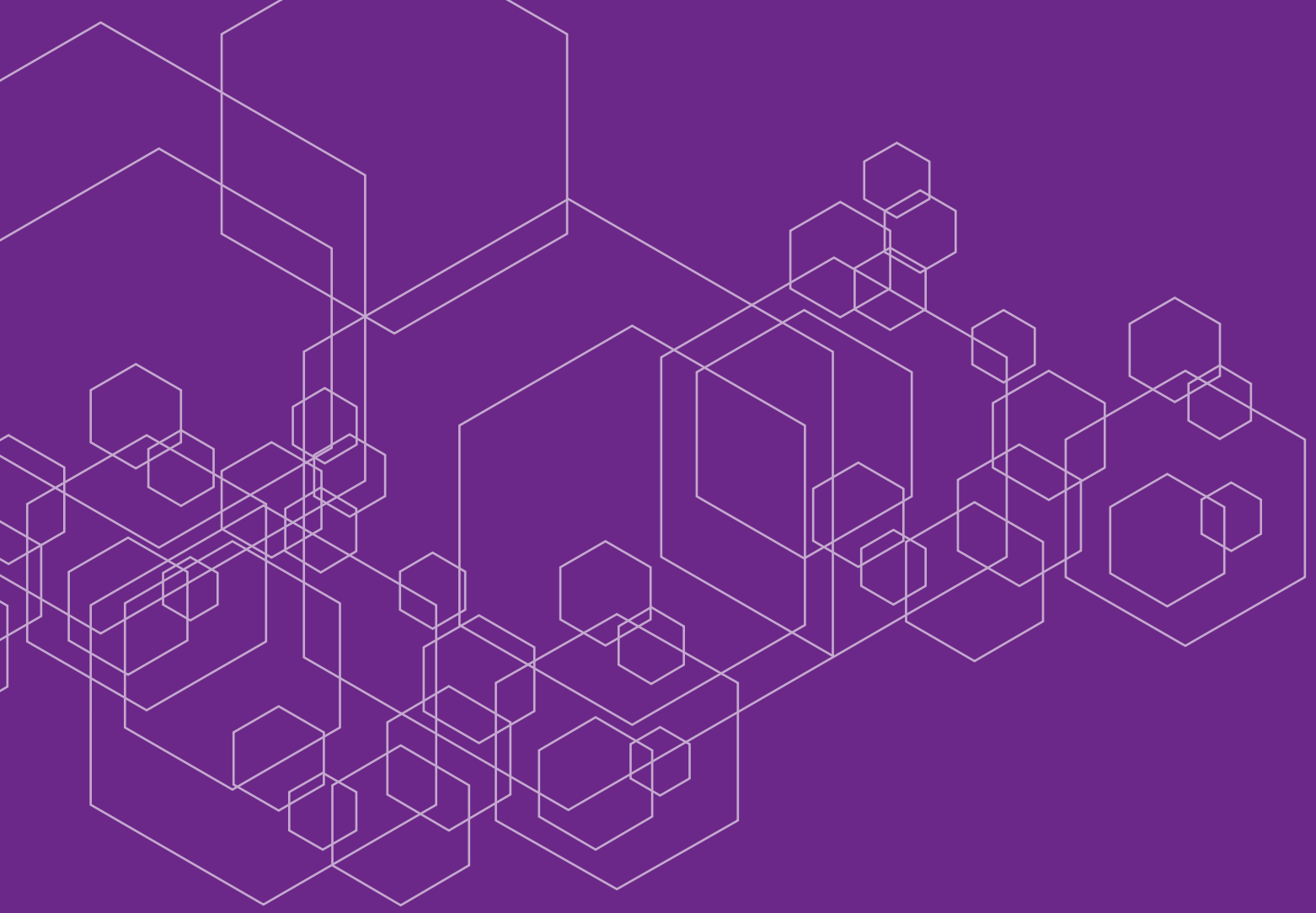
THE RISK REVOLUTION

November 2016

AON

Empower Results®



Contents

Executive summary

The 2016 Aon Advanced Risk Conference (ARC) built on last year's conference theme of disruption and delved further into the risk revolution —fuelled by big data, the sharing economy, social media, and what is termed the next industrial revolution - the Internet of Things.

Lambros Lambrou
CEO Australia
Aon Risk Solutions

Speed of change

The world is rapidly changing from an economic and societal perspective and if Moore's Law (that price performance doubles every 18 months) holds true, this will only continue to quicken. We can see this with Uber. Commencing with just 11 ride-share vehicles in San Francisco in 2011, its global fleet of drivers completed their two billionth ride by June this year, just six months after completing their first billion.

From a societal perspective, conventions of how trust is built and managed – in brands, leaders, and systems are being upturned. Technology is now facilitating new ways which help us trust unknown people, companies and ideas. Think Blockchain and Airbnb.

Likewise, more data has been created in the past two years than in the previous history of the human race. And within the next three years it is anticipated that artificial intelligence will pass the Turing test — meaning the machine response will be indistinguishable from the human response.

Two of the things that have fuelled these accelerated changes are the internet and the ubiquity of the smart phone. Yet for all the benefits this global connectivity brings to business, every new technology you introduce into your organisation opens another attack vector for malicious actors who may want to steal your IP or customer data, or hold you to ransom, which has serious potential to cripple your business.

Against this backdrop, our economy is undergoing significant structural change. Knowledge is the currency of the future, with agglomeration the key to sparking new ideas and new ways of doing things.

Disrupt or be disrupted

New business models aided by a perfect storm of unmet customer needs, new technology and reduced barriers to entry are tapping into consumer appetite for more relevant and customer-centric offerings. Clearly these are exciting times, but the rapid rate of change that is opening so many new business opportunities is also delivering new sets of risks. Legacy players are under threat from nimble new entrants, who themselves are negotiating a constant minefield of risk as they attempt to achieve scale and maintain their first-mover advantage.

Chances are, whatever you're doing today, someone is working on a way to do it better tomorrow. That certainly applies to insurance.

Across the board, opportunities to disrupt the insurance sector clearly exist for those who are willing to question the fundamentals of our industry and ask "why is it so?" rather than remain complacent and comfortable in adhering to a set of practices that originated in a London coffee house in 1688, which eventually became Lloyd's of London.

This report presents a summary of the insights provided by our panel of Australian and international speakers at the 2016 Aon ARC. I trust you will find it informative, and that it will assist you and your organisation to think differently about your approach to managing and mitigating risk.

The new economic revolution: Australia and the knowledge economy

Professor Ian Harper, Deloitte Access Economics and Chair of the Harper Review of Australia's competition laws and policies, provided an overview of the re-balancing that is taking place in the Australian economy post the investment phase of the mining boom. He also outlined the importance of competition, innovation and creativity in achieving the productivity growth that will deliver our future prosperity.

China remains Australia's most important trade partner

Any examination of the risks to Australia's economic prosperity must begin by looking at China. As things go in China, so they go in Australia — at least for the time being.

