

Strategic RISK

Risk and corporate governance intelligence

- › HOW TO TACKLE CYBER ESPIONAGE
- › BENCHMARKING SURVEY RESULTS: HOW HAS OUR FOCUS CHANGED?
- › THE DUO BEHIND CYNCH SECURITY
- › SPECIAL REPORT: FUTURE RISKS
- › THE MALEVOLENT SHADOW VALUES BUSINESSES TRY TO KEEP HIDDEN


ASIA PACIFIC EDITION [Q4] 2019 | Issue 26 US\$25



CAUTION: BEAR SIGHTED

The next recession could be just around the corner. What can risk managers do to prevent their organisations getting mauled? >



 Insurance



Think globally

When the world is your oyster, you need a partner to help handle the complexities of global risks. With over 30 years of network management experience, 5000 global programs in our care, and serving clients in more than 200 countries, our scope and scale can help your business reach further.

Know You Can

axaxl.com

AXA XL is a division of AXA Group providing products and services through four business groups: AXA XL Insurance, AXA XL Reinsurance, AXA XL Art & Lifestyle and AXA XL Risk Consulting. AXA, the AXA and XL logos are trademarks of AXA SA or its affiliates. © 2019 AXA SA or its affiliates.

Q4 2019
ASIA PACIFIC EDITION

StrategicRISK

www.strategicrisk-asiapacific.com

EDITOR

Lauren Gow

PUBLISHER

Adam Jordan

HEAD OF EVENTS

Debbie Kidman

MANAGING DIRECTOR

Tim Potter

HEAD OF FINANCE

Paul Carey

DESIGNER & SUB-EDITOR

Laura Sharp

email: firstname.surname@nqsm.com

ISSN 2517-5734

PUBLISHED BY

Newsquest Specialist Media Limited,
registered in England & Wales with
number 02231405 at Loudwater Mill,
Station Road, High Wycombe HP10 9TY –
a Gannett company

SUBSCRIPTIONS

StrategicRISK Subscriptions Department
21 Southampton Row, London,
WC1B 5HA
email: customerservices@
strategicrisk-asiapacific.com
tel: +44 (0)20 8955 7015

tel: +44 (0)20 7618 3456

fax: +44 (0)20 7618 3420

email: strategic.risk@nqsm.com

For all subscription enquiries please
contact: william.sanders@nqsm.com

Printed by Warners Midlands Pl
© Newsquest Specialist Media Ltd 2019

Contents

LEADER > P2

KEEP CALM AND... MOVE ON?

When best-laid plans, and risk assessments, are torn apart by change, the best risk managers know how to adapt and keep moving.

VIEWPOINTS > P4

CYBER ESPIONAGE: THE INSURANCE IS NOT ENOUGH

It's the most devastating form of cyber crime, but don't assume your policy will cover it.

WHY DO PROJECTS FAIL?

Our focus must change if we want to guide our companies to take projects over the finishing line.

DIRECTORS BEWARE

These five mega trends could spell trouble for corporate management in 2020 and beyond.

AUSTRALIA'S GREEN SCENE

The logistics behind booming renewable energy growth require a specialist understanding.

SURVEY > P10

HOW'S IT GOING?

Our 2019 Benchmarking Risk Survey asked the industry – what are your biggest fears and focuses for the coming year?

PROFILE > P18

THE DREAM TEAM

Starting up is never easy. But Cynch Security's Susie Jones and Adam Selwood had faith that they were onto a winner.

Survey's in. What's changed for you? > P10

RISKS > P22

COVER: ON A BEAR HUNT

Some say they hear the snarls of a recession approaching. Do risk managers have the power to protect their businesses?

SPECIAL REPORT > P26

KEEP PACE WITH CONNECTIVITY

The Internet of Things is changing everything. But this new world of risk is keeping us on our toes.

IS 3D PRINTING DANGEROUS?

Companies can not be complacent about possible worker health threats from this revolutionary tech.

STAYING AS SMART AS 5G

How insurers must actively assess and adapt to this changing landscape.

REPORT > P30

REVEALING MR HYDE

The official values say one thing, the murky and immoral shadow values say something else. How can risk managers tackle a malevolent alter ego?

