RISK NZ

RISKPOST

ONLINE READING - THIS YEAR IS DIFFERENT

SUE TREZISE – *Sue-lutions Ltd*

Looking beyond the Top 10 and doing the 'Pivot'

By this time any other year I would be providing a summary of reports such as the Allianz Risk Barometer or the AON Global Risk Survey, using the insights to benchmark risk activities and awareness in the New Zealand context.

2020 is one out of the box (as they say) with the COVID-19 pandemic creating a completely different context for risk practitioners, given the depth and breadth of unknowns and the velocity with which change has happened.

What's different this time?

It is as if the Top 10 risks have all been realised in the same event, rather than as independent developments as might normally be anticipated. It's the earthquake risk (low likelihood, high consequence risk) realised in all places at once – no one and no place is unaffected. It's a collection of threats that has become a super-issue situation: mass business closures; supply chain breakdown; loss of resources through lockdown or quarantine; a substantial decline or significant increase in customers depending on the face-to-face or online presence; sudden change in business regulations/requirements (eg social distancing constraints in work and retail space); and the malevolent presence of IT cyber attacks, security breaches and internet failures.

From the same setting, new thinking has been triggered. For example, opportunities created by the acceleration of telework (increased use of virtual meetings, confidence in online productivity), working from home flexibility, sharing of strategies for coping with isolation (cooking, exercise and mindfulness videos), and big wins for those industries well positioned to respond to demand for online products and services.

Where to from here?

The context for the future is wide open and looking towards the horizon shows an unfamiliar landscape. Organisations and managers may be tempted to retreat from the uncertainty and seek to avoid risk – despite such impossibility! Now is the time for risk practitioners to champion the contribution (value-add) of risk to business success. Risk management is about understanding all of the things that need to go right for an enterprise to be successful, as much as assessing and quantifying all the things that could go wrong. The ability to adapt to change has always been a fundamental survival mechanism, it is the speed of change in an uncertain and changing environment which requires an equally rapid responsiveness.

Continued on next page…

Doing the 'pivot'

Many businesses and organisations will "pivot" in adapting to changing circumstances - radically transforming themselves because their previous strategies and plans are no longer appropriate/relevant/actionable (take your pick). The associated, and rapid, disruption of operating models, redefining of how products and services are delivered, rebuilding of customer and stakeholder relationships, are examples of where pivoting and adaptation will be essential for survival.

Some relevant insights can be gained from a study co-authored by Paul Tracey of Cambridge Judge Business School which focused on the prevalence and pitfalls of pivoting for new ventures. While not necessarily embarking in a truly entrepreneurial way, for many organisations the pivot required in COVID-19 times has similar concerns. A key approach is creating a bond with 'user communities' by shared experience of the difficult transition journey, to rebuild their connection with the organisation's products/services/values. The study noted that while entrepreneurs (or businesses) can rebuild relationships with customers and suppliers, there is a flip side – that building these kinds of relationship creates a sense of obligation and a sense of expectation for continued engagement. As needs change or new opportunities for the business are discovered, further pivoting will continue. Applying a risk-lens will minimise the chance of a poorly planned or managed pivot alienating those relied-on supporters.

In her Icehouse webinar, Melissa Wragge presented the following Pivoting Tips and Traps

1. **Being adaptable is your biggest asset.** Things are changing daily so stay open and move where the market is.
2. You might think you need clarity first when actually **you get clarity from the doing**. Test and learn.
3. You can **move quickly in short sharp sprints**.
4. **Before you go on the journey, it's really important to know where you stand.**
5. **Once you've mapped your future model, you need to circle back and think about how you protect essential assets in the transition,** and how you **eliminate the non-essential** as quickly as possible. From a governance perspective, you want to **ensure the decisions made now are consistent with the future model you're creating.** And be prepared to review those decisions as the landscape changes.

To paraphrase a Darwinian quote "It is not the most intellectual or the strongest of the species that survives; but the species that is able best to adapt and adjust to the changing environment in which it finds itself." The unexpected will always happen and progress is dependent on solving problems that were not anticipated. COVID-19 events and lessons learned need to be embraced as opportunities to pivot and adapt so businesses and organisations not only survive but flourish.

