is required is a clear and simple communication, but in a manner which provides enough information to assure an accurate portrayal. This can be accomplished with a well formulated risk statement. The purposes of this paper expand on an earlier article (Pace, 2013) to explore the contraction of logical sound risk statements for both positive and negative risks. What is considered here is the logical aspect of the argument identifying the risk. While the factual questions within the argument are of considerable significance they are outside the logical construct of the argument and require input from subject matter experts in addition to the knowledge of the risk analyst.

Firstly, consideration needs to be given to how the risk statement structure was formulated in the earlier article. Robertson (2010) provided a list of rules for the communication of risk statement which were repackaged (Pace, 2013) into a series of four guidelines, as below:

1. Written as a complete sentence, consisting of cause and effect
2. Link the clauses with phrases such as “resulting in”; “causing”; “leading to”
3. State the cause as an event of set of conditions
4. State the effect upon the programme goal, objective, or value under examination

Taking the aforementioned rules into consideration, together with the concepts of cause and effect modelling (Johnson-Laird & Goldvarg-Steingold, 2007) the following statement was devised (Pace, 2013):

“As a result of **<definite cause>**, **<uncertain event>** may occur, which would lead to **<effect on objective(s)>**.”

“As a result of **the implementation of new software, unexpected integrations errors** may occur, which would lead to **spending more time and resources than originally planned for**.”

This statement can be rewritten in the form of a compound proposition so it can be examined in terms of its logical construction.

“If **<definite cause>** and **<uncertain event>** then **<effect on objective(s)>**”

“If **new software is implemented** and **unexpected integration errors occur** then **more time and resources will be needed.**”

This is a revision on the original article which suggested that the **<definite cause>** would lead to the **<uncertain event>**, which is not always the case. In some instances the **<uncertain event>** occurs independently of the **<definite cause>**, suggesting the lack of predictability within the situation thus reflecting the true nature of the risk.

In terms of presenting the risk statement as an argument the following premise-conclusion structure can be taken:

<definite cause>	(Premise)
<uncertain event>	(Premise)
If **<definite cause>** and **<uncertain event>** then **<effect on objective(s)>**	(Premise)
<effect on objective(s)>	(Conclusion)

New software is implemented.	(Premise)
Unexpected integration error occurs.	(Premise)
If **new software is implemented** and **unexpected integration errors occurs** then **more time and resources will be needed.**	(Premise)
More time and resources will be needed.	(Conclusion)

In order to critic the statement structure from a logical perspective it needs to be represented in a manner which allows an examination to take place whilst avoiding the restriction found in the nuances of the English language. To achieve this, the formal language structure (which is a set of symbols that may be constrained by rules) of propositional logic can be utilised.

1. C	(Premise)
2. E	(Premise)
3. (C & E) ⊃ O	(Premise)
4. ∴ O	(Conclusion)

In this instance only the knowledge of three of the propositional logic operators is required (&, ⊃, ∴). The ampersand (&) is the logical operator represented by a conjunction. In the case of propositional logic, in order for the premise to be true both the left hand expression (in this case 'C') and the right hand expression ('E') need to be true. The second symbol (⊃), the Horseshoe, is the 'implies' or 'then' operator. In this instance in order for ('O') to be true, both ('C') and ('E') need to be true. This leaves the final operator, therefore (∴). This operator implicates the outcome or conclusion of the above premises within the argument.

Within this revised structure allowance can be given for one or more **<definite cause>** and/or **<uncertain event>** as it is often the case that multiple factors/variables need to be taken into consideration with a causal chain. For example,

"If **<definite cause>** and **<uncertain event 1>** or **<uncertain event 2>** then **<effect on objective(s)>**"

The propositional logic representation of this would be:

1. C	(Premise)
2. E	(Premise)
3. C & (E ∨ F) ⊃ O	(Premise)
4. ∴ O	(Conclusion)

In this case a new propositional logic operator is present, the 'or' operation symbolised by a descending wedge (∨). In this instance either ('E') or ('F') need to be true, and ('C') needs to be true in order to imply that ('O') is true.