COMPLAINTS – WHO TO CONTACT

StrategicRISK adheres to the Editors' Code of Practice (which you can find at www.ipso.co.uk).

We are regulated by the Independent Press Standards Organisation.

Complaints about stories should be referred firstly to the editor-in-chief by email at: complaints@strategic-risk-global.com or by post at StrategicRISK, 120 Leman Street, London, E1 8EU, UK.

It is essential that your email or letter is headed "Complaint" in the subject line and contains the following information:

- Your name, email address, postal address and daytime telephone number.
- The newspaper title or website, preferably a copy of the story or at least the date, page number or website address of the article and any headline.
- A full explanation of your complaint by reference to the Editors' Code.

If you do not provide any of the information above this may delay or prevent us dealing with your complaint. Your personal details will only be used for administration purposes.

If we cannot reach a resolution between us then you can contact IPSO by email at complaints@ipso.co.uk or by post at IPSO, c/o Halton House, 20-23 Holborn, London EC1N 2JD.

Keep calm and... move on?

As a risk manager, you aim to think inside and outside of every box. But we all know what they say about best-laid plans. What defines us is how quickly and smartly we adapt to inevitable changes. So here's to another year of thinking on our feet. See you there!



EMAIL > lauren.gow@nqsm.com

It has been two years since I took the reins of the editorship for *StrategicRISK* in Asia Pacific. As I wrote my first leader in late 2017, perched atop a tea chest filled with books and DVDs, my walls covered from top to bottom with to-do lists and enough paperwork to overwhelm even the most seasoned auditor, the aim was to get my two-legged and four-legged family and a decade's worth of possessions from London to Sydney, and make the Australia city our forever home.

I had 'The Big Move' perfectly planned and under control. What could possibly go wrong?

As I write this leader, I am preparing to do this whole move in reverse. Yes, you read that correctly: just two years later, I am once again preparing to move my entire two-legged and four-legged family (the original three dogs, plus an extra large rescue dog with a dubious penchant for eating socks and rugs, and an additional two cats) now from Sydney back to London. You might be wondering if I have genuinely lost my mind.

In truth, it was those darned plans going astray. Despite holding more than a decade of international commodities trading experience, my husband was unable to find work in his industry in Sydney. You see, we planned every aspect of my job, my son's schooling, two home rentals (London and Sydney), banking, all those pets, you name it – I planned and executed everything to perfection.

Unfortunately, what I could not plan for, and what was entirely beyond my control, was the lack of commodities trading in Sydney. The irony that Australia is known globally for its mining and

commodities but has virtually no local commodities trading is not lost on me.

He is now happily employed with an Australian bank in a London-based risk management role (I know, more irony) and we are once again packing up and moving on.

What has been the most curious part of all of this is the reactions when telling people we are again moving. We have been met with repeated cries: "But that wasn't the plan!" and "Why did you move all the way there if you are just going to move back?"

Well that, my readers, is something we can all learn from, but is something you likely already understand well. You can make all the plans in the world. You can risk register, heat map, evaluate, mitigate, manage, Bow-Tie analyse, Monte Carlo scenario yourselves until your fingers bleed, but that may not stop fate intervening in the most inconvenient way possible, throwing all your predictions and plans to the wind.

What will define you as a risk manager is how you handle the situation when things don't go to plan. Moreover, what will mark you as an excellent risk manager is your ability to take repeated changes of plans and still stay calm.

Ralph Ellison wrote in his modern parable novel *The Invisible Man*: "Life is to be lived, not controlled; and humanity is won by continuing to play in face of certain defeat." When control is lost to fate, fortune hands you an opportunity to make a new plan.

Whether that plan is what you had in mind is uncertain but, for me, embracing life in the UK once more will give me a chance to make new plans. Maybe even ones that stick this time.

"YOU CAN MITIGATE AND MANAGE UNTIL YOUR FINGERS BLEED, BUT THAT MAY NOT STOP FATE INTERVENING IN THE MOST INCONVENIENT WAY POSSIBLE, THROWING ALL YOUR PREDICTIONS AND PLANS TO THE WIND."