Cyber crime in a pandemic environment

Cyber incidents remain the #1 business risk according to the Allianz Risk Barometer 2020. The annual survey (responses by 2,718 risk experts in 102 countries, across 22 industry sectors) predates Covid-19 chaos, however its relevance should not be overlooked.

While we are focused on the multiple and more obvious impacts of the global shutdown – business closures, home isolation, staff layoffs, remote working, social distancing requirements, etc – it is a timely reminder to maintain vigilance for the less visible risk of IT failure/outages and cyber crime in particular.

While we are focused on the multiple and more obvious impacts of the global shutdown – business closures, home isolation, staff layoffs, remote working, social distancing requirements, etc – it is a timely reminder to maintain vigilance for the less visible risk of IT failure/outages and cyber crime in particular.

Organised criminals seize on topical issues like Covid-19 to lure people to bogus websites with malware on them or harvesting credit cards through fake charity donation pages. Organisations can be more vulnerable in times of crisis if staff are distracted by the urgency of response work from watchfulness for phishing emails (for example). Working from home also increases the likelihood of clicking malware through into business systems as people operate in a more relaxed 'office' environment which crosses into their personal space.

Continued on next page…

Some close to home examples of cyber incidents include:

- IT system attacks on freight company Toll Group. In the most recent of two incidents already this year, Toll had its IT system attacked and a ransom demanded by hackers. The system had to be shutdown (and customers notified) and was offline for 36 hours leaving staff to process bookings manually and using the external gmail accounts to communicate. Toll has a clear policy of not paying any ransom. https://www.newsroom.co.nz/2020/05/05/1158942/freight-firm-toll-struck-again-by-cyber-threat
- A news report of computer issues at meat processing company AFFCO described a disruption to supply deliveries of meat for at least three nights in a row and interruption to its ordering system. Staff were also reported to have had their pay affected. The company did not contribute to the article[1]. https://www.newsroom.co.nz/2020/05/05/1157253/affco-meat-supply-affected-by-it-issue
- From across the Tasman - A sophisticated form of malware was detected in an email sent to the Western Australian Premier's office by the Indonesian Embassy in Canberra. It is claimed hackers infiltrated the computer of a diplomat, found a draft email, completed it and concealed the malware within an attached document before sending it. The malware involved was designed to give the hacker administrative access, basically near total control over their victim's computer system with access to copy, delete or create files, carry out extensive searches of the device's data, and send emails on behalf (ie allow a hacker to digitally impersonate their victim). https://www.nytimes.com/2020/05/07/world/asia/china-hacking-military-aria.html

The impact of COVID-19 has increased our already high dependence on technology and with it the magnitude of the threat posed by cyber crime. While money is at the heart of some if not most cyber crime, collateral damage includes further business interruption/failure/loss through system shutdowns, operational rework, IP/data theft, reputation damage, loss of business custom and customers.

Cyber crime is not an 'earthquake' risk (the standard low likelihood, high consequence risk), it is an 'elephant' risk (the risk no-one wants to mention). The increasing likelihood of high to extreme consequence at any level (local, global, all sectors) makes this a red flag topic for risk practitioners to continually raise. We have seen how bad it can be with a contagious people virus, where might a computer virus take us?

---

[1] It is noted that this is not uncommon, with companies attacked in this way being typically quiet about it. The Government's Computer Emergency Response Team (CERT) to whom such incidents are generally referred also respects the sensitive nature of any reports and does not confirm or deny involvement.

SUE TREZISE

Sue Trezise has over 12 years experience providing risk expertise and advice for government and organisations on strategic, enterprise and operational risk management. An experienced facilitator, Sue assists communication between technical experts and non-technical stakeholders and makes managing risk practical and effective.

SUE LUTIONS Ltd
An independent and practical approach

REFERENCES

The Art of the Pivot: *How New Ventures Manage Identification Relationships with Stakeholders as they Change Direction* Sources: https://insight.jbs.cam.ac.uk/2019/pivoting-successfully/ and https://journals.aom.org/doi/10.5465/amj.2017.0460

Icehouse Webinar:

Source: https://info.theicehouse.co.nz/webinars

This article first appeared in RiskPost Edition 1 2020, and has been republished with the permission of the author. To read other articles from this RiskPost edition please click here and you'll be taken to the members area of RiskNZ. website.