NEW WORLD DISORDER
ADVANCED RISK CONFERENCE
10–11 OCTOBER 2017

Advanced Risk Conference

NEW WORLD DISORDER

AON
Empower Results®

Contents:


NEW WORLD DISORDER
Mental Health
Micro/Macro economic risks
Wanna Cry, Dark Web, Cyber Crime
Bad Risk Culture
Geopolitical Risk
Multinational Risk
Litigation Funders
D&O exposures
Sharing Economy
AI/ Autonomous Vehicle

Executive Summary

Lambros Lambrou

The 2017 Aon Advanced Risk Conference (ARC) held in Melbourne in October built on last year's conference theme of the 'Risk Revolution' and delved deeper into global uncertainty to explore the New World Disorder. We live in an era of unprecedented volatility. Slow economic growth, changing demographics, rising geopolitical tensions, populist economics and rapid changes in technology are all converging to add complexity to traditional risks.

Now, more than ever, businesses have to face a number of new risks that simply add to the challenge of trying to survive in the most competitive business climate anyone has experienced. Businesses require the insight, tools and solutions necessary to succeed in understanding new risks and learn how they can mitigate, control or transfer them.

Lambros Lambrou, CEO Australia, Aon Risk Solutions

Top ten Risks

1. Damage to reputation/brand
2. Economic slowdown/ slow recovery
3. Increasing competition
4. Regulatory/ legislative changes
5. Cyber crime/ hacking/viruses/ malicious codes
6. Failure to innovate/ meet customer needs
7. Failure to attract or retain top talent
8. Business interruption
9. Political risk/ uncertainties
10. Third-party liability (incl. E&O)

Source: Aon 2017 Global Risk Management Survey

Executive Summary

Is uncertainty the new norm?

The global Economic Policy Uncertainty (EPU) index has tracked 'uncertainty' on a global basis over the past 20 years, which is based on several sources of information including over 12,000 newspaper articles that discuss policy-related economic uncertainty. The recent revolution of populism, nationalism and protectionism has seen 'uncertainty' reach an all-time high, demonstrating that it may well be the new norm (see fig. 1).

Scenario planning is critical to navigating an uncertain future

The new world disorder presents both peril and prosperity. On the one hand are the challenges of stagnant wages growth and our reliance on a strong Chinese economy, while on the other are massive opportunities from Asian growth and digital transformation. Navigating these uncertainties becomes a lot easier once you understand the scenarios and then recognise the possibilities.

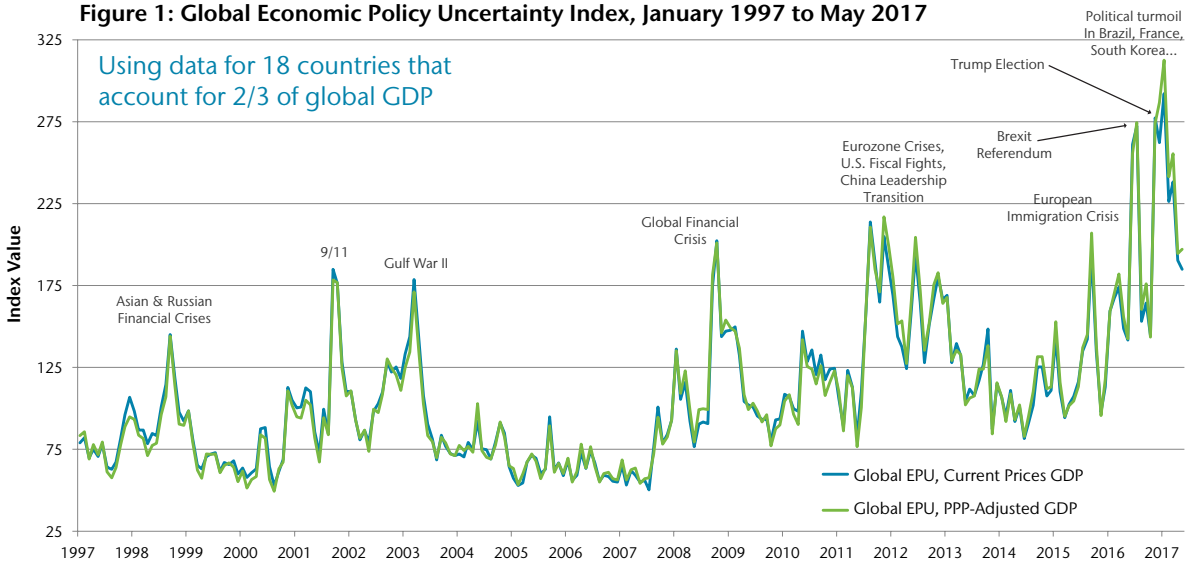
Cybercrime is a risk for everyone

The cyber threat landscape has changed dramatically over the last four years. Cybercrime is now the number one economic crime in Australia, according to PwC. The sophistication and resources of cybercriminals means attacks are more common, more successful, and more damaging than ever before. Cybersecurity Ventures has estimated losses from cybercrime could rise to US$6 trillion by 2020. With most organisations taking at least 201 days to learn they have been penetrated, the need to quantify and transfer cyber risk is essential.

Creating the appropriate risk culture is critical

Risk culture is the human element of risk management, which is somewhat obvious, but often overlooked. Risk culture describes what happens in an organisation when no one is watching. The stronger the risk culture, the less worrisome the unobserved behaviours should be.

Figure 1: Global Economic Policy Uncertainty Index, January 1997 to May 2017



Notes: Global EPU calculated as the GDP-weighted average of monthly EPU index values for US, Canada, Brazil, Chile, UK, Germany, Italy, Spain, France, Netherlands, Russia, India, China, South Korea, Japan, Ireland, Sweden, and Australia, using GDP data from the IMF's World Economic Outlook Database. National EPU index values are from www.PolicyUncertainty.com and Baker, Bloom and Davis (2016). Each national EPU Index is renormalized to a mean of 100 from 1997 to 2015 before calculating the Global EPU Index.

Source: Economic Policy Uncertainty

Effective risk culture is more than just risk mitigation; it will move the needle and drive higher business performance. A recent study by Aon found that organisations that align their culture with their business strategy have four times higher sales and earnings growth compared to companies with low cultural alignment. Speaking on the ARC 2017 panel, Michael Vainauskas from Perpetual outlined that establishing a strong risk culture starts from the top, and is enacted through risk champions who spread the message that risk is something which is owned by everyone, and included on each employee's scorecard.

A diverse business is no barrier to effective risk management

Hong Kong-based Swire Pacific, a publicly listed company with a diverse portfolio spanning property, transport, beverages and other interests across Asia and America, is recognised for its high standard of risk management and corporate governance. But despite the risks it faces from regional economics, regulatory changes, cyber threats and more, Swire Pacific maintains high risk maturity through a consistent framework that accommodates regional differences.

Navigating the D&O storm

With $1.7 billion in securities class action settlements likely to take place in 2017, protecting directors and officers is becoming a minefield for insurers and clients alike. And it will only become more complicated, thanks to changing regulations, the rise of litigation funders, and the increasing prominence of cyber-related liabilities. Insurers are becoming more aware of aggregated risk and reading the fine print and open dialogue are more important than ever.

A strong risk culture also means protecting minds

Reducing risk in the workplace means not just protecting the bodies of employees, but also their minds. With one in five Australians aged from 16 to 85 likely to experience a common mental illness in any given year, poor mental health costs Australian businesses $10.9 billion every year, says PwC. An integrated approach to mental health must be based on support, prevention and promotion. Both organisational and individual factors must be considered when thinking about the mental health of employees. Coca-Cola Amatil led the way, embarking on a journey to improve mental health that incorporates an evidence-based programs to create a workspace that is compassionate and effective in identifying and delivering early intervention.

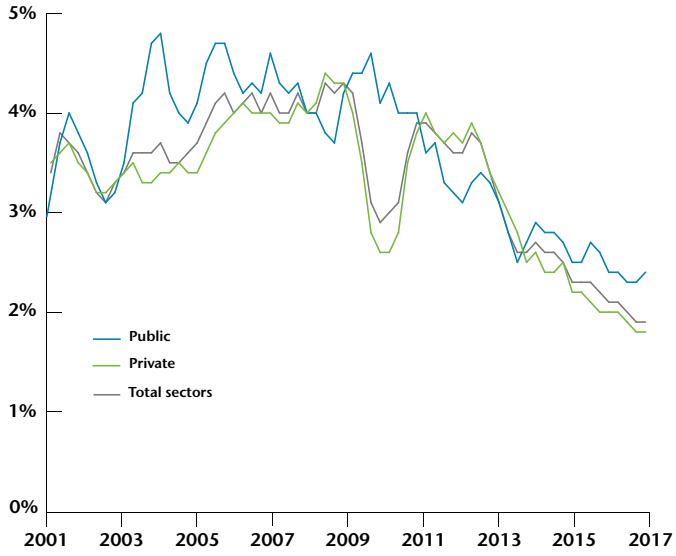
New World Disorder – Micro and Macro Implications for Australia

Australia has enjoyed more than two decades of economic growth, the global economy has recovered from the GFC, and Australia's largest trading partner, China, is on its way to becoming the world's largest economy sometime in the 2030s.

Overall, the outlook for Australia is positive. But there is no guarantee it will stay that way.

Speaking in the opening session of Aon's ARC 2017, Deloitte Access Economics senior advisor Professor Ian Harper described a disjunction between what we might normally expect to see during an economic recovery, and what we are seeing now. While the Australian economy and employment figures have grown, wages have not (see fig. 2). Prof Harper explained how low wages growth leads to low inflation, and hence to low interest rates. And with the market forecasting low interest rates out beyond 2020, that indicates little expectation of wages growth – a situation the world has not experienced before.

Figure 2: Australia Wage Price Index



Source: ABS

The result, as Prof Harper described, is that a population can lose faith in its leadership if economic growth does not accrue evenly, and this might be driving the rise of populist movements in Europe and the US. Meanwhile the jobs being created during the upswing cannot generally be filled by the people who are currently losing theirs, leading to further social imbalance.

Prof Harper also explained how the Australian economy has transitioned from the mining investment boom without entering a recession, as some predicted, thanks to a pick-up in non-mining investment. But the real star has been the services sector (see fig. 3). Prof Harper said Victoria for instance had no mining sector to speak of, but was reporting net migration and employment growth because of the growth in its services economy.

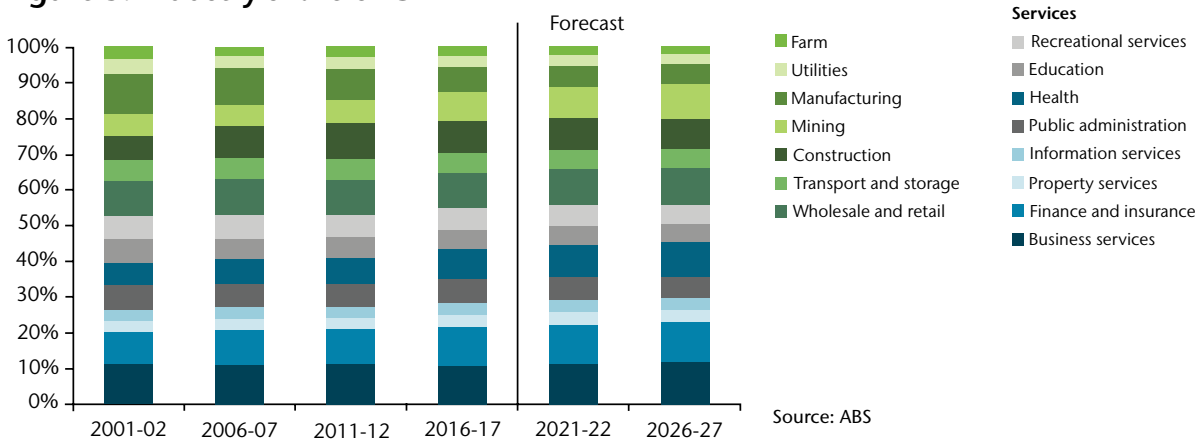
But whether Australia can stay strong depends greatly on the global economy, and specifically China, with Prof Harper describing three possible scenarios for Australia. The first flowed from a hypothetical sharp slowdown in the Chinese economy, which would quickly translate to massive reductions in income and growth, along with decreases in employment, profit, and overall wealth. Such a scenario would decrease sales by 8% and wipe $140 billion off earnings, with the loss of 500,000 jobs. Thankfully, while Prof Harper described this scenario as high impact, he also rated it as being low in probability.

A more likely scenario was that growth across Asia would see our nearest neighbours increasing demand for the services that underpin Australia's economy. This scenario would see Australia earn an extra $650 billion over the next 20 years, with employment rising by 1.6% and a boost to inbound tourism of 5.6% thanks to the growing Asian middle class. However, he cautioned that even in such an optimistic scenario there could be losers, as changes to the exchange rate could decrease manufacturing employment by 3%.

The final scenario asked the question what might happen if Australian organisations fully embraced the opportunity presented by digital transformation. Rather than running from the apparent cyber threat, Prof Harper suggested that seizing opportunities in digital could boost business investment by 5% and boost jobs by 0.5% in Victoria and NSW. Importantly, wages would grow by 2%.

Hence amidst the new world disorder, there was still some significant benefit to be gained from reducing cyber risk.

Figure 3: Industry share of GDP



Source: ABS

WannaCry, The Dark Web and Cyber Crime – What Does it Mean?

The impact of cybercrime on the global economy is hard to measure exactly, but there is no doubt it is vast and growing.

In 2014, the Washington-based Center for Strategic and International Studies estimated the losses from cybercrime had reached U$445 billion each year. Cybersecurity Ventures has since estimated that will grow to US$6 trillion by 2020.

Speaking on cybercrime, Aon's Senior Vice President for Cyber Solutions Jim Trainor described how the cyber threat landscape had changed dramatically over the last four years.

The pace of change will accelerate, thanks to trends such as the Internet of Things, which will lead to billions of more devices connected to internet over next several years. The more devices connected to the internet, the more opportunity for criminals to ply their trade.

At the same time, organisations are collecting more and more data, presenting more and more opportunities for criminals to steal data and make money.

As a former Assistant Director for the Cyber Division at the FBI, Trainor led several agents, analysts and computer scientists in hunting down cyber criminals. He described how at any given moment there were thousands of computer intrusion cases under investigation at the FBI, with 60% perpetrated by criminal actors and 40% by nation states.

"The pace has changed, the threat environment has changed," he told the audience. "So regardless of the threat environment your organisations has faced previously, it really has very little to do with what you will face in the future."

Trainor encouraged organisations to work with law enforcement rather than go it alone, as the peers of any compromised organisation would likely be desperate to know how an intrusion happened.

"We all are in this together to remediate and reduce the risks we face," he said.

And the risks are spreading. Whereas once those organisations considered at greatest risk would have been those holding personal, health, or credit card information. Now organisational data such as trade secrets, intellectual property and military technology all have value. Data can also be used for extortion purposes, such as when client data is stolen from a law firm, with the threat that data would be disclosed if a ransom is not paid.

Attacks today were generally carried out by five diverse groups: terrorists; hacktivists; insiders; nation states; and criminals. Cybercrime was also highly organised, with different organisations and individuals playing different roles on a service basis.

Regardless of their motivation or origin, Trainor said they all followed Lockheed Martin's Cyber Kill Chain, a seven-stage process of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. That meant a hacker would generally undertake reconnaissance of its target to understand their people and systems, then launch their attack and work their way through the system to find their target. Shockingly, it generally took 201 days for an organisation to learn it had been infected, leaving them plenty of time to do so.

"You can do a lot of damage in 201 days," Trainor said, according to the Ponemon Institute.

All organisations can reduce their threat level by learning what should and shouldn't be on their network, tightening up the network and access privileges, blocking malicious domains and patching old software, and discovering and preventing unknown threats by working with specialist organisations.

With so much complexity to manage, Trainor said insurers were generally underwriting to resiliency. And with every organisation open to suffering an intrusion, the real concern is how an organisation chooses to respond to cyber attack.

Managing Cyber Risk in the Current Business Environment

While the threat of cyber-attacks has been well-publicised, there is still a degree of complacency amongst Australian organisations regarding the investments necessary to insure an adequate defence. But while it is generally agreed that organisations need to spend more, knowing how much to spend can be difficult to determine.

These were key themes of a panel discussion on managing cyber risk held at the conference. Australia's comparatively low level of engagement on cybercrime could be attributed to a 'she'll be right' attitude, coupled with Australian organisations having yet to experience a massive hack on the scale of those experienced in the US by Yahoo, Sony, Equifax or Target.

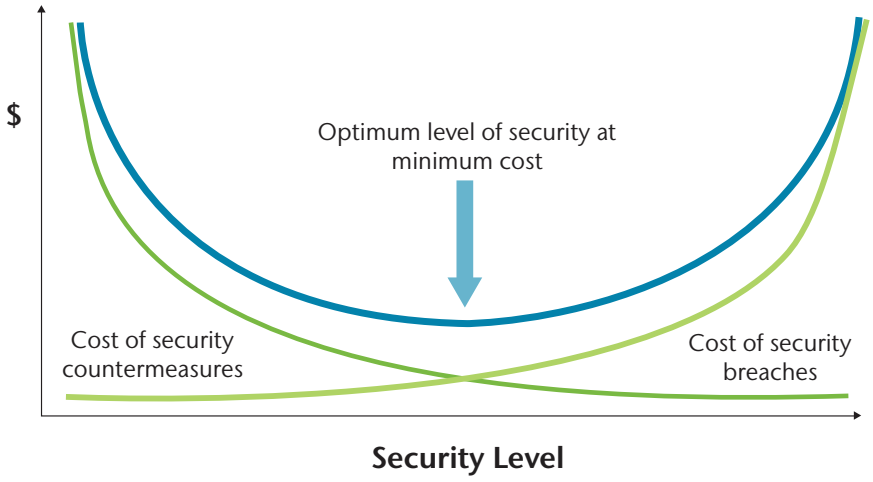
The audience heard how many Australian organisations had been safe in the knowledge that in most instances, even when an attack has been carried out successfully, they were under little obligation to tell anyone. That would change however on 22 February 2018 with the introduction of mandatory data breach notification laws, with fines of up to $1.8 million for failure to notify.

According to Les Bell, a course developer and presenter at the Optus Macquarie University Cyber Security Hub, simply adhering to the Australian Signals Directorate's 'Essential 8' cybersecurity recommendations could do a lot to reduce threat levels and subsequent losses through breaches and interruptions to the business.

But he added that chief information security officers (CISOs) often reach a point where increasing investment yielded diminishing returns without ever achieving perfect security. Hence most would overspend by 30%, which was a safer than underspending (see fig. 4).

Bell added that effective security required a multidisciplinary approach, and for that, the most effective common language revolved around risk management.

Figure 4: A CISO's view of Risk



Cybercrime is now the

NUMBER ONE ECONOMIC CRIME IN AUSTRALIA,

according to PWC.

The new mandatory data breach notification law requires organisations to report the compromise of as little as

ONE DATA RECORD.

Optus' Vice President of Enterprise and Government, David Caspari, described how in addition to Optus being a cybersecurity service provider, as a top 10 brand Optus could not afford to be the next headline. He told the audience how Optus' email servers received 20 million emails each month, of which only 15% were legitimate, with the other 85% being spam or malicious. It only takes one to get through for a breach to occur.

As a telecommunications provider Optus had already been the subject of mandatory reporting, under the existing Privacy Act. Caspari said this meant Optus had become highly sensitive to the risk profile of the devices and actions on its networks. But while new technology was constantly coming onto the market, many of the risks came from legacy technology, which was more expensive to patch and maintain. Hence Optus maintains an extensive risk register of all appliances and applications, and takes a multidisciplinary approach to the issue with more than 1000 people having passed through cyber awareness training.

Fellow panellist and Vice President in ANZ for the US-based networking technology company Cisco, Ken Boal described how his organisation survived its own scare 10 years ago, which led to creation of a cross-functional cyber team. Boal advocated that the CISO role should report outside of the line of IT leadership and be closer to the risk management function. He added that some organisations were now bringing cyber and physical security together under the same principles and leadership.

But to the key question of how an organisation should determine how much it spent on cyber security, Bell described the theory that no organisation should ever spend more than 37% of a value of an asset on securing that asset. But within the CISO community itself, he said the question remained the subject of fierce debate, with a different answer for each organisation.

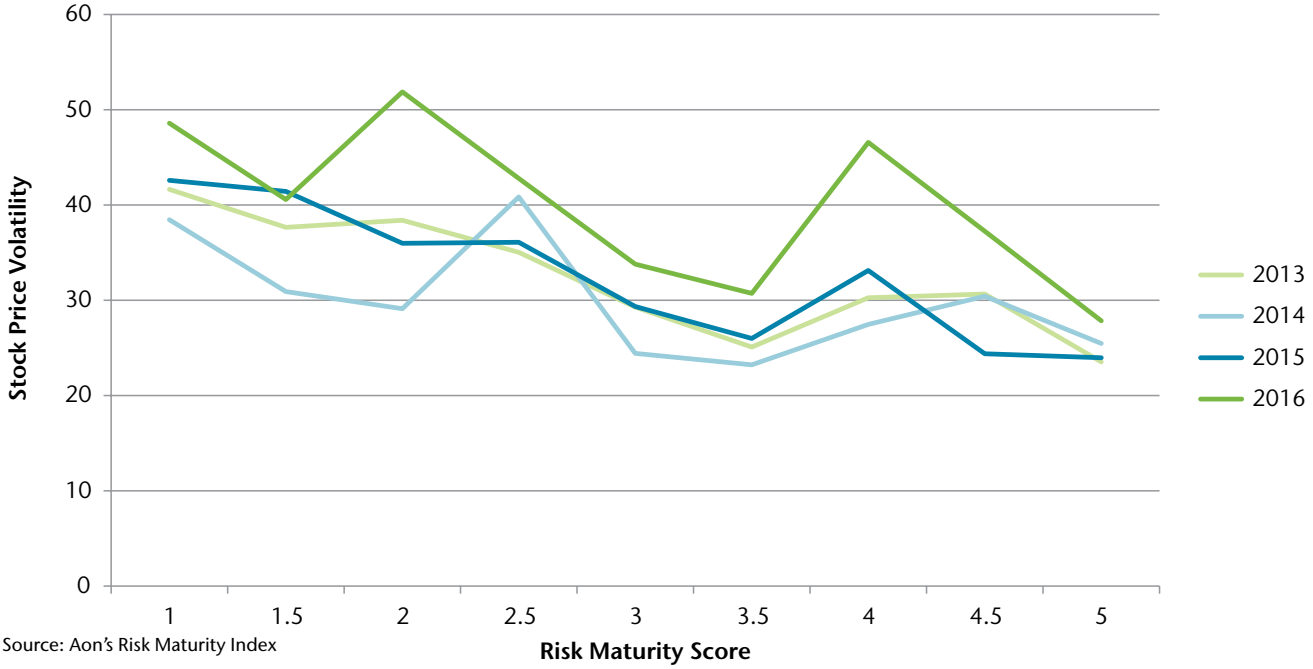
How to Build Effective Risk Culture

The human element is an obvious but often underserved component of risk management. But setting and maintaining an appropriate risk culture can do much to improving an organisation's overall risk maturity.

Risk culture was the key theme of a panel discussion at Aon's ARC 2017, where experts discussed Aon's Risk Maturity Index and the links between risk culture and risk maturity.

Since 2010 more than 1700 organisations across 25 industries have participated in the Risk Maturity Index, with statistically significant correlations have been found between advanced risk maturity and financial performance, share price performance, returns on assets, returns on equity, and even on the pricing of D&O insurance (see fig. 5).

Figure 5: Risk maturity = financial performance



Source: Aon's Risk Maturity Index

Risk culture is a key subset of the Risk Maturity Index, and the Managing Principal for Growth Strategies at Aon, Marcus Vaughan, described how risk culture is critical amongst the tapestry of fundamentals to managing risks, enterprise wide. How an organisation communicated its expectations to staff, and how those staff understood those accountabilities and responsibilities, correlates with high overall risk maturity. Ultimately improving risk culture enables an organisation to ramp up its overall risk maturity rating.

According to Ashley Palmer, an Actuary and Principal at Aon, the GFC showed how compliance and checklists would only get an organisation so far.

"It's culture that determines behaviour," Palmer said. "You can have the best business plans and strategies in the world, but if your culture doesn't support it, you'll fail."

Palmer described risk culture as 'how people behave when nobody is looking' (see fig. 6). While no single solution would fit every organisation, finding the right culture traits depended on the organisation's primary strategy. But all high performers shared the traits of decisiveness, long-term orientation, proactivity, openness and people orientation. Moving the needle required strong leadership and cross-business collaboration.

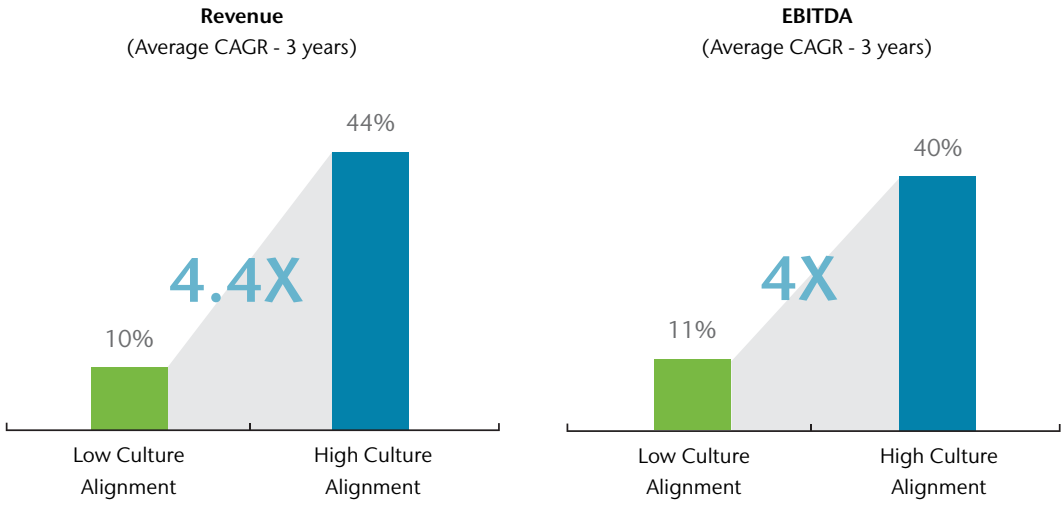
Figure 6: Risk Culture

© Aon propriety model

A recent Aon study on Getting Real About Creating a High-Performance Culture found that organisations that align their culture to the business strategy have 44% more engaged employees, and twice as many employees will stay with the company; and organisations that align their culture with their business strategy have four times higher sales and earnings growth as compared to companies with low culture alignment (see fig. 7).

Figure 7: Cultural alignment drives business performance

Compound Annual Growth Rate (CAGR) - Low Culture Alignment vs. High Culture Alignment



Source: © Aon Global Research

The panel also included comments from the Chief Risk Officer at Perpetual Limited, Michael Vainauskas, on how they built a positive risk culture. Vainauskas described how Perpetual had fully integrated culture into its programs, with the initiative led and supported from the top of the organisation.

Critical to the process had been the creation of a team of risk champions across the organisation. These were people for whom 5% to 10% of their time was spent on risk-related activities across the business units and the support areas. Each was trained up on new policies, how to manage risk systems, and how to do good control testing.

Vainauskas also described the importance of simple messaging, and the need for all staff to take ownership of risk, which began with the staff onboarding process. He stressed the need for everyone to be aligned, and hence Perpetual had included a risk overlay in its employee's scorecards.

Swire Pacific Case Study – Managing Risk from a Multinational Perspective

The Hong Kong-based publicly listed company Swire Pacific employs more than 90,000 staff across a diverse portfolio of operations covering property, transport, engineering, beverages in Asia and the Americas.

Swire Pacific's Group Head of Risk Management Tom Cohen described the steps his company had taken to improve its risk maturity in the face of such significant industrial and geographic diversity.

Swire Pacific has had a risk management committee in place for about 15 years, but 10 years ago, in recognition of the diverse nature of its businesses, the company created new overlays to accommodate that diversity.

The result was the formation of a group risk management committee comprised of the CEOs of each of Swire Pacific's five divisions, as well as the group CFO to act as the chair. Swire then identified specific areas of risk and selected the subject matter experts from each of the divisions to form additional committees. These communicate and share information on common risks, with the goal of generating policy recommendations for the risk committee. Swire Pacific also created sub-groups of risk champions in functional areas that the committees can tap into when needed.

As the Head of Risk Management, Cohen described his role as the organiser-in-chief of these committees, sitting on all the functional risk committees. He reports to the group CFO, and manages a team of six specialists, including for cyber risk. They ensure risk processes are carried out according to standards, but also get involved in scenario analysis and reviews of divisional risk.

Cohen also oversees the central committee on health and safety, working with experts from each of the divisions, and works closely with the public affairs team on crisis management plans. Cohen described a key part of his role as being to highlight emerging risk issues and challenge the status quo through involvement in workshops in risk registers. Hence cyber was a key focus, along with the need to assess the impact of disruptive technologies on Swire Pacific's investments in property and other industries.

Another significant area of risk focus came from Swire Pacific's investments in mainland China, where any shock to the economy had a direct impact on investments there and flow-on impacts to its global activities.

In terms of insurance, Cohen said Swire Pacific generally worked on country-based programs with decisions based on pricing and market fit, although initial steps have been taken to globalise programmes where appropriate.

With such a diverse portfolio of businesses, streamlining risk management was always desirable. But Cohen said ultimately the five individual businesses had their own risk appetites. Hence he and his team worked to instil a risk culture through sharing of best practice, and aligning divisional teams to adopt agreed methodologies to ensure a more consistent approach to measuring, reporting and identifying risks.

Navigating the D&O Storm

It is not an easy time to be a director.

Since the first shareholder securities class action to the most recent, total settlements, including defence costs, have reached a staggering $1.7 billion; protecting directors and officers is becoming a minefield for insurers and clients alike. The rise of litigation funders, increasing regulatory investigations, and the growing prominence of cyber-related liabilities is making that landscape more complicated yet.

None of this bodes well for D&O insurance providers. Research by JP Morgan Taylor Fry found the combined ratio for D&O insurance for 2016 was 121%, which is likely to be 250% to 300% by the time insurers eventually close the books on the 2016 policy year. A target combined ratio for an insurer would be 85%, with 100% representing break even. Anything above that represents a loss.

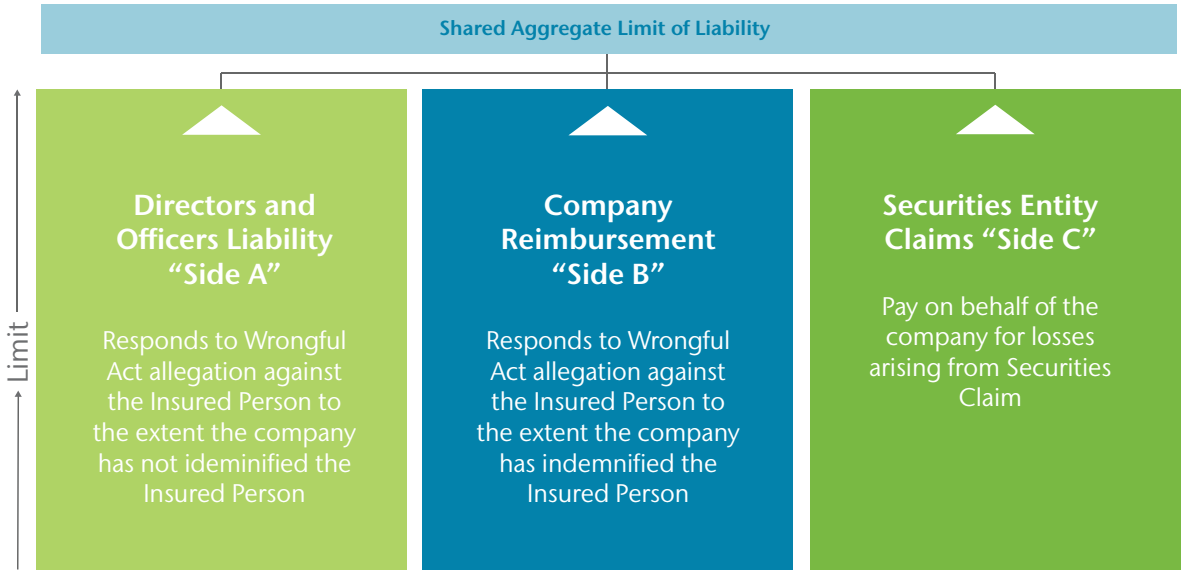
These issues were key points in a panel session at this year's conference, which discussed the risks for directors and the increasing complexity of D&O insurance.