Commercial Insurance

Construction & Engineering

General Casualty

General Property

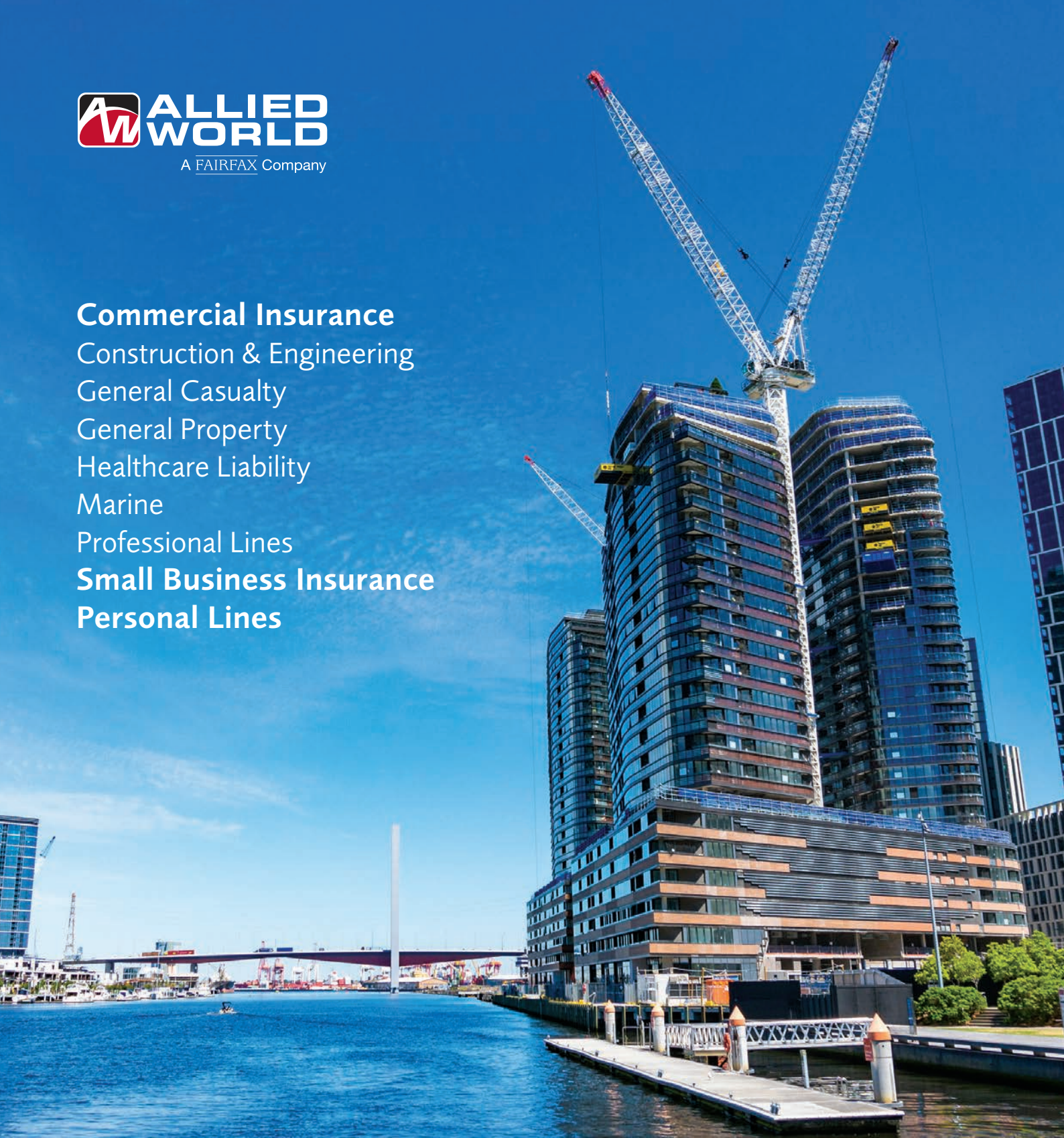
Healthcare Liability

Marine

Professional Lines

Small Business Insurance

Personal Lines



ABOUT ALLIED WORLD

26 Global Re/Insurance Divisions

21 Offices Worldwide

37,000+ Clients

Over 50 Claims Handlers Across Asia-Pacific

www.alliedworldinsurance.com

This information is provided as a general overview for agents and brokers. Allied World Assurance Company, Ltd is incorporated in Bermuda with limited liability. Coverage will be underwritten by the Hong Kong branch office of Allied World Assurance Company, Ltd, which is regulated by the Insurance Authority, the Singapore branch office of Allied World Assurance Company, Ltd, which is regulated by the Monetary Authority of Singapore, the Australia branch office of Allied World Assurance Company, Ltd, or by our Lloyd's Syndicate 2232, as applicable. Syndicate 2232 is managed by Allied World Syndicate Services (Singapore) Pte. Ltd., which is regulated by the Monetary Authority of Singapore. Coverage is only offered subject to local regulatory requirements and through licensed agents and brokers. Actual coverage is subject to the terms, conditions and exclusions of the actual policy issued.
© 2019 Allied World Assurance Company Holdings, Ltd, a Fairfax company. All rights reserved.

Cyber espionage: The insurance is not enough

Many companies don't know that the cyber insurance policies they rely on won't be able to mitigate or manage the most catastrophic cyber crime of all – cyber espionage – says EverEdge's Paul Adams.

Inga Beale, former CEO of Lloyd's, recently remarked: "Today, a company's most valuable assets are more likely to be stored in the cloud than a warehouse." It seems the insurance sector is finally waking up to the fact that intangible assets are the most valuable assets modern companies own – which is something that cyber criminals unfortunately figured out long ago.

According to estimates by Cybersecurity Ventures, cyber crime will cost the global economy more than \$6 trillion in 2021, up from \$3 trillion in 2015. But, while most companies now recognise that cyber crime is a major issue, many senior managers and boards are focusing their attention on the wrong kinds of cyber damage. Damage from cyber crime breaks down into four broad categories:

- Financial theft: Manipulation of systems to misdirect funds, e.g., an illegal bank transfer
- Extortion: Withholding access to or damaging systems to extort payments, e.g., ransomware