Positive Risk

In simple terms, positive risk is achieved when opportunities are realised through taking the risk, in which the benefits are greater than want would have resulted from not taking it. Thus, the organisation/individual has received an overall benefit from undertaking the activities that resulted in exposure to the risk or set of risks. By expanding on the work of Robertson (2010) and maintain a similar structure to that used above the following statement structure has been devised.

"If **<definite cause>** is undertaken, **<uncertain event>** maybe realised, leading to **<opportunity>** occurring."

"If **during the project process any opportunities for improvements are identified that can be immediately** undertaken, **the resulting improvements** maybe realised, leading to **continuous improvement during project develop time** occurring."

As with the previous example this statement can be rewritten in the form of a compound proposition so it can be examined in terms of its logical construction.

"If **<definite cause>** and **<uncertain event>** then **<opportunity>**"

"If **during the project process any opportunities for improvements are identified that can be immediately** and **these improvements are untaken** then **continuous improvement during project develop time will occurring**."

In terms of presenting the risk statement as an argument the following premise-conclusion structure can be taken:

<definite cause>	(Premise)
<uncertain event>	(Premise)
If **<definite cause>** and **<uncertain event>** then **<opportunity>**	(Premise)
<opportunity>	(Conclusion)

Opportunities for improvements are identified.	(Premise)
Improvements are untaken.	(Premise)
If **opportunities for improvements are identified** and **improvements are undertaken** then **continuous improvement will occur.**	(Premise)
Continuous improvement will occur.	(Conclusion)

As with the former example in order to critic the statement structure from a logical perspective it needs to be rewritten used the formal language of propositional logic. The structure of which in this example is identify to the first propositional logic argument given.

1. C (Premise)
2. E (Premise)

3. (C & E) ⊃ P (Premise)
4. ∴ P (Conclusion)

Predicate Logic

In all the above cases, although the logic may look sound there is room for improvement. The extent of propositional logic syntax provided into its predicate logic counterpart allows of the additional of further operators which better reflect how the logical arguments given would appear in the 'real world'. This is achieved principally through the use of existential qualifier (∃x). The existential qualifier can be interpreted as 'there exist', 'there is at least one' or 'for some'. In other words the statement will not hold true in all case. So, if we rewrite the compound proposition form the first example we would get:

"In some cases If **<definite cause>** and **<uncertain event>** then **<effect on objective(s)>**"

Or in the formal language structure:

$$(\exists x)\ (C \ \&\ E) \supset O$$

The use of the existential qualifier allows for the uncertainty within the risk statement to be reflected. It is never the case that the chain of events is known; if this was the case then by its very nature the risk is non-existent as no uncertainties exist. Now that uncertainty is reflected within the logical structure the original risk statement structure is more accurately reflected.

"As a result of **<definite cause>**, **<uncertain event>** may occur, which would lead to **<effect on objective(s)>**."

The same holds true for positive risk statements:

"In some cases If **<definite cause>** is undertaken, **<uncertain event>** maybe realised, leading to **<opportunity>** occurring."

Or:

$$(\exists x)\ (C \ \&\ E) \supset P$$

Conclusion

The purpose of this paper has been to illustrate the value of a well formed risk statement within the risk assessment and management process. If the risk is not clearly articulated there is a very real possibility that the controls and mitigations put in place will not be addressing the correct areas, making the exercise redundant. Additionally, having worked through the statement structure logically provides an additional level of assurance that the method is scientifically sound and robust.

References:

Johnson-Laird, P. N., & Goldvarg-Steingold, E. (2007). *Models of cause and effect.* In W. Schaeken, A. Vandierendonck, W. Schroyens, and G. d'ydewalle (Eds.). The mental models of reasoning: Refinements and extensions, pp. 167-189. Lawrence Erlbaum Associates: London.

Pace, B. (2013). The logical construction of a robust risk statement. *The Journal of the New Zealand Society for Risk Management, 13,* (4), 8-9.

Robertson, E. (2010). How to do risk assessment – risk statements. Retrieved from http://riskcommentary.com/tag/risk-statement-example/

Standard and handbooks update

Roger Estall

Roger was the first Chairman of the Society and represents it on the trans-Tasman joint standards committee for risk management known as OB-007. He also represents New Zealand on ISO Technical Committee TC 262 which is responsible for ISO risk management standards. He was one of the authors of ISO 31000 and has been a principal author of many related SNZ/SA standards and handbooks

They say that a week can be a long time in politics but on ISO's committee for risk management standards, just one sleep can see things turned on their head. And so it was last Friday night.

As I explained in the last edition, at the end of a 5 day meeting of the Working Group (WG) of ISO's TC 262 Technical Committee in Paris in March, it was decided to abandon 18 months of work developing a 'Limited Revision' of ISO 31000.

Having ditched the Limited Revision, the WG decided to start on the process of an unlimited revision and established a Task Group, led by a WG member from Ireland with strong project management experience, to develop a 'Design Specification' for the revision.

Until I went to bed last Friday night, I thought that I would be able to share with you the Purpose Statement (which not surprisingly had much to do with decision-making and uncertainty) and to be able to outline, the main thrust of the Draft Statement (DS) and an associated Explanatory Note (which has still to have some minor fine tuning completed).

That optimism reflected the plan (on Friday night) that within a couple of weeks it would be sent to all National Standards Bodies for a 3 month review period with the opportunity for comment. But alas, when I woke on Saturday morning, that plan (which, together with the general timetable had been agreed in Paris) seemed to have come unhinged so we are now in a wait and see period.

Hopefully all of this will be resolved soon so that everyone will get to see the DS and be able to have a good deep think about the document (referred to in the DS as 31000:20XX) which once drafted and finalised (after the usual consultation) will essentially pave the way for dealing with uncertainty in decision-making (as has the existing standard) for 8-10 years from its publication.

The Task Group (TG) is very keen that compared with the existing standard, 31000:20XX will be easier to understand, have fewer defined expressions and less jargon, offer improved technical advice, be easier to apply, and will be much more closely linked to what actually happens in organisations (as distinct from the more introspective focus of the existing standard on 'risk management' per se). That said, I would be surprised that any organisation that has actually become very proficient at applying the existing standard in their organisation would see their world suddenly upended by the new document. The biggest case for revision is that there are still many organisations that are still struggling to optimise the way they take account of uncertainty in relation to their objectives as they make their day to day decisions.

At stages during the development of the DS, the TG sought structured feedback from the larger membership of the WG and one particular comment stayed in my mind. "*The main objectives of an organisation is not to effectively manage risk, nor to have effective controls, but to ensure it makes the best decisions in order to achieve its objectives."* I anticipate that 31000:20XX will respond to that clarion call and I hope soon to be able to outline the Design Specification to RiskPost readers.

Invitation

I will shortly be asking Standards NZ (which on the ISO committees, I represent) to appoint a further delegate because the work load (even without the nonsense) is getting rather high and besides, it would be mean of me not to share these special experiences!

If anyone would be interested and would like to know more about what is involved, please contact me. The core skills that are needed (additional to a touch of madness) are:

- Subject matter expertise
- Experience of operating in committees – especially where the line of debate can change very rapidly and advocacy of even good ideas, although in English are not necessarily the Queen's or President's English and thus creative listening and careful expression are very important.
- Willingness to learn and master the rules (known as the ISO Directives) under which committees operate (or are meant to)
- Writing and drafting skills
- Advocacy
- Ability to travel (SNZ is not in a position to fund travel)

Please see contact details below.

Any member wishing to send Roger suggestions relating to any of the work of ISO 262 or OB-007 is welcome to do so at roger_estall@yahoo.com.au

RiskNZ news and information

Management Board and Officers

The management board and officers of RiskNZ are:

Chair: Geraint Bermingham **Secretary:** Ross Wells

Executive Officer: Tim Jago **Treasurer:** Tony Yuile

Administration Officer: Rachel Allan

Committee members: Nigel Toms, Brian Potter, Loata Stewart, Hilary Walton, Sally Pulley, Sue-Anne Lee, Sharyn Bramwell

---

RiskNZ's Website

RiskNZ's website is located at www.risknz.org.nz.

As part of this year's business plan initiatives, our website has been upgraded. Although we have made every endeavour to ensure all aspects of the website are functioning as they should, if you do notice any broken links or other gremlins, please notify the Administration Officer at adminofficer@risknz.org.nz.

The website is your RiskNZ's shop window, and a major risk management information resource, so please take the opportunity to browse the new site. We welcome your feedback on it.

As a financial member of RiskNZ you are entitled to access the members-only section of the website. For this you need a user name and a password. If for any reason you do not have the password or have forgotten it, please contact the Administration Officer.

New Members

RiskNZ welcomes the following new Members. Contact details are included in the Members' section of the Website.

Individual Members

Jack Milford, Risk and Personal Safety Consultant, OPSEC Solutions Ltd

Paul Leslie Floyd, Director, Algerian Operations and Maintenance Company

Brendan Norrie, Business Systems Manager, YHA New Zealand Ltd

Sarah Thompson, General Manager, Shared Services, Chartered Accountants Australian and New Zealand

---

Become a Member

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/membership/how-to-join/

Social networking – Follow us on

LinkedIn https://nz.linkedin.com/groups/RiskNZ-3945531/about

Find us on Facebook http://www.facebook.com/pages/The-New-Zealand-Society-for-Risk-Management/178021535579772

twitter http://twitter.com/nzrisksociety

Information for Contributors

Next Issue	The next edition will be published in September 2015. RiskNZ strongly encourages all members to contribute items for this newsletter on practices, developments or issues in your particular area of risk management. Contributions for the next issue should be sent to editor@risknz.org.nz and received by 31 August 2015. Members are welcome to submit material for the following sections:
Articles	Articles are welcome at any time; please contact editor@risknz.org.nz if you wish to propose an article.
Developments in risk management and new information sources	Significant new web page content including online articles and major reports available on the web. New publications (including brief descriptions, and where possible website links to further information). This will include new journals in risk management, new books, where they are available, etc.
Activities, services and situations vacant	*RiskPost* provides a membership service for the display of notices and advertisements, if aligned with RiskNZ's objectives. Notices may describe an activity or service, or advertise a risk management vacancy. Notices must not exceed 150 words of plain text, inclusive of all contact and reference details..

For further details on RiskNZ's submissions and advertising, please contact the Administration Officer: adminofficer@risknz.org.nz,

RiskNZ,
PO Box 5890,
Wellington 6145

Links

This section in RiskPost provides our members with useful links to websites and LinkedIn discussion sites. These links hold a lot of information that our members should find useful to enhance their knowledge in Risk Management and related areas. We welcome comment from our members on the usefulness of these links and suggestions for others sites they found useful. Please send feedback or links to editor@risknz.org.nz

Consumer Affairs – Product Safety
http://www.consumeraffairs.govt.nz/for-business/compliance/product-safety

ISO 10377:2013 Consumer Product Safety — Guidelines for suppliers and ISO 10393:2013 Consumer product recall – Guidelines for suppliers.
http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1726

Internet sites:

http://globalriskcommunity.com/

http://www.valuebasedmanagement.net/

http://www.knowledgeleader.com/

http://poole.ncsu.edu/erm/

Groups within LinkedIn:

ComplianceX
http://www.linkedin.com/groups?gid=865117

Conference Board of Canada ERM
http://www.linkedin.com/groups?gid=2561072

Enterprise Risk Management
http://www.linkedin.com/groups/Enterprise-Risk-Management-82279?trk=myg_ugrp_ovr

Enterprise Risk Management Association
http://www.linkedin.com/groups?gid=89308&trk=myg_ugrp_ovr

Governance Risk & Compliance
http://www.linkedin.com/groups?gid=95089&trk=myg_ugrp_ovr

ISO 31000 – Risk Management
http://www.linkedin.com/groups/ISO-31000-Risk-Management-1958423?trk=myg_ugrp_ovr

ISO 31000 Risk Management Standard
http://www.linkedin.com/groups/ISO-31000-Risk-Management-Standard-1834592?trk=myg_ugrp_ovr

Research & Benchmarking Risk Appetite Practices
http://www.linkedin.com/groups/Research-Benchmarking-Risk-Appetite-Practices-2401677?trk=myg_ugrp_ovr

Risk Managers

http://www.linkedin.com/groups/Risk-Managers-65207?trk=myg_ugrp_ovr