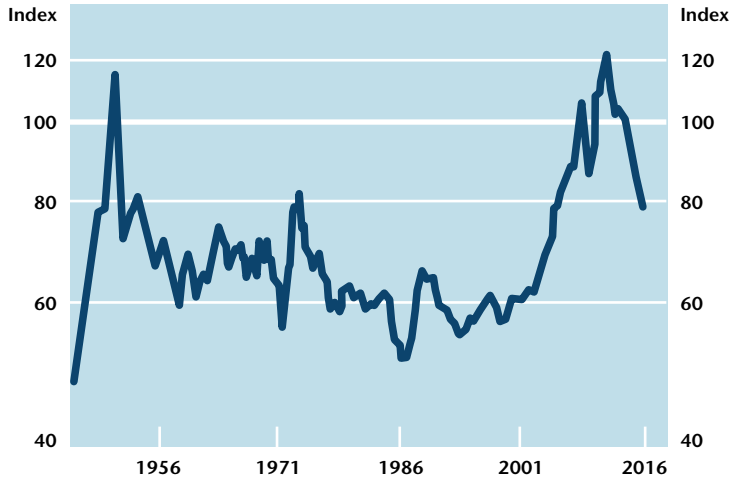
For close to two decades, as the Chinese economy grew at extraordinary rates and its development trajectory rose at a pace and scale never seen before, China was a massive buyer of our resources. Through low-cost labour they turned these resources into cheap manufactured goods that we then bought. This ability to sell our commodities at a high price, and buy goods at a low one, raised Australia's terms of trade, which in turn drove up our living standards.

However, with the Chinese economy now transitioning away from its resources-intensive construction phase to one driven by consumption, which is more focused on services and characterised by reduced investment in industrialisation, our exports to China have become less commodity-intensive, and our terms of trade have fallen. That affects all of us.

The correlation between terms of trade and living standards is shown in the following two charts.

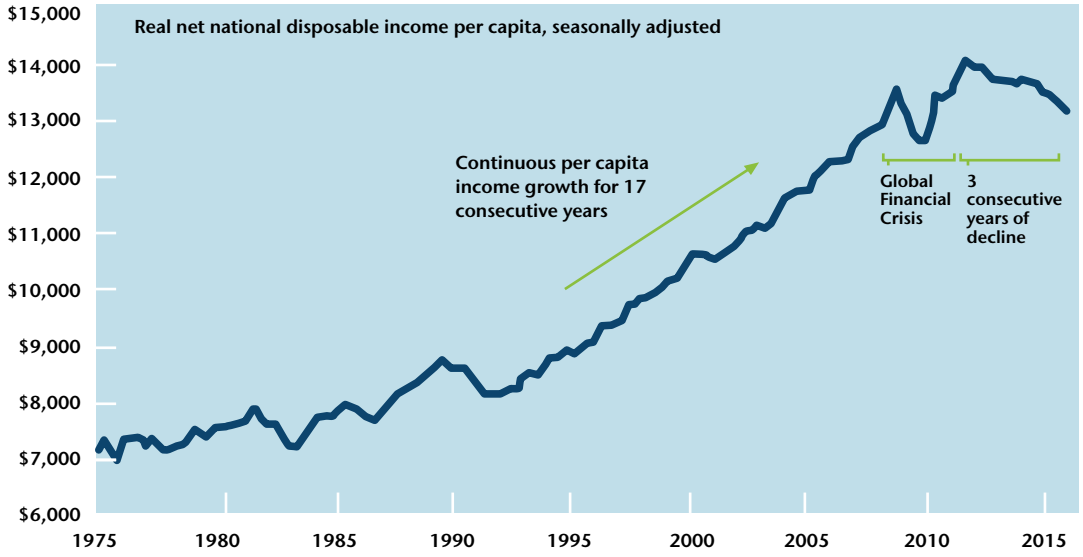
Chart 1: Australia's terms of trade*

2013/2014 average = 100, log scale



*Annual data are used prior to 1960
Sources: ABS; RBA

Chart 2: Changes in Australian living standards



Source: ABS

What are the key risks from China's transition?

The Chinese economy is forecast to continue its gradual slow down, out to 2020. The risk is that this is an overly optimistic outlook and that, instead of a smooth transition from the first phase of growth to the next, it might become a very bumpy one.

Recently there has been a great deal of unease about what is happening in the Chinese real estate market. There is also a considerable focus on the rising indebtedness of Chinese banks, and concern has been raised that the Chinese financial system could get into trouble.

While these are all certainly risks, it is important to note that the Chinese government is in a very strong position to recapitalise the banking system if necessary. Chinese foreign exchange reserves are enormous and at historic highs. For this reason, if some such difficulty arose, its impact on the world economy would be disruptive, but not on the same scale as the Global Financial Crisis.

However, well short of any need to draw on its substantial financial armoury, the Chinese government is starting to impose restraints on the quality of lending. It is also beginning to close down loss-making businesses, such as inefficient power stations and steel producers. This latter action is delivering dividends for our coal and steel exporters as it has led to an upturn in the price of these commodities over the past couple of months.

Will Australia's terms of trade deteriorate further?

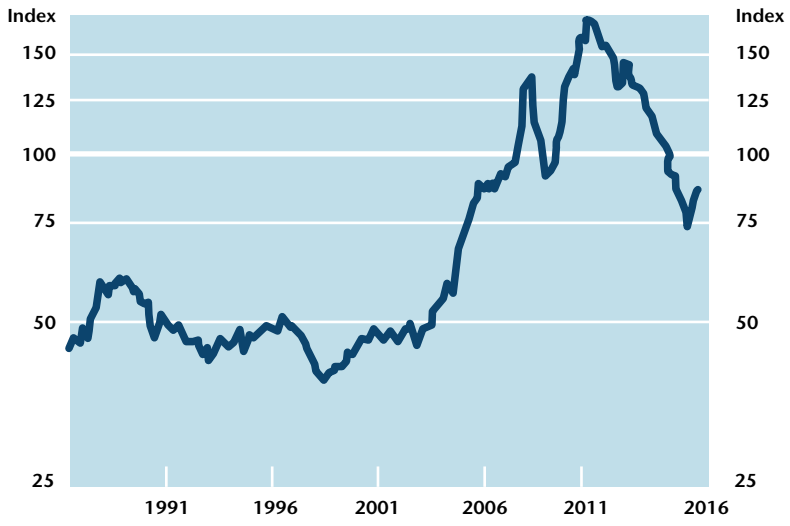
After many consecutive years of riding an enormous wave that drove growth in wages, company profits, and government income, over the past three years our terms of trade have fallen and our economic growth has slowed, primarily due to what's been happening in China. In turn, this is driving the decline in per capita real disposable income.

What we've been experiencing is the economic equivalent of the tide going out. And as Warren Buffet said, "only when the tide goes out do you discover who's been swimming naked".

However, while the terms of trade are still falling, most economic forecasters expect them to stabilise at current levels.

It is important to understand the cyclical nature of our economy and that, as China goes through its development phase, we will recover to the sorts of growth rates we've experienced in the past. The Australian economy is underpinned by resources rather than a strong manufacturing sector. While commodity prices drive our terms of trade, they move much more than the price of manufactured goods. The following chart shows that commodity prices may have bottomed, which supports the view that our terms of trade will do the same.

Chart 3: Movement in commodity prices
SDR, 2014/2015 average=100, log scale



Source: RBA

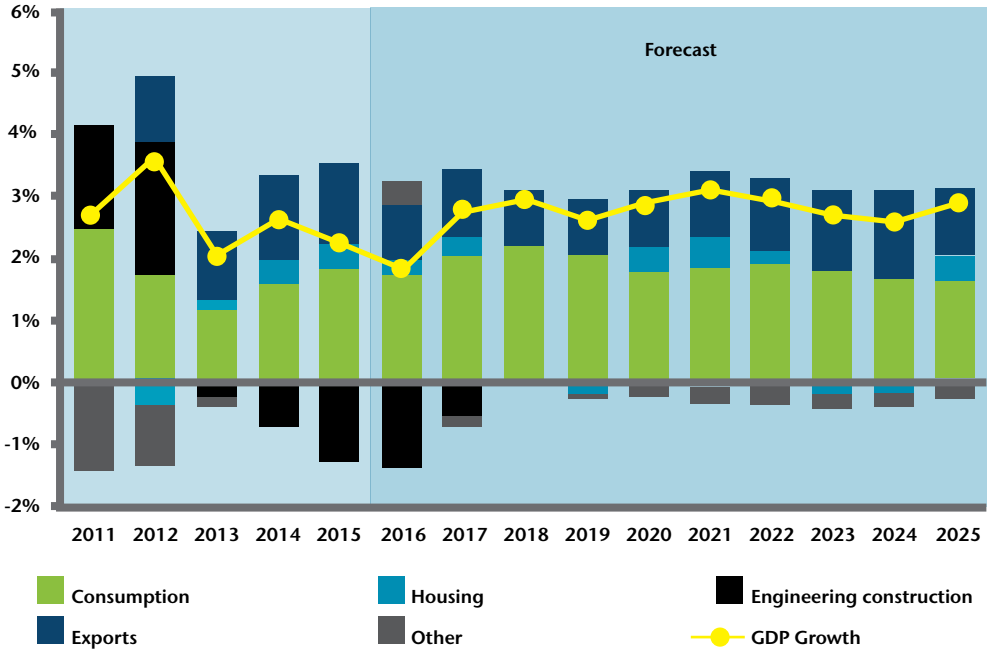
Growth is forecast to return to historical averages

Looking forward over the next three years, consumption — which accounts for 60% of our economy — is expected to show some slight increase in growth, indicating that the impact on living standards from stalled growth in wages and other forms of income is starting to moderate.

Falling business investment, which has been the manifestation of the downdraft in output growth, will be less negative. Conversely, although the investment phase of the mining boom has ended, we have entered the export phase and expect to see strong growth in exports of natural gas, coal and iron ore over the next three years.

The following chart shows the expected timeline for economic growth to return to the historical average of 3 to 3¼%.

Chart 4: Components of demand and growth forecasts



Source: Deloitte Access Economics Pty Ltd

Future prosperity requires productivity growth and innovation

The most powerful lever for lifting real incomes and living standards is domestic productivity growth. Productivity improvements are driven by competition and creativity. Competition works across both the private and public sectors and provides the spur to improve processes, develop new products, and better meet customers' needs.

The recently completed competition policy review (which Professor Harper chaired) extends the reforms recommended by the Hilmer Review of 1993. It includes competition law reform recommendations designed to sharpen the competitive impetus within businesses — to turn up the Bunsen burner under the competitive process, rather than protect particular competitors.

In the knowledge economy, place takes on greater importance

The industrial age was about economies of scale. The knowledge age is about economies of agglomeration. It thrives by bringing people together, so they can spark off one another to create new ideas, new ways of doing things.

This is why our cities and regions are so important. Cities are the engines of productivity growth. In Australia, we are blessed with some of the world's most liveable, and hence most productive cities. We have a comparative advantage in the way our places are distributed and the way they are run.

When you blend liveability with amenity, you drive productivity in the knowledge age.

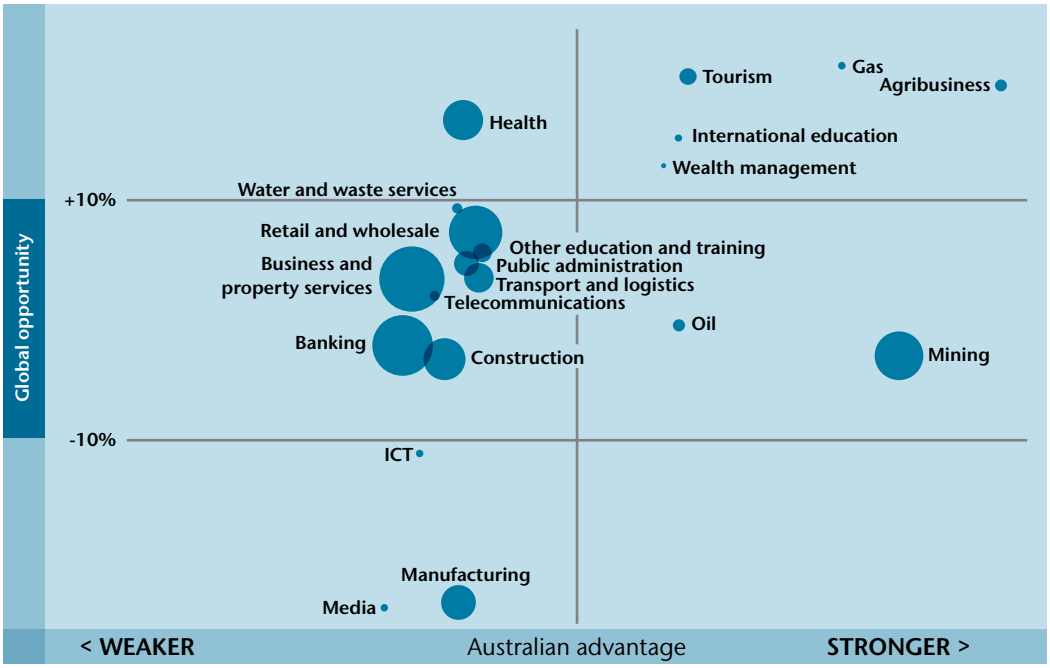
So who will be the winners?

Looking to 2030, there are certain sectors that are forecast to grow 10% faster than global growth. These are the industries in which we have an international comparative advantage:

- Agribusiness.
- Gas.
- Tourism.
- International education.
- Wealth management.

They won't necessarily be the biggest sectors but the fastest growing.

Chart 5: Longer term growth outlook



Source: Deloitte Access Economics Pty Ltd

The challenge of embracing risk

While rising living standards are driven by creativity, innovation and productivity, all of these bring risk, but in general it is good risk. The downside is that each involves change, disruption and displacement. But they will also fuel engagement, collaboration and growth.

The big challenge for us is that our future prosperity depends on embracing these sorts of risks, managing them, and profiting from them at every level of our economy. Doing this will raise our living standards and leave our country in better shape for our children and grandchildren, better even than what we have enjoyed in our lifetimes.

The unstoppable rise of the evolving sharing economy

Jason Disborough, Chief Executive Officer, Multinational Accounts, Aon Risk Solutions, facilitated a panel discussion between three experts in the sharing economy space — Chris Noone, CEO, Collaborate Corporation; Perry Abbott, Managing Director and CEO, Friendsurance; and Randy Nornes, Executive Vice President, Aon Risk Solutions, Chicago — about the unstoppable rise of this business model, which is driven by mobile technology and a world of constant connectedness.

While Uber and Airbnb are two of the sharing economy's most widely recognised names, its game-changing potential to disrupt traditional business models and upend entrenched players goes beyond providing a discovery and transactional platform that connects buyers and sellers of both assets and labour.

This panel discussion examined different facets of the sharing economy, and provided insights into the common challenges faced by most platforms. It also demonstrated how the technology that enables the sharing economy can either provide new opportunities for private and public sector organisations, or make their offering seem increasingly irrelevant.

The two industry presenters, Chris Noone and Perry Abbott, have extensive experience in developing and operating sharing economy enterprises, however their businesses are vastly different. Collaborate Corporation operates three businesses (DriveMyCar, MyCaravan, and Mobilise.com) that are focussed on enabling under-utilised assets to be monetised, and are tied together through a proprietary verification platform, PeerPass. On the other hand, Friendsurance is in the process of launching a peer-to-peer insurance offering into the Australian market, which allows people to come together online and create their own risk pools for small claims and deductibles. Founded in 2010 in Berlin, Friendsurance holds the claim of being the world's first genuine peer-to-peer insurance provider.

Randy Nornes from Aon, Chicago, provided an additional perspective based on his work with clients such as Uber, GrubHub, PayPal and Getaround, sharing his thoughts on emerging trends and future areas of growth.

Trust is crucial

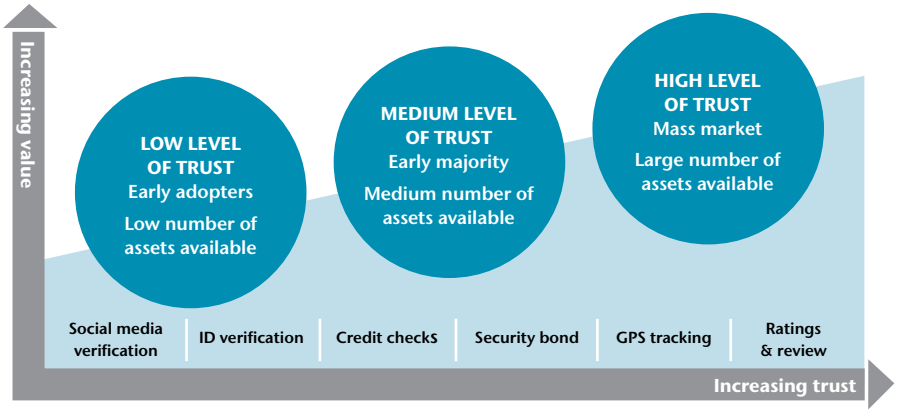
A common feature of most platforms is that they facilitate discovery — they make it easy for buyers to find sellers. But that on its own doesn't create the confidence required to transact.

Ratings and reviews of — and by — sellers and buyers have become a staple of the sharing economy. The more positive reviews an Airbnb property receives, for example, the greater the sense that this will be a good accommodation choice. But, as Chris Noone points out, all this happens post the transaction, which is why Collaborate developed PeerPass. This verification platform uses ID and credit checks, social media analytics, and various other data to rate individuals before the first transaction.

"The more we can do to verify our customers, the greater the assurance we can provide the owner of the asset that in addition to receiving an economic benefit, it will be respected and looked after. And the more trust we build, the more our market will grow, as the owners of assets become satisfied that their appetite for risk has been met."

Chart 6: The value of trust and reputation

As trust increases, more idle assets become available for listing in peer-to-peer marketplaces



Chris Noone sees a future where a platform such as PeerPass could be used across multiple marketplaces, enabling users to take their online reputation from one platform to the next. Collaborate's verification process is also paying dividends through lower insurance costs.

"We've now reduced our Claims Loss Ratio to 46%, which is much lower than what you're seeing in the consumer market, and certainly much lower than what you see in the rental car market. The premium discount we're enjoying as a result of that claims experience is delivering a good return on the investment we've put into the verification side of the business."

The market is outpacing legislators and regulators

The sharing economy business model doesn't always fit neatly into existing regulatory models. That affects a number of things, including insurance, and highlights the fact that risk is at the core of such platforms.

Randy Nornes' view is that one of the issues making the regulatory situation more complex, is the opposition by legacy operators to these new entrants. "There's automatic friction between the competitors, and a lot of this friction arises from dated, unclear regulatory frameworks. Technology has changed the nature of customer / provider relationships, requiring new regulatory approaches. Regulators don't like to be put on the spot. It's uncomfortable for them. They like to run the playbook, run the rules, but now we're forcing them to make choices."

The same obstacles exist for players looking at cross-border transactions. Perry Abbott says that from a global insurance perspective, this is an issue for Friendsurance. "The next evolution for us is where the regulatory framework allows people to peer-connect across different countries."

Similar concerns were also raised in Anthony Belfiore's presentation, when he spoke about regulatory compliance. "At Aon, we're in 120 countries. I deal with 360 global regulators, each with their own view of cyber policy, and each having prescriptive views on the regulatory environment in their country and what they expect."

A further issue is that insurance cover is often contingent on regulatory compliance. Both rely heavily on historical data, which is a challenge when you have a new operating model. Randy Nornes asks, "Whether you're trying to get an insurance company on board, or convince a regulator that your business model is a good business model, how do you translate the new business model into something that people feel comfortable with?"

Changing the dynamics of the insurance model

Friendsurance demonstrates that the potential of the sharing economy is much more than just the monetisation of under-utilised assets and labour.

Driven by social media, Friendsurance enables a number of friends to get together (the model is based on groupings of ten) to put aside some money each year to cover off small claims across electronics, household, and personal-liability insurance. Large claims are still covered by traditional insurance carriers but small claims, and the deductible, are covered by the group. At the end of the year, if claims are small or non-existent, the group receives a refund.

Perry Abbott says that by dealing with the moral hazard aspects, Friendsurance is trying to change some of the dynamics that sit within the insurance model. "Our goal is for people to make fewer claims, either because they are following less risky behaviour, or that claims that shouldn't be put in, aren't being put in."

He acknowledges that trust is also central to Friendsurance, however with this model it is based on the trust you have within your peer group. "If you want to make a minor claim that isn't real, you're making it off people you know, and not off a faceless insurer. That's something that's very complementary to the insurance industry because it means that both the consumer and the insurer share the benefit."

The speed of growth and the importance of scale

Many sharing economy businesses are growing at an extremely rapid pace, which is essential to achieving the scale and penetration required to prevent replication of the model by competitors, eroding any first-mover advantages.

For example, with ride-share services, the first entrant was Sidecar, but they grew too slowly and only raised about $35 million from investors, which ultimately meant they couldn't keep up with either Uber or Lyft. Founded in 2012, Sidecar eventually exited the market in late 2015.

Speaking of his experience with Uber, Randy Nornes says, "When I started working with them, they had a valuation of less than a billion dollars, and now their valuation is somewhere around $60 billion. They raised more capital than any start up in history — north of $12 billion. In five years, Uber has literally gone from just being an idea with 11 cars in San Francisco, to now operating two billion rides a year, all over the world."

Balancing supply and demand

Apart from the financial resources required for such accelerated growth, one of the major challenges is to grow supply and demand equally. For some time this was an issue for Collaborate who have always had a lot of demand, but initially found it hard to maintain supply.

Chris Noone credits the PeerPass platform as one of the major reasons they've been able to address this disparity. "Because we're now able to show the type of results we can get from both a financial and trust point of view, we are able to do deals with corporates such as McMillan Shakespeare Group, Australia's largest salary packaging and novated leasing provider, for whom we rent out their ex-lease vehicles. We also have an agreement with Subaru to rent out their brand new vehicles, and on the other side of the equation, we provide Uber drivers with the flexibility of accessing a well-priced rental vehicle for their work."

Where to next?

The sharing economy principles are already being applied across multiple industries. From a global perspective, one of the hot areas of growth is office space. A major player here is WeWork, which is creating collaborative work spaces and developing incubators in most major cities, and already has a global valuation of $10 billion.

In automotive, Randy Nornes cites models being developed that are taking dealer inventory and turning leases into subscriptions. Instead of leasing a Mercedes for three years, you subscribe to a class of vehicle, such as a BMW 750 or an S-class Mercedes, and then swap the vehicle whenever you want a change. "It's turning the dealer into a rental car lot, while also giving the customer a different experience. And dealers get a higher return on assets than under a traditional model."

Sharing economy models are now also being incorporated into traditional businesses. One of the best examples of this is what's happening in retail, where the customer service expectation turns on delivery — a demand for instant fulfilment.

"You can now order products online, and in many places in the world, get it literally delivered in an hour," says Randy Nornes. "The people that are making this happen, are the sharing economy drivers who are connected up for delivery. It's changing the customer expectation, so if you're a retailer and you're not able to offer instant delivery, your customer experience seems rather old. This is an example of how the sharing economy now enables an old industry model to perform at a different level."

Chris Noone sees that theme continuing, with the sharing economy becoming more mainstream. "State governments are either fully embracing it or putting in place legislation, where required, or clarifying existing regulation. Some are also looking at how it can work for them. We now have the opportunity to rent cars to the NSW government — that enables them to take advantage of other assets and delivers savings to taxpayers."

Clearly we are just seeing the beginning of how the sharing economy model is transforming the transactional landscape. On its current growth trajectory, it truly looks unstoppable.

Cyber terrorism: Protecting critical infrastructure

With mandatory data breach notification laws soon to be enacted, the presentation by Anthony Belfiore, Senior Vice President and Chief Security Officer, Aon Risk Solutions, Chicago, provided a comprehensive overview of the global cyber threat environment, and examined strategies for managing and mitigating cyber risks. His role at Aon encompasses global physical security, global cyber security, IT risk and resiliency, fraud, investigation — basically anything that deals with the security or risk spectrum relating to Aon's people, information, assets or technology.

The cyber threat landscape

Cyber is a massively obtuse term that gives rise to innumerable risks. With the uptake in cloud computing and outsourcing, the extent of your vulnerability now extends beyond third party risks to involve fourth and even fifth parties.

As technology changes, new risks emerge, and over the past decade we have not only seen the type of threat change, but also the motivations of malicious actors.

Historically, data loss was the main concern for the corporate world, and this centred mostly on the theft of credit card numbers or user identifiable information. Today, we are broadly dealing with three distinct types of threat, which are often being carried out by cyber criminals with quite distinct motivations:

1. Data theft.
2. Monetisation of fraud.
3. Attacks that are designed to take down companies, governments or infrastructure.

However we are no longer just dealing with individual hackers or criminal gangs. Since around 2012, there has been a sharp increase in cyberattacks sponsored by nation-states.

One of the most notable occurred in August 2012, when the computer networks at Saudi Aramco — the state-owned national oil company of Saudi Arabia, and the world's largest exporter of crude oil — were attacked by a competing foreign nation seeking to gain a competitive advantage through obtaining details of a deal being negotiated by Saudi Aramco. To cover their tracks, the attackers wrote a piece of malware, which partially wiped or totally destroyed the hard drives of 35,000 computers. The malware was activated when a Saudi Aramco employee clicked on a link in a spear phishing email.

In September 2012, there was an attempt by a Middle Eastern-based group to take down Wall Street through a distributed denial of service (DDoS) attack. Such attacks are designed to overwhelm a website or server through launching a tsunami of traffic, denying access to legitimate users.

Attacks are now more frequent and severe

If such attackers can take out the largest companies on the planet with the biggest cyber security budgets, it leaves smaller organisations in a very vulnerable position. The attacks of 2012 also served as a wake-up call to governments, highlighting the potential threat to transportation, water supplies, power and other critical infrastructure.

Such large scale attacks are now quite frequent. In late 2014, Sony Pictures Entertainment was hacked (most likely by the North Korean government), locking employees out of their computer network and making internal data public. And in September this year, Yahoo disclosed a 2014 breach in which 500 million user accounts were hacked — also, allegedly, by a state-sponsored actor. As a result of the disclosure, Verizon has reduced its bid for Yahoo by $1 billion.

External attacks are just one part of the picture

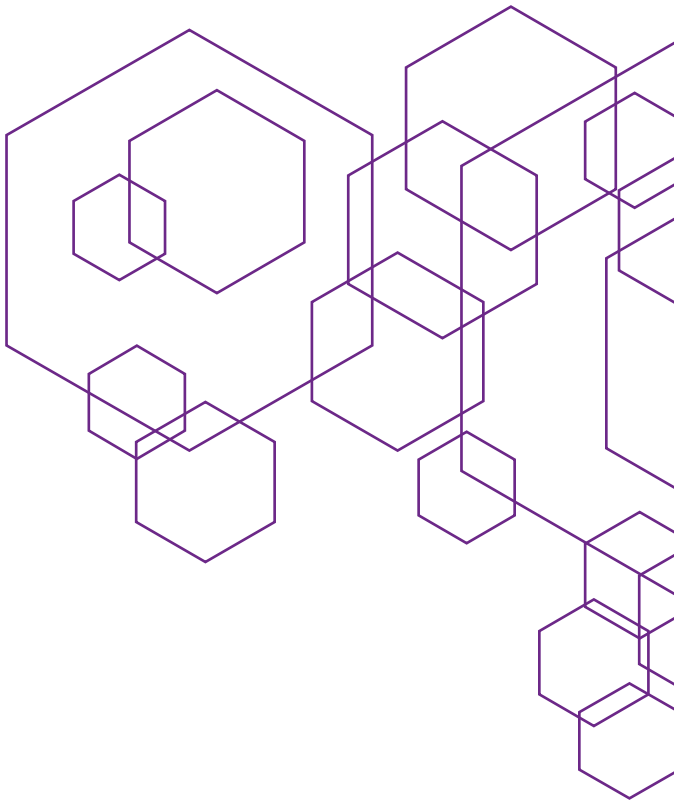
While these types of large scale attacks occupy the headlines, there are many different cyber threats. They include:

- **Technology disruption:** Examples of this are ransomware, DDoS attacks and other actions that are designed to disrupt an organisation and its networks.
- **Directed compromise:** Acts by nation-states targeting an enterprise to gain information or take it down.
- **Compliance deviation:** When an individual doesn't comply with the corporate cyber security policy, such as emailing documents to their Gmail account so they can be worked on at home, rather than logging in to the company network remotely and accessing its VPN (virtual private network) using a security token.
- **Information tampering and leakage:** Information theft by insiders, which could be from people stealing data and walking out the door with it, or still having access to the corporate network despite leaving the firm or being transferred to a different division.
- **Code of conduct and insider threat:** This is the biggest risk to most corporations and can range from employees making mistakes through to disgruntled ones deliberately causing harm. In Anthony Belfiore's experience, 80% of the most impactful and egregious issues occur within the firm.
- **Social engineering:** Thanks to the almost universal use of LinkedIn and Facebook by professionals, hackers have access to a wealth of personal information that makes it easier for them to hack into your accounts.

Cyber risk is an enterprise issue

Cyber is so massive that it's not simply something for IT to sort out. Breaches and issues are going to occur no matter how good your preventive controls, or how much capital and operational expenditure has gone into securing your environment. It's a question of "when", not "if".

A cyber issue involves numerous stakeholders across the enterprise, including PR and communications teams to manage reputational issues, and legal teams to ensure the correct regulatory notifications take place. From an operational perspective, the financial impacts of a cyber issue can be staggering. In addition to first party issues, most companies have interactions with other corporations and contractual agreements with clients and supply chains, all of which can result in significant third party breaches.



Aon's view

Are you prepared for mandatory breach reporting?

While in Australia today there is no mandatory obligation for an organisation to notify an individual of a data breach that involves their personal information, this is soon set to change.

The Department of the Prime Minister and Cabinet has proposed the long-mooted "Data Breaches Bill" in the current session of the Australian parliament. Given the bi-partisan support this Bill has previously enjoyed, it is more than likely that it will be passed imminently. It will then take effect 12 months after receiving royal ascent.

Clearly, the time to prepare for mandatory breach reporting is now.

What will it mean for you?

If there is a risk of serious harm to an individual as the result of a data breach, an organisation will be required to notify the Privacy Commissioner and the affected individual. The term "serious harm" describes a broad set of outcomes that may have adverse physical, psychological, emotional, reputational, economic, or financial consequences for the individual whose data has been breached.

The amount of data may be as little as one record.

Why does it matter?

Incident response costs and third party claims arising from a significant breach of your organisation's data can be financially crippling, while brand and reputational damage may be irreversible.

Whether it's business interruption and legal costs, or customer notification expenses and damage to data, organisations can no longer afford to ignore the real risk of cyber threats.

What next?

In preparation for the introduction of mandatory breach notification, you should:

- Review your risk exposures to breaches.
- Understand what data you possess or control and how your data is secured.
- Assess how a data breach would affect your organisation's reputation and balance sheet.
- Plan how you would respond to such an incident should it occur.
- Understand what risk management strategies you have in place to respond to the risks faced by your organisation.

Fighting the pace of innovation

With today's interconnected technology, the same forces that are pushing new disruptive technologies being leveraged for competitive advantage are also creating new risks.

With millions of lines of code written every day, it's impossible to understand their full implication at the time you put them into hardware, discrete software platforms or mobile devices. Sometimes you don't know where the holes are until things have been put into production. And while it's one thing knowing what a technology looks like on its own, it may not be possible to know what happens when it interacts with other technologies, and what gaps that will open up.

When you're leveraging technology, you need to know where your data assets sit, and how your end users interact with them. And you have to establish your general risk appetite for how much risk you're going to take.

Anthony Belfiore emphasises, "Cyber security risk management is always about shades of grey. It's a calculated risk and if the upside to the business makes sense from a cost-benefit perspective, then you need to consider it. You can't be in the dark ages and say you're not going to the cloud because it's scary — your data will be in someone else's hands".

Developing an enterprise cyber risk strategy

With mandatory data breach reporting legislation soon to be enacted in Australia, it will become even more important for organisations to understand and effectively manage their cyber risk exposures.

Anthony Belfiore employs an enterprise cyber risk strategy based on the following three actions:

1. Know the risks.
2. Rank the risks.
3. Have a plan.

"The first thing I do is work with my executive management team to know the risks. We identify them and then build an enterprise risk inventory, which may include things such as, liquidity and regulatory compliance; the cyber posture of the firm; massive disruption of service and lack of technological resiliency; third party supply chain; people capital and insider threat — to name a few."

These risks are then ranked and plans developed as to how to address them.

He stresses the importance of having the right conversations within your organisation, and to be able to answer questions such as, "What if someone locked us out of our back office for a day" or "What if we came in tomorrow and no one could communicate by email, chat or phone".

Aon's new Cyber Risk Management Advisory Group

Aon has recently entered into an agreement to acquire Stroz Friedberg Inc., a leading global risk management firm. Strotz Friedberg's 550 employees will join Aon's Cyber Solutions Group to create a comprehensive Cyber Risk Management Group that will deliver distinct client value, by combining standards-based cyber assessments and industry-leading risk transfer solutions.

The new group enables Aon clients to improve their proactive posture to the threat of cyber risk, and respond more effectively in the event of an attack.

The acquisition underscores Aon's understanding that companies need an integrated approach to managing and mitigating the systemic risk of cyber threats, and builds on its industry-leading position in cyber risk brokerage.

The role of cyber insurance

There are many costs — both financial and tangible — that can arise from a cyber issue. First party losses can include:

- PR, response, and continuity costs.
- Immediate and extended revenue loss.
- Restoration expenses.
- Defence costs.
- Property damage.
- Bodily damage.

Third party losses may extend to:

- Civil penalties and awards.
- Consequential revenue loss.
- Restoration expenses.
- Property damage.
- Bodily damage.

While cyber insurance has been problematic in the past, there are better and more comprehensive solutions available, such as the recently launched Aon Cyber Enterprise Solution™. (See "*A new approach to enterprise cyber coverage*", page 21.)

Anthony Belfiore also points out that managing cyber risk is related to scale. "Large corporations have the resources to invest in cyber security teams. For mid-sized companies, paying the premiums of an annual insurance policy will be more cost-effective than putting several million dollars of operating expenditure on the books for in-house cyber security resources and people."

A new approach to enterprise cyber coverage

In a Q&A with Jennifer Richards, Managing Director, Specialties, Aon Risk Solutions, Australia, Anthony Belfiore was asked about the rationale behind the development of the new Aon Cyber Enterprise Solution, and how the policy differs from other existing cyber solutions.

"Historically, when I was working in the financial services sector, I felt that the way cyber insurance risks where quantified and qualified didn't do any justice to the issues concerning the clients. One of the reasons for this was the difficulty for people to really understand or articulate their actual cyber exposure. There are thousands of risks under cyber, so it behoves the insurance industry to get on board and break down the risks into their more rudimentary components.

What we have done at Aon is to take our methodology to the big providers, and ask, 'If we can assess clients based on a new proprietary diagnostic tool we have built, and then provide you with assurance that they have a certain level of posture against a certain set of risks, would you insure them for a higher cap or would you give them a better deal on the insurance?'. In response, the providers have agreed that they want a better way to quantify and qualify the operational risk exposure related to cyber risk.

The methodology that backs this new policy focuses on assessing your organisation's cyber resilience versus walking you through a checklist. Rather than making you answer a hundred questions, we look at the risks you should be cognisant of based on your industry and our expertise."

The new Aon Cyber Enterprise Solution was developed through a collaboration of Aon cyber practitioners, including representatives from risk, technology, actuarial modelling, incident response, and security. It addresses emerging areas of cyber risk and related regulation, and features:

- Comprehensive limit approach — up to USD 400 million in capacity per policy.
- Aon proprietary language — single policy form.
- Property damage arising out of a network security breach.
- Products liability coverage to address Internet of Things exposures.
- Business interruption and extra expense coverage arising out of a systems failure.
- Contingent network business interruption for IT vendors and the supply chain.
- Cyber terrorism coverage.
- European Union General Data Protection Regulation fines and penalties (where insurable).
- Privacy/security liability and event expense coverage.
- Media liability and technology errors, and omissions by endorsement.

Australian case study: Data in the digital age

If one of the challenges of managing cyber risk is the pace of innovation, Craig Scroggie's presentation put some hard numbers and real world examples around the ever-evolving way we use technology. As Chief Executive Officer and Executive Director, of cloud computing services provider, NEXTDC, his organisation's growth is fuelled by the digital revolution, and the almost insatiable need across organisations for greater data storage capacity.

Technology disrupts the disruptors

There has been a massive shift in the way we use technology. However technology itself is a double edged sword, capable of delivering enormous business benefits, as well as destroying existing business models.

The obvious example is the way that buying and consuming books, music and videos has changed over the past decade. Stories of the many well-known, long-established businesses that closed their doors in response to this digital disruption, have become some of the best case studies in what not to do with an organisation when it comes to ignoring change.

Likewise, the impact of the digital camera, and the integration of that technology into smart phones, irreversibly changed the film camera business. With this technology reducing the marginal incremental cost of taking the next photo to zero, the number of photos taken and shared has exploded. The ability to share those photos digitally, has seen the number of photos being printed, plummet. In 1999, the year the film camera business peaked, Kodak estimated that around 80 billion photographs had been printed by consumers. In 2014, it is estimated that some 800 billion photos were shared on social media.

The organisations that will successfully navigate the digital age are those that are able to disrupt themselves and transform, taking advantage of new technologies as they arise. Those that lack the ability to cannibalise their own core business will fail, and some of the world's largest organisations will be among them.

To put it simply, when the core shifts, you also need to move.

Amazon: Continual transformation in action

There are also several stand-out companies that have done amazing things in leveraging technology and disruption. For example, Amazon. Not only did they build the world's largest book delivery platform, they then launched a book reader to digitally disrupt that leadership position. And it worked spectacularly. In the last two years, Amazon shipped more digital books than the number of physical books they shipped in the last decade.

This type of transformation shows how much potential we have to disrupt the globe through technology.

Building the backbone of the digital economy

The NEXTDC business, which could be described as providing hotels for computers, supports organisations ranging from some of the largest cloud computing providers (including Optus and Telstra), through to very small organisations that are looking to build advantage in this new hyper-connected world.

Driven by the phenomenal growth in data, the scale of cloud computing is enormous. Companies such as Amazon, Microsoft and Google are forecasting to spend in the order or $10-15 billion each this year alone — building massive cloud computing platforms globally.

Cloud computing is going to be — and has already proven to be — a massive disruptive force, providing the backbone for the digital economy. Part of that disruption is because the cloud assists business to be more agile. Today, even the smallest companies can get to market with nothing more than a credit card and a few thousand dollars, and have access to more computing power than we have had at any other time in our history.

The new revolution

The digital age can be seen as the beginning of the fourth industrial revolution. The disruptive nature of the applications, products and business models that a hyper-connected world enables, presents a real and ongoing threat to those who believe it's going to be business as usual — albeit just a bit faster.

Some of the disrupters, and the industries that are most vulnerable, include:

- **Commercial drone deliveries:** Unless regulatory issues intervene, this will happen and will be massively disruptive. They are already being piloted, and people are working on predictive modelling algorithms to cut delivery times by anticipating what buyers are going to buy before they buy it, and putting it into the air before the sale is even completed.
- **Gaming:** The next stage for gaming goes beyond the builders and players to involve watchers, creating a completely new spectator experience.
- **3D printing:** The opportunities of being able to print almost anything are literally endless, and put us on the cusp of being able to produce anything we want without having to leave the home. The downside? Prohibited items now become accessible — for example, printing synthetic drugs at home.
- **Mobile payments / wearable technologies:** Leaving the house without their mobile is now a bigger issue for most people than forgetting their wallet.
- **Virtual reality:** The commercial application of virtual reality (VR) is quite extraordinary — NEXTDC is currently building 3D virtual tours that will enable them to give customers a full walk through a facility before it's even built.
- **Personal wellness:** The success of Fitbit is not simply due to the functionality of the device, but also to the network of connections and partnerships that are embedded in its ecosystem.

- **Healthcare / Tricorder:** The quest to develop a portable wireless device that will accurately diagnose 13 health conditions and capture real-time vital health signs, independent of a health care worker or facility, could become a reality in the next twelve months. Imagine what that means to third world countries that don't have access to this type of healthcare.
- **The transport revolution:** The vision outlined by the founders of Lyft (the competitor to Uber) in their recently released paper, The Third Transportation Revolution, is that by 2021, a majority of rides on its network will be in autonomous vehicles. Already, Uber and Lyft are so convenient and cost-effective, that in many cities around the world people are rethinking the need to own a car. And the move to truly autonomous vehicles will bring even greater shifts, such as the opportunity to repurpose carparks. However it will also present threats, such as the change in demand this will create for automobile and accident insurance.
- **The internet of Things (IoT):** This is the biggest disruptor, as trillions of devices connect to the internet and create information, back it up, store it, and share it. Not only will we have more devices in the home, but the home will be able to connect and talk directly to the grid, changing the way we use power, including when we use it, and whether we use it directly or store it for later use. This more efficient use of power will happen automatically, through a combination of logic and machine learning. Each of these devices will become its own technology company, creating data, allowing it to be mined and sharing it online. The advancements we are going to make as a result of this are huge.

Can Moore's Law continue to hold true?

It is argued that Moore's Law (price performance doubles every 18 months), has to come to some physical end. However Craig Scroggie believes it will continue to be true and even accelerate.

"We are seeing a massive shift in technology occurring in a very short period of time. When we think of the huge amount of information being created as a result of this shift to the IoT, we are going from thousands of computers, to millions and billions of phones, and now to trillions of online sensors playing a part in every facet of our lives."

Ray Kurzweil, head of artificial intelligence at Google, has said that, "Technology goes beyond mere tool making; it is a process of creating ever more powerful technology using the tools from the previous round of innovation".

Mobile is growing faster than any other technology in history, and it's not going to slow down. In 2015, mobile data traffic grew by 74% to 3.7 exabytes per month.

In addition, there's a whole segment of the world that hasn't yet woken up and started to compete. And when they do, those billions of new entrepreneurs won't know what the client-server computing era even looked like. They will have missed the entire period of being tied to a desk, stuck in an office. Almost everything they do will be centred on mobile, and things will become even more disruptive.

Hyper–growth accelerates risk

More data has been created in the past two years than in the previous history of the human race, and it will only increase. However, this hyper-growth is accompanied by a substantial increase in risk.

Data retention, data breach and data sovereignty pose enormous problems and challenges to every organisation that operates in a connected world.

From a risk management perspective, a digital document policy is becoming an imperative. In framing this, one should consider:

1. A policy for cloud data location.
2. Employee education.
3. Individuals tasked on cloud data protocols.
4. An internal review committee.
5. Tools that enable data retrieval from obsolete systems.
6. A policy covering all electronic devices.
7. Objective third party review.
8. A plan for litigation or law enforcement action.

In a similar vein to Anthony Belfiore, Craig Scroggie warns that while it's important to be protected from external threats, the biggest risk is the people that are inside pretending to be someone they are not. Think Edward Snowden. And before him, Private Bradley Manning.

What's next?

The next wave of digital disruption could come from artificial intelligence (AI). On latest developments, AI is set to crack the Turing test within the next three years — which means that the machine response will be indistinguishable from a human response. What will that mean for the rules of risk?

Managing brand and reputational crisis in the age of disruption

John Morgan, President and CEO, Japan and Asia, of the highly regarded global public relations consulting firm, Hill + Knowlton Strategies, led this session with a detailed discussion on how social media, and the power of the smart phone have disrupted the traditional approach to reputation management. He was then joined by Craig Scroggie and Anthony Belfiore for a discussion on how they manage reputational risk within their own organisations, and what they consider to be some of the greatest challenges. The following are key points from John Morgan's presentation.

In numerous global and Australian risk surveys conducted by Aon, *Brand and Reputation* has constantly been ranked among the greatest threats to business. The universal concern for this issue was articulated by Craig Scroggie earlier in the day, when he nominated reputation as the number one risk that keeps him awake at night — in particular, the fear that NEXTDC could be subject to a data breach, such as the ones experienced by Sony and Yahoo. "Brand is ultimately the crown jewels — it's the number one thing we have to protect."

While cyber risk has raised the threat of organisations experiencing such reputation-damaging attacks, technology itself has changed the news cycle and the traditional approach to reputation management.

Why is brand and reputation such a risk concern?

For John Morgan, reputation is the number one risk because its effect on an organisation is unpredictable. "You can lose in the court of law and get fined, some people might be terminated and perhaps your insurance will need to make a payment. These all very predictable things. If you have well trained professionals you can put these things to rest and get on with business. However, if you lose in the court of public opinion, at the end of the day, trust is eroded. When you lose trust, things just don't happen. Whether you sell cars, insurance, coffee or whatever it might be, you may well be on your way to being out of business."

The public is now the newsmaker

In the past, if something unpleasant happened, you were usually the first to know. Then, various stakeholders such as government bodies, attorneys, insurance companies and others would become aware. After that, the details would spread to traditional media.

This was a very controlled situation. However today there's been a complete disruption. When a crisis happens, someone, or a collection of people, adopt the role of the citizen journalist and react to that crisis on social media. From there, it reaches two key audiences: traditional media and then you.

With the company now becoming the last to know, there is the danger that by the time you are aware of a situation, millions of people will have found out about it and formed their own (usually unfavourable) opinion.

The game has changed

With power shifting to the public, there have been four significant changes to the way news is now received:

1. **Speed:** Things happen instantly. If something unpleasant happens in your business today, it only takes one Facebook post or a tweet for that incident to be shared with many people.
2. **Transparency:** In this environment, customers demand to know what's going on — they expect to know more details than ever before. If they don't get what they want, they'll post about it and apply pressure.
3. **Noise:** With so many channels in which to express an opinion, there's a lot of noise. Those who scream the loudest are the ones that are heard.
4. **New media:** New media is pervasive across our society and like any technology, it is continuing to evolve.

Understanding the firepower of social media

The volume of conversations and content generated by social media is staggering:

- **Facebook:** 70 billion items of content shared each month.
- **Twitter:** 500 million tweets per day, 6,000 tweets every second.

And then there are LinkedIn, Pinterest, Instagram, SnapChat — and so many more.

Of even greater concern, nearly 80% of individuals who send a tweet about a specific brand or company, expect a response within an hour. And if they don't, they just keep tweeting. Eventually that is picked up by a social media channel and then a traditional media channel.

What separates the winners from the losers?

There are five crucial elements of an organisation's approach to reputation management that are essential to minimising the time something remains an issue in the public's mind, and the size of the balance sheet impact.

- **Preparation:** When you invest in your brand and understand what can potentially harm that brand, you are able to predict about 85% of what may happen. Preparation is crucial, as you don't have time to figure out how to extinguish the fire when the house is already burning down.
- **Leadership:** Leaders play a heightened role in today's environment. They not only have to navigate their way through the crisis, but be able to talk very persuasively to stakeholders — and anyone who's involved — to convince them about the steps being taken to manage this particular issue. This type of communication is not just the role of public relations people.
- **Action:** Actions need to be rapid, decisive and effective. Your leaders have to respond with lightning precision.
- **Communication:** To regain trust, communications also need to be well-coordinated and frequent. In addition to responding to something that has gone after your brand, you need to be willing to have two-way communication, such as through an effective call centre and ensuring there are enough people available to respond to emails. This is an investment in resources, but if you don't have that two-way communication, the public gets angry, and that anger spreads.
- **Sensitivity:** Social media unveils everything. If you don't communicate with a sense of compassion and purpose, social media will quickly go after you. There's a herd mentality and you'll be pointed at very firmly.

What does it mean for the C–Suite?

Here are some key points for executive management teams to consider when managing their brand during a crisis:

- **Be first:** When something bad happens it's always better — if possible — that you are the one that breaks the news. That doesn't mean going out with a tweet or Facebook post, but thinking about what is the most effective way for you to communicate the situation.
- **Be flexible:** For every plan we have, something else can happen, and you need to be able to change course. Fortunately, social media allows you to do that very quickly.
- **Be frequent, be timely:** Fifteen years ago your PR people would send out a press release. The negative news cycle would last from two to five days, and then go away. It just doesn't happen that way on social media.
- **Be transparent:** If you don't tell the news, someone else will tell it.
- **Be visible:** You don't just need to be doing the right thing, you also have to be visible. If your customers don't see you doing something about an unfortunate situation, they'll assume you're doing nothing.

PayPal case study: Risk and reward in a cashless society

The conference concluded with an international case study presented by Laura Langone, Senior Director, Global Risk Management and Insurance, PayPal.

As is custom with these types of case studies, we do not share or publish the content outside the conference room. However, those who attended gained valuable insights into how PayPal combines predictive analytics and machine learning with human oversight, to accurately and quickly reduce credit and fraud risk. It was also fascinating to hear Laura speak of the challenge to remain nimble and disruptive when operating in an environment that is as highly regulated as financial services.

The future ...

We sincerely thank the 2016 ARC keynote speakers, presenters and panellists for sharing their insights into the many facets of the risk revolution, a fast evolving revolution that is changing — and will continue to change — the way we do business or even make certain businesses obsolete.

With respect to the insurance industry, we see the following as some of the key action points that should be informing business strategies:

Embrace a creative culture

By nature, the insurance industry is extremely conservative, but developing products and services for the knowledge economy requires innovative thinking and an ability to imagine the future rather than rely solely on historical data from the past.

Listen and respond to clients' needs

The sharing economy demonstrates the value of developing a feedback loop or cultivating effective customer conversations, which in turn provides a better understanding of how to make existing products more relevant, or develop new ones to fit emerging needs.

Be more transparent

In a click and connect world, where smart phone apps are providing consumers with simple and effective ways to transact, it will become increasingly important to reduce industry jargon, complex policy wordings and cumbersome documentation.

Enhance the claims settlement experience

A cash flow transaction approach is needed, not a complex and onerous process. The power of social media means that those who don't provide a seamless process or unnecessarily delay the payment of claims will quickly be vilified.

CORP0087E 1116