- Vandalism: Damage to systems or leaking data with no apparent financial motive, e.g., the Sony hack
- Cyber espionage: Theft of intangible assets to be used or sold

Unfortunately, while most cyber insurance policies generally cover an organisation for theft, extortion and direct loss (such as system repair and downtime) associated with vandalism (1 through 3 of the above list), many companies do not realise that their policies do little against cyber espionage.

UNDERSTAND THE THREAT

Cyber espionage includes the theft of confidential information such as algorithms, ingredients and formulas, manufacturing trade secrets and processes, product designs, bills of material, customer, supplier and employee data, pricing information and strategic business and financial information. In short, it is about your most valuable assets – your intangible ones.

The scale of intangible asset theft is huge: in 2019,

the Commission on the Theft of American Intellectual Property estimated that the theft of American intellectual property by Chinese entities alone currently costs the economy \$225–\$600 billion annually. In Singapore, it is estimated that cyber crime now accounts for 19% of the country's overall crime.

In the 'Second Annual Study on the Cybersecurity Risk to Knowledge Assets' released earlier this year by Kilpatrick Townsend & Stockton and the Ponemon Institute, 634 North American companies were surveyed about their approach to cyber risks to their "knowledge assets".

The results were stark – revealing that cyber theft is rampant and is an increasing threat, with 82% (up from 74% in 2016) reported it is likely that their company failed to detect a loss or theft of knowledge assets. Some 65% (up from 60% in 2016) stated it is likely one or more of their company's knowledge assets are now in the hands of a competitor.

The average total cost incurred by organisations included in the research due to the loss, misuse or theft of knowledge assets over the past 12 months increased 26% from \$5.4 million to \$6.8 million.

A majority of 84% of respondents stated that the maximum loss their organisations could experience as a result of a material breach of knowledge assets is greater than \$100 million (compared to 67% of respondents in 2016). The study showed that executives and boards aren't focused on the issue and its resolution. Over 65% rate their approach to the problem as 'not effective' and cite lack of in-house expertise (73%) and lack of clear leadership (55%) for this.