Part of the growth in shareholder class actions can be attributed to the rise of litigation funders. The general counsel and company secretary for litigation funder IMF Bentham, Jeremy Sambrook, told how IMF Bentham itself claimed a 91% success rate, which was achieved through a rigorous vetting process that examined the likelihood of a positive result, as well as the potential value of the payout, including examination of the balance sheet and insurance.

Another significant change has been the rise of side C insurance, in addition to sides A and B (see fig. 8). However, with cover often capped across all three sides, this could lead to the potential for cover to be used up in a side C settlement, with nothing left for directors who would otherwise be covered under side A.

According to Rehana Box, an insurance advisory partner with the global law firm Ashurst, the solution for some organisations was to simply buy more insurance, although this could quickly prove to be too expensive.

Figure 8: D&O policy structure



Box said additional problems lay ahead for directors and officers thanks to the increasing potential for personal liability and penalties flowing from regulatory changes. One example was the incoming Banking Executive Accountability Regime, which would impose additional fines, penalties and possible disqualification on directors and officers of Authorised Deposit-taking Institutions (ADIs) , and might prove uninsurable. Also, she added that while most policies still provide cyber cover, insurers were becoming more aware of what the aggregated risk is. Reading the fine print is more vital now than ever.

The Head of Aon's Financial & Professional Services Group for the UK, Tracey-Lee Kus told how Australia was only second now to the US in terms of losses and their impact on D&O policies, and Australia was also now leading the way in litigation funding. She also warned of the growing risk from cyber.

"We've seen a number of potential actions on D&O coming through on the back of cyber," Kus said. "We are expecting any day now to have a cyber suit come through and for it to be fairly large."

She added that governments and regulators were now communicating and working together much more effectively, leading to more cross-border activity.

The result was that boards were now being more careful and only insuring those officers they need to provide deeds of indemnity for, and in some cases restricting themselves to only side A. On the flipside, she said changes were also making it more difficult for some organisations to buy cover, adding that the key to securing to coverage from London often came down to one-to-one meetings with insurers.

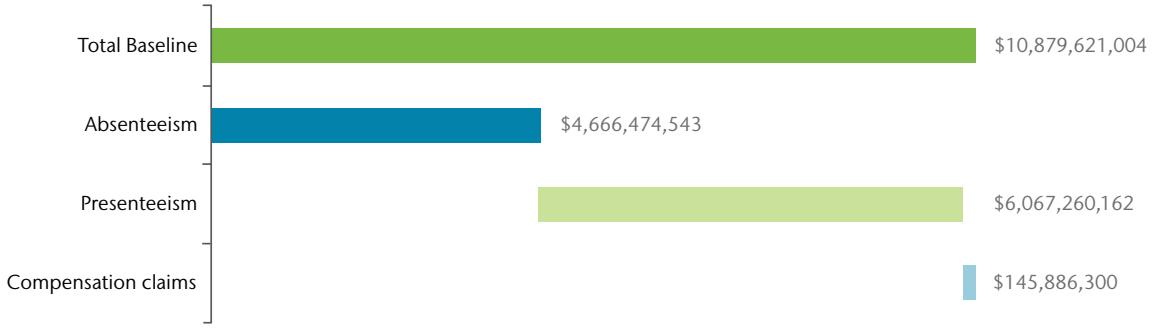
"Getting on a plane and actually getting to London really helps," she said.

Mental Health – What is it truly costing your organisation?

A person's mental health is the result of a complex interplay between their biology, their psychology, and their environment, as well as whatever life throws at them.

One in five Australians aged between 16 to 85 are likely to experience a common mental illness in any given year, and this increases to 45% over a lifetime. And as PwC reported in 2014, the cost of poor mental health to the Australian economy is $10.9 billion every year (see fig. 9).

Figure 9: Baseline mental health condition impacts (per year), by individual impact



Source: PwC, Creating a Mentally Healthy Workplace, 2014

Mental health is dynamic, and whether a person has good mental health or not can easily change through the course of a day, and absolutely over a lifetime.

The final panel at the Aon ARC 2017 discussed mental health in general, and the role of the workplace in supporting good mental health.

According to Jennifer Cameron, Client Director for People Risk at Aon, an integrated approach to mental health had to be based on the three pillars: support; prevention; and promotion. She added it was important that employers considered organisational factors when thinking about the mental health of the employees.

"Both organisational and individual factors must be considered to create a mentally healthy workplace," Cameron said.

Cameron recommended the use of the Guarding Minds @ Work survey, which gave a reading on the workplace factors impacting psychological health and safety. This is one tool that could be used to create a strategic and evidence-based perspective on the psychosocial risk that existed within the workplace.

She said existing data sources such as employee assistance program (EAP) utilisation, engagement and absence data could also provide useful insight into mental health, while qualitative research provided a window into the perceptions of people in an organisation.

Finally, she advised that taking a management systems approach to mental health could ensure it was embedded into the organisation on a business-as-usual basis.

Coca-Cola Amatil's Head of Health, Safety and Wellbeing Danielle Odd also shared what her company had achieved in mental health, starting in 2014 with the training of 80 Mental Health First Aiders. This training gave participants an understanding of mental illnesses and strategies to connect people with professional help.

Coca-Cola Amatil also developed a psychological injury flow chart to provide a simple way for managers to navigate through crises and support workers with problems, while an injury triage hotline provided a means to immediately support anyone who used it. Choosing a new EAP provider gave the company a chance to shift that model to staff assurance, and a program called Healthy Minds @ Work was developed to assist managers to understand common mental health conditions.

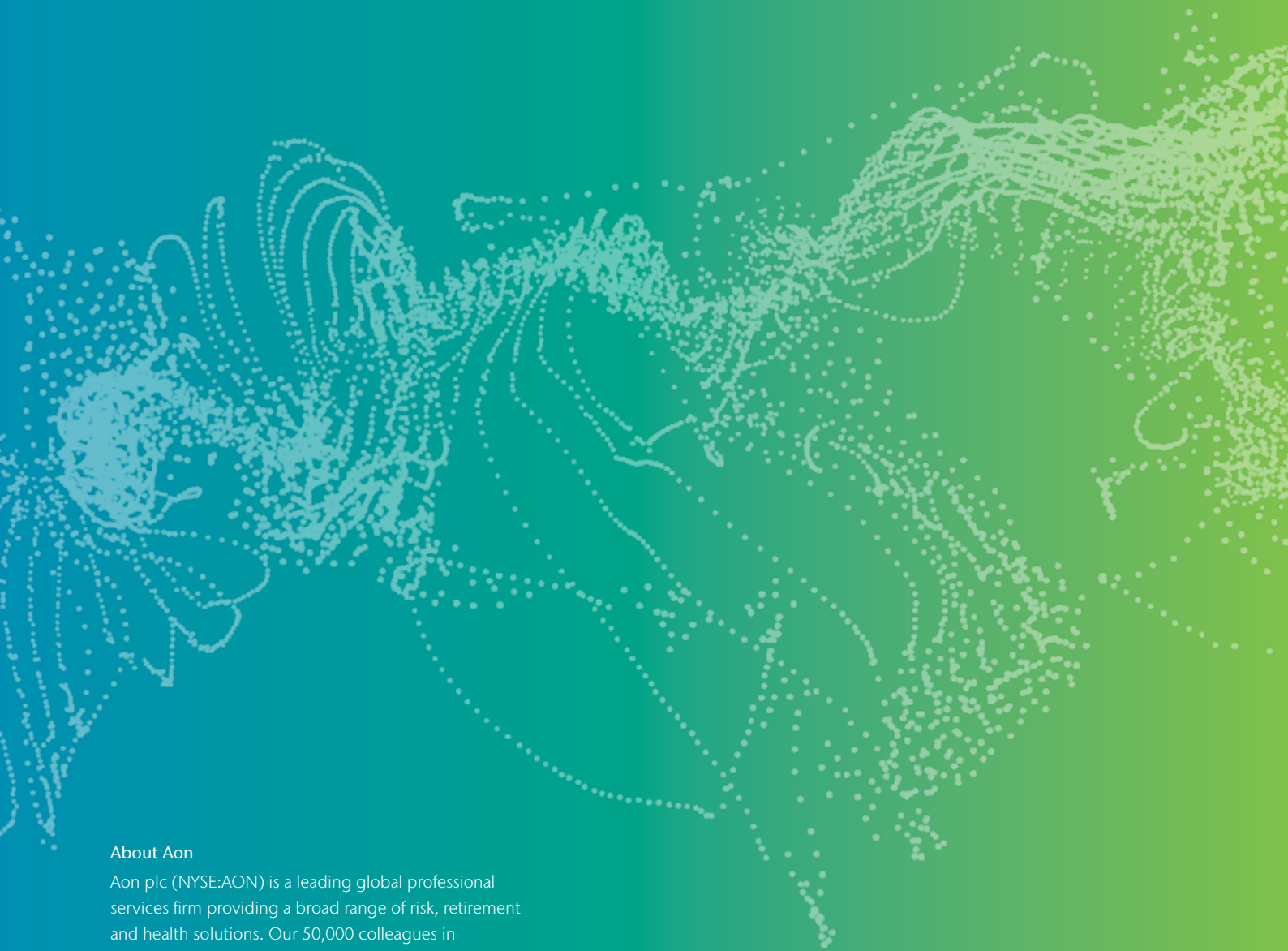
The Executive Director of the Lifeline Research Foundation Alan Woodward also spoke, and suggested five things that any organisation could do to assist the mental health of its employees.

Firstly, he suggested showing compassion and support to a person in crisis by creating a compassionate environment. Second was to be aware that a person may be struggling as a result of an underlying mental health issue, be it diagnosed or not. Third, he said confronting issues earlier rather than later was always a better strategy, and his fourth recommendation was that, as crisis situation can lead to suicide, it was important that organisations took crisis situations seriously and worked to de-escalate a crisis quickly. Finally, he said that sometimes a crisis occurred because of circumstances in a person life, such as financial troubles, workplace pressures, or discrimination, and so organisations could play a role in preventing crises by creating workplaces that were open, non-discriminatory in nature, and looked into issues of work pressures.

But most important of all, he told the audience the one thing that could really make a difference when a person is in crisis - another person.

NEW WORLD DISORDER

ADVANCED RISK CONFERENCE
10–11 OCTOBER 2017



About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com.au

CORP0115X 1117

AON
Empower Results®