Special Report

Risk reimagined

Sponsored by KPMG

www.afr.com | Wednesday 23 October 2019

Humans are still vital in the data loop

Value Machines lack the intuition people bring to analysis.

James Dunn

The confluence of data and technology is a paradox for the modern organisation, opening up new sources of risk.

The terms “technology risk”, “cyber risk” and “data risk” are all here to stay on any organisation’s list of risks it faces, and must be bedded down in its risk culture – but data and technology also give the organisation’s risk function unprecedented ability to review, assess, monitor and manage risk.

The positive side of this paradox is that technology has enabled organisations to automate aspects of their governance and risk management.

Speaking at the recent Risk Reimagined roundtable in Sydney, co-hosted by *The Australian Financial Review* and KPMG, Kevin Smout said organisations were starting to understand the ability of the risk function to add value to the business, to enable them to make smarter business decisions, and to contribute to sustainable business growth.

However, he said there were big discussions to be had about the “quality of the data and what is the governance framework around it.”

The role of the risk function had changed in the last two decades as it had become driven by technology, said Mr Smout, who is KPMG’s global lead, governance, risk & assurance and risk strategy & technology partner.

“The risk function can start to be seen as value-adding, because it is taking in all the data on the external and environmental factors, and can help (management and the front-line) see how those trends might impact both the current strategy, as well as its traditional role of risk mitigation.”

Fellow roundtable participant Robb Eadie, BHP’s global chief risk officer, said 20 years ago the role of the risk function “revolved around stopping bad things happening”.

Now the risk function is “all about making good things happen”, and that is primarily enabled by technology.

The risk function has changed recently as it has become driven by technology, says KPMG’s Kevin Smout. PHOTO: JEREMY PIPER

The role of technology in risk has also been greatly empowered by the realisation that risk resides at all levels of an organisation, and is not just handled centrally by a risk function, according to Jason Smith, board director at the Risk Management Institute of Australasia.

“Risk management has to be embedded not only in operational performance, but business planning and performance management, and really every function. Technology is accelerating this process.” If one looked at organisations’ operational risk, said Mr Smith said there was “huge opportunity” to use digital tools.

“That is certainly an area where businesses can start to collect and collate and understand their operational data better, to understand the relationships between the operational data and the key risk indicators, and allow AI and machine learning to start to discern the trends and the relationships between them,” he said. “Historically, risk managers have tended to rely on what the historical loss events have been, and doing scenario analysis, and it’s actually been very subjective and very backward-looking.

“Technology is now allowing organisations to be a bit more objective and predictive around what’s happening with the operational risk profile of the organisation.”

As we see automated technologies advancing, the human element becomes more important.
Zoe Willis, KPMG

But, Mr Smout said, a wonderful kitbag of tech tools did not guarantee great insights.

“A tech solution doesn’t fix an inherent problem that an organisation has, culturally, with its attitude to, and appetite for, risk. You can have the best governance, risk and compliance (GRC) platform or system, for example, but if you don’t have the right people, processes, and quality of input data, you can’t use it,” he added.

“The value in such a platform comes when you start to get the business actually inputting the data into it, owning it, and keeping it up to date. Otherwise, the platform is viewed as not having worked, it gets written off.

“But if it is ‘owned’ by the business, that’s where you get the value in good risk management.”

Mr Smith agreed and said, “Often, it’s not so much that the system doesn’t work, it’s that the system doesn’t give the organisation the value it should.”To a large extent, the insights still come from humans – as do the risks.

“The biggest risk you have in any organisation is the human being, because as an entity we are quite error-prone in comparison with the alternative, with the alternative being algorithmic machine-based data analysis,” Mr Eadie said.

“But on the other hand, the one thing that human beings are exceptionally good at is that element of insight – that intuitive interpretation of data. The factual algorithmic interpretation of data is very useful, but sometimes it can miss the subtle nuances that will be seen by people who have many years of experience, and in-depth knowledge and insight into specific areas,” he said.

This factor is “the human in the loop,” said Zoe Willis, KPMG Partner Data and RegTech. “As we see automated technologies advancing, the human element becomes more important. The ‘human in the loop’ is what actually provides the context.”

And this is the paradox of technology and data, says Anne O’Driscoll, non-executive director at Steadfast Group.

“The business processes themselves are being increasingly automated, and the risk processes and access to data and tools to interpret that data are increasingly prevalent,” she said.

“The challenge is ensuring that you have people on the frontline and people in the risk function that have the experience,” Ms O’Driscoll said. “Ultimately, will people have the experience to say, ‘Just because the machine says that, it still doesn’t look right to me, based on my experience? That’s my concern.”

Data-led strategies hit a snag

Innovation gain Ethical questions and fairness are often forgotten.

James Dunn

Insurance companies can use data to tailor premiums, says Steadfast Group's Anne O'Driscoll. PHOTO: JEREMY PIPER

While tools such as artificial intelligence and machine learning have given businesses an unprecedented ability to segment their data to the individual level, they are posing increasingly deep ethical questions for organisations.

Businesses are now able to find out much more about their users and customers than in the past.

In theory, this allows them to personalise the marketing and pricing of products and services – allowing more competitive pricing, and happier, more engaged customers who feel they are being considered as individuals. It's win-win.

But there is plenty of downside in this data-led business revolution, as new risks emerge.

"We have situations such as banks being much better able to understand the propensity to default and charging differently, and insurers knowing how much you use your car, for example, and tailoring the premium," said Anne O'Driscoll, non-executive director at Steadfast Group.

At the recent Risk Reimagined roundtable held in Sydney, she said: "On the one hand, your consumer, who's very digital, says, 'You are my banker, you are my insurer, and I expect you to know a lot about me because I've transacted with you for years. You have all this data about me and I expect you to charge me an insurance premium that relates to my individual risk.'

"But when, for example, we actually know things that make their insurance premium more expensive, they're less accepting."

Insurance as an industry has always worked hard to properly assess risk, and to investigate claims, but the data revolution creates some grey areas.

One is the problem of unintentional discrimination – the insurer's artificial intelligence (AI) algorithms might judge someone as being a higher or lower insurance risk because they belong to a particular demographic group, driven by factors such as age, sex, income or ethnicity.

"As companies know more and more about that, if things get inaccessible for the poorer risks, is that fair, is that the appropriate use of data?" asked Ms O'Driscoll.

If we're keeping the social licence front of mind, we can focus on the benefits.
Zoe Willis, KPMG

Social media's role is also being assessed. Its data can improve risk assessment in the insurance industry and improve fraud-detection capabilities. Insurers can look at customers' social media activities and compare them with their claim records, looking for differences. Banks use social media in much the same way.

"Using social media as an indicator on somebody's risk or their propensity to default is a very grey area," said Zoe Willis, KPMG partner Data and RegTech.

"Should you use social media analytics, or the data that people post about themselves online, to drive that? There are a lot of very deep conversations being had on that."

Potential discrimination and data privacy are emerging risks in many industries. Retail, for example, has come under scrutiny for the use of facial tracking technology, which can capture the faces of shoppers and cross-reference biometric data potentially to identify known shoplifters, with the ability – in a "smart", or interconnected shopping centre – to alert tenants as the tracked person moves around the mall. The abilities that technology can give businesses can often "over-excite" them, said Scott Guse, partner audit, assurance and risk consulting at KPMG.

"That is a situation where the technology's wonderful, and it has great application for stopping leakage in a retail business, so the retailers love it, but those ethical elements are very difficult," he said.

"If people get too excited about the technology and its capability, you could argue that they can lose sight of the bigger ethical picture."

The use of data, and of any technology, should always be considered in terms of the social licence to do so, said Ms Willis.

For example, facial recognition technology could be used to spot vulnerable people that may need help as well as people likely to commit a crime.

"Where we can, I think we have to focus on the positives that can come from the use of this technology, as well as the negatives. If we're keeping the social licence front of mind, we can keep the focus on the benefits to society as a whole."

Surveillance is a "particular minefield" for the insurance industry, said Ms O'Driscoll. "The justification for surveillance is the extent to which people actually try to defraud insurance (companies), and fraudulent claims drive up the cost of insurance for everyone.

"But on the other hand, the industry better understands ... the interaction of injury, and claims for injury, with mental health. So instead of the focus of surveillance being on potential fraud, the industry is changing that to a focus on the fact that, where possible, people will be better off getting back to work."

According to Jason Smith, director at the Risk Management Institute of Australasia, it ultimately comes back to the human element.

"Whatever technology you're using, for whatever role, you need to maintain human oversight," he said.

"You need to have governance in place that ensures that the data that you're collecting is actually fit for purpose, and you need to make sure that you've got absolute transparency."

Hackers make a beeline for the internet

Jonathan Porter

The internet of things, the network of embedded software in devices of common use, has increased the amount of risk we are exposed to. Every business in Australia is at risk – as long as it's connected to the internet.

Worldwide, the number of internet-connected items will grow from 14.2 billion to 25 billion by 2021, according to research heavyweight Gartner.

Professor Jill Slay, La Trobe University's Optus chair of cyber security, says these low-power devices are often inadequately protected and make a tempting target for hackers.

"Every user, whether home or business, who uses a device connected to the internet is at risk," says Professor Slay, who is also director of the Optus La Trobe Cyber Security Research Hub.

"Especially where a hacker can manage to infect many of the same type of device and create a botnet – or use the collective power of large numbers of devices together.

"The devices at risk include webcams, any kind of home monitoring device. We have heard of attacks on cow trackers (they wear them to monitor the amount of milk given)."

Other larger devices Professor Slay says are at risk include small internet-of-things (IoT) devices such as connected security systems, cars, light bulbs, alarm clocks, speaker systems, vending machines and coffee pots.

"There are huge unknown and unmitigated risks produced by the massive uptake in IoT devices. If they are not secured downstream, the risk is unacceptable," she says.

"Australian businesses need to first be aware of and find out which devices are connected to the internet, and find out which devices, if any, have any kind of built-in security."

The rewards for getting the security right make the expense and effort worthwhile, Professor Slay says.

"It means they will be able to use IoT devices for competitive advantage, to use sensors and gather big data, for positive digital disruption and flexibility for their business."

Foolproof solutions are yet to emerge, she says. "As yet there is no consensus on how to secure IoT devices, and no comprehensive solutions have appeared to date.

"We see large-scale acceleration of the use of IoT sensors, more excitement about their use, some development of security standards, but no obvious engagement with potential disruption."

Hybrid wars will be won without a fight

Cyber conflict The strategy is to exploit weakness on the quiet.

Mark Eggleton

AustCyber's Michelle Price: cyber is being weaponised. PHOTO: PETER BRAIG

The term "hybrid war" has been around since the former US Secretary of Defense General James Mattis and Lieutenant Colonel Frank Hoffman used the term back in 2005.

In a paper titled *Future Warfare: The Rise of Hybrid Wars,* Mattis and Hoffman outlined a major component of future wars would involve "psychological or information operations aspects", and this would be melded with more conventional methods.

Interestingly, it was first alluded to in 1991 when the US National Research Council warned of our over-reliance on computers and their inherent vulnerability in a report titled *Computers at Risk: Safe Computing in the Information Age.*

As for the relevance of hybrid war to business – one of its key tenets is a focus on economic entities. It's often referred to as "grey" or "cool" war, where action is deliberately kept below the threshold that would spark a major war by using non-military means to achieve warlike aims. Put bluntly: to undermine a nation's business entities and its wider economy.

The most obvious example of hybrid war in recent years has been the Russian government's attempts to influence the 2016 US presidential election, although other powers are also quickly moving into the field. China acknowledged its value in 1999 by advocating targeting areas such as a reliance on technology and respect for the rule of law in democratic countries.

A recent paper by the Australian Strategic Policy Institute's Dr Samantha Hoffman, titled *Engineering global consent: The Chinese Communist Party's data-driven power expansion,* outlines the extent the Chinese government's tech-enhanced surveillance is expanding globally.

In the report, Dr Hoffman says China's efforts don't revolve around obvious technology such as surveillance cameras in countries outside China, but through useful technologies such as 5G and, potentially, smartphones.

She says these "services are designed to bring efficiency to everyday governance and convenience to everyday life".

"The problem is that it's not only the customer deploying these technologies – notably those associated with 'smart cities', such as 'internet of things' (IoT) devices – that derives benefit from their use. Whoever has the opportunity to access the data a product generates and collects can derive value from the data. How the data is processed, and then used, depends on the intent of the actor processing it," she says in her report.

The report cites Global Tone Communications Technology Co. (GTCOM) as a case study to illustrate how the global expansion of the party's tech-enhanced authoritarianism can work.

GTCOM is a subsidiary of a Chinese state-owned enterprise that the Central Propaganda Department directly supervises. It openly co-operates with the state's intelligence services and strategically co-operates with large Chinese firms such as Huawei and Alibaba Cloud.

According to AustCyber chief executive officer Michelle Price, it would be wise for Australian business to be alert to businesses that have been flagged to have close ties with organisations such as GTCOM.

"There's enough global competition out there that companies going through their procurement processes should be asking more questions around cyber risk," she says.

Ms Price says Australian organisations need to immunise themselves against malicious cyber activity and this will involve getting the right policy settings out of the federal government.

"While there has been lots of investment on the national security side of the coin, more needs to be done on the economic side."

While much nefarious cyber activity is often the work of cybercriminal networks, Ms Price warns we're also seeing more nation states accessing bank details and changing business invoices, for example, in a bid to undermine trust in economies.

Social media giants are among the many culprits

Data breaches

Jonathan Porter

Angelene Falk

The nation's finance and health sectors are ground zero for data breaches, Australia's privacy watchdog has found.

Private health service providers reported 19 per cent of the total breaches reported between April and June under the Office of the Australian Information Commissioner's (OAIC) National Data Breach scheme.

The finance sector was next, with 17 per cent of data breaches for the period, the commission said in its latest report. This was followed by the legal, accounting and management services sector (10 per cent), private education (9 per cent), and retail (6 per cent).

The most common information revealed in the breaches was contact information (90 per cent), financial details (42 per cent), identity information (31 per cent), health information (27 per cent), tax file numbers (16 per cent), and other sensitive information (9 per cent).

Human error was the leading cause of data breaches in the health sector, accounting for 55 per cent of breaches, compared with an average of 35 per cent for all other industries annually.

Personal information sent to the wrong recipient was the most common human error in health, whether by email, mail or other communication.

In the finance sector, human error accounted for 41 per cent of data breaches (higher than the cross-sectoral average of 35 per cent).

As in the health sector, a number of these data breaches were the result of personal information sent to the wrong recipient.

"The fact that there is a human factor involved in so many cases demonstrates the need for staff training to increase awareness of cyber risks and to take the necessary precautions," Information and Privacy Commissioner Angelene Falk said on release of the report.

A commission spokesman said the consistent presence of health and finance at the top of the rankings likely reflected the scale of data holdings and volume of processing activity in those sectors.

Other factors included the "sensitivity of the personal information held by those sectors"."Both industries have also been subject to long-standing information protection obligations (including duties of confidentiality and strict regulatory frameworks) which have likely contributed to their relative maturity and preparedness to meet obligations under the NDB scheme," the spokesman said.

The OAIC said cyber attacks in the finance sector had risen in recent years.

Meanwhile, the Business Council of Australia said its members from all sectors were working together to counter growing cyber security threats.

"Cyber security is critical for business to address the connectivity conundrum: providing consumers connectivity, while building trust and security," chief executive Jennifer Westacott said.

"Business has to do much of the heavy lifting in increasing our cyber resilience. The business community is committed to working together, and with government and research, to share information on threats and co-design a fit for purpose regulatory environment," she said recently.

"By actively working together as well as focusing on maximising the cyber security of our individual companies we can provide the community with greater confidence in the capacity of our economy to stay a step ahead of would-be cyber criminals."

A spokesman for the Financial Services Council said the OAIC report was a sobering reminder of the importance of cyber security.

"Cyber attacks on the nation's largest industry, financial services, carries long-lasting consequences on our financial stability, productivity and overall economy," the spokesman said.

"It's important the financial services sector is equipped with the defences and infrastructure needed to prevent malicious attacks …

"Cyber security should remain bipartisan. Industry and government must work together to ensure the financial burden of preventing future attacks isn't passed down to consumers."

Opportunity rising with threat levels

Change velocity

Businesses face fear of being left behind.

Lydia Maguire

"The opportunity doesn't sleep, but the threat doesn't sleep, either," said Robb Eadie at the recent Risk Reimagined Roundtable, co-hosted by *The Australian Financial Review* and KPMG.

Mr Eadie, global chief risk officer at BHP, said: "Historically, in the risk function, we've taken the view that the pace of opportunity and the pace of threat is at a level that we can manage, nine-to-five, five days a week, 300-and-something days a year.

"The fact is, we can't, because of the current rate of change; and consequently, we need to have some form of response to that rate of change, and one of the ways to do that is through effective data manipulation, management and control," he said.

That "control" cannot be total, however.

"It's in the context of risk, where we control things that either are opportunities and we reduce the risk of hazard, and we increase the opportunity of success," Mr Eadie said.

"Most of the discussion around risk relates to being able to match the pace of change in the world that we see today. As these threats evolve and these negatives evolve, we need to be able to match that pace.

"At the moment, I think in both counts, business is lagging behind both the rate of change of opportunity and the rate of change of threat, and the risk function has a huge part to play in matching those paces, and accelerating to match those paces."

For Mr Eadie, the traditional view of risk is of "multiplying probability and impact of a potential event to get the risk effect: if the benefit is greater than the risk, then you do it, and if the benefit is less than the risk, then you don't.

"That's the traditional view.

"But the more modern view is that the risk function gives the organisation the insight that allows the business to place the right bet.

"You have to take the right risk at the right time, in the right place, in the right way and use data to give you the information that tells you what is the right risk, what is the right place, when is the right time, and what is the right way.

"And you can only do that through data.

"But we've only been existing in the data world for a couple of decades."

Zoe Willis, KPMG partner, data and regtech, said the pace of change is demonstrated by what is now commonplace.

"Five years ago, would we have sat here and talked about using facial recognition, and voice analytics? No, but they're now very relevant," Ms Willis said.

"Will it be different in five years? Absolutely.

"As professionals, we always need to think about how do we disrupt ourselves, because we need to be anticipating that change."

Kevin Smout, KPMG global lead, risk strategy & technology and global lead, governance, risk and assurance, said the firm is experiencing this itself.

Its risk hub product takes in all of the operational data of a business, data on the external environment and factors that affect the business, and uses augmented reality to create a 3D picture of the organisation's risk profile in order to get a better idea of how to contain and manage it as sweeping changes in the external environment exert mounting pressure.

"With that 3D picture, you can actually grab hold of a risk as a bubble and squeeze it to make it smaller, or expand it to make it big, and watch that contagion flow," he said.

"It's taken us six months to have a prototype operating, and with the pace of change in technology and the rate of change, I could see within six months that that will be a market for us.

"And in two years, it will be common for people in boardrooms to be having discussions based on the risk hub: for example, a mining client might say, 'We're actually focusing on a different mineral now. What does that do to our environment from a risk and opportunity perspective?'"

BHP chief risk officer Robb Eadie says businesses now have the insight to place the right bet. PHOTO: JEREMY PIPER

KPMG Australia's Zoe Willis says we need to anticipate change. PHOTO: JEREMY PIPER

While models are "only as good as what you put in," Mr Smout sees the risk hub as a decision-making tool.

"It's a way to take the external signals, from an industry perspective and the market, and combine it with the organisation's own data, and blend them into a live model that informs the experienced executives around the table, and on which they can make decisions."

The point, he said, is to get directors, front-line, risk and investment all on the same page, and "enrich the dialogue" around risk.

And this is where risk management in an organisation should be, at the heart of the strategic direction, according to Jason Smith, board director at the Risk Management Institute of Australasia.

"I actually think the most successful risk functions don't use the word 'risk' – they talk about the opportunity as what really matters, and then, from a risk appetite perspective, is 'what is our willingness to lose in this particular strategy'.

"When you change that lexicon and change that thinking – along with harnessing the technologies – that's when risk can really start to offer value," Mr Smith concluded.