But 50% felt that senior management is more concerned about a data breach involving credit card information or customer information than the leaking of knowledge assets. Only 35% say their companies' senior management understands the risk caused by unprotected knowledge assets. Two-thirds (65%) believe that senior management does not make the protection of knowledge assets a priority.

The board of directors is even worse off: only 31% say the board is made aware of all breaches involving the loss or theft of knowledge assets. Just 44% indicated that the board asked for assurances that knowledge assets are managed and safeguarded appropriately.

WHY PREVENTION IS CRITICAL

Cyber espionage has the potential to cause catastrophic damage than can be far more destructive than financial theft, extortion or vandalism.

It directly and systematically degrades the long-term competitive edge of a company and transfers it to

"IF SOMEONE IS ABLE TO STEAL YOUR INTANGIBLE ASSETS AND MARKET THEM UNDER THEIR OWN BANNER, THEN WHY WOULD THEY INVEST IN DEVELOPING THE PRODUCT OR SERVICE THEMSELVES?"

CEO, EverEdge
Paul Adams

competitors. Companies expend substantial resources to develop a competitive edge. However, if a cyber criminal comes along and steals the intangible assets that give the company its advantage, the thief will enjoy the advantage for free (i.e., the victim pays 20% for its advantage, the thief gains 20% – a net 40% shift).

Paying a false invoice of \$50,000 is bad but a 20% net shift in margin in a large company can be catastrophic. According to Kilpatrick et al, the average direct cost to remediate attacks against knowledge assets has risen to \$6.8 million (up from 5.4 million a year ago) but 84% of respondents said that the real cost for such attacks is more likely to top \$100 million.

Over the long term, cyber espionage corrodes the incentive to develop new products. After all, ‘why buy the cow if you can get the milk for free’. If someone is able to steal your intangible assets and market them under their own banner, then why would they invest in developing the product or service themselves?

Writing in the *Harvard Business Review*, Erik Meyerson found that even prior to the advent of cyber risk, the theft of intangible assets from West German companies by East German interests substantially narrowed the productivity gap between East and West Germany and “was so successful it crowded out standard forms of R&D in the West”.

Add to this the fact that damage associated with intangible asset theft is frequently uninsurable. The damage from cyber espionage can potentially run for years and have far-reaching consequences, making it difficult for an insurance provider to identify the quantum of damage (and thus be unable to pay out).

Interestingly, insurance is also unlikely to cover indirect loss associated with a hack, such as damage to brand reputation (another form of intangible asset). Again this is likely to be because it is difficult (though not impossible) to value the extent of the damage.

This is not to say boards should not consider taking out insurance against cyber risk. Cyber risk should absolutely be evaluated and where appropriate insured against, as is the case with any risk. However, companies that take out cyber insurance should carefully check their policies to determine if cyber espionage is really covered and to what extent.

It’s worth noting here that no company is immune to cyber crime. At the big end of town, Huawei estimates that it endures around a million cyber attacks a day on its computers and networks; while at the smaller end, Accenture estimates that 43% of cyber attacks are now aimed at small businesses.

A PLAN OF ACTION

So what can companies do to mitigate risk around cyber espionage? While there is plenty of evidence around why cyber espionage is a growing concern, many companies are still at a loss regarding what to do.

Beyond having a cyber security system in place to prevent, monitor and contain breaches effectively, there are a number of other steps that companies can take to minimize the risk of cyber espionage.

Identify your intangible assets

The first step is to identify your intangible assets, along with which of these assets are truly critical and



which ones are not. Once you’ve identified which assets drive your competitive edge, you can take steps to ensure that these don’t leak outside of the company and are protected from cyber attacks.

Institute policies and processes

According to Kilpatrick et al, only 14% of those companies surveyed restricted access to their knowledge assets, with 61% of respondents also stating that third parties have access to their company’s knowledge assets. With the majority of data breaches resulting from the carelessness of employees or third parties with access to information, it is important that companies institute policies and processes to proactively identify, protect and monitor access to key trade secrets and critical confidential information.

Educate and create employee awareness

It is also important to educate employees on the importance and value of confidential information as a strategic asset for the company. Ensure employees understand the policies and processes in place and the steps that they can take to minimise the risk of confidential information and knowledge assets leaking or being targeted outside of the organisation.

GET SERIOUS

Intangible assets now account for 87% of all company value. They frequently comprise a company’s most valuable assets – would you rather a competitor steals a company car or your customer database?

It is essential that senior managers and boards of directors don’t fall into the trap of believing “we have a cyber insurance policy so that’s a tick for cyber”. Companies need to take the risk of theft of their most valuable assets, their intangible assets, far more seriously than previously.

“THE DAMAGE FROM CYBER ESPIONAGE CAN HAVE FAR-REACHING CONSEQUENCES, MAKING IT DIFFICULT FOR AN INSURANCE PROVIDER TO IDENTIFY THE QUANTUM OF DAMAGE.”

CEO, EverEdge
Paul Adams

Why do projects fail?

It comes down to helping managers manage, and make decisions, by honing in on real business impacts and goals. AKTUS' Hans Læssøe explains how risk managers can guide their companies to hit more targets.

Analysis of a portfolio of projects often reveals that many projects fail to meet deadlines, as well as other targets. One company I am in contact with have just had a good year as “only” 53% of their projects were more than 10% over time and budget.

Working on a range of different projects over several years, I have found five common reasons projects fail. The bad news is that these are not new, yet they prevail to this day. The good news is that organisations can opt to leverage their risk management teams and rectify/improve on these without having to bend over backwards to improve performance.

FAIL #1

DESIRED GOALS NOT DEFINED

In many projects, the target is defined based on doing something, rather than achieving something

– “to install IT system X by Y within a budget of Z”. Now, this may be a good idea, but it is not a target in its own right. There is a reason you want the IT system, and that reason may be the achievement. So your target should be something like: “we wish to reduce costs of process P by Q% by installing system X by Y at the cost of Z”.

HOW TO FIX IT

Targets drive decisions, and hence project managers should push back and ask questions until they are certain they know and understand the “real” target – and how to measure this.

FAIL #2

YOU'RE TOO RISK FOCUSED

Whatever actions are taken on managing risks are focused exclusively on managing risks – without any consideration as to how that may impact the

“ORGANISATIONS CANNOT REALISTICALLY AVOID TAKING RISKS – DO TAKE RISKS, BUT TAKE THEM INTELLIGENTLY, LEVERAGING THE VALUE DECISION OF RISK MANAGEMENT.”

Founder, AKTUS
Hans Læssøe

overall project or business performance. When that happens, some risks may appear very important, and a lot of effort and resources are spent on minimising these – despite the fact that even if they materialise, they will not have any significant impact on project/business performance.

I have seen numerous times where project deadlines were rigorously adhered to, in some cases by reducing scope/value of the project, and where the business impact of a delayed implementation would have been



minuscule. I have also seen projects where delivery on time was absolutely pivotal, and even a 100% budget overrun was acceptable to avoid 10 weeks of delay.

HOW TO FIX IT:

Risks should be addressed based on their impact on meeting objectives/targets and based on intelligent risk taking. Organisations cannot realistically avoid taking risks – do take risks, but take them intelligently, leveraging the value decision of risk management.

FAIL #3

RISKS NOT FULLY IDENTIFIED

This goes for risks irrespective of whether their impact on performance is negative or positive – it covers risks and opportunities alike. The identification tends to be based on tunnel vision, not considering the business system of whatever the project addresses. Some of these may be irrelevant to any one project – but use this as a checklist and be open-minded.

HOW TO FIX IT

Ensure risks (positive as well as negative) are holistically identified, by liaising with those affected by whatever the project is working on. Leverage the insights of specialists around the company. Some may not have anything, leading to a 10-minute touch base, others may have something helpful to add, and it will add to the quality of project planning and management.

FAIL #4

DISTRIBUTIONS ARE SKEWED

When analysing/assessing each risk, qualitative assessments such as high/medium/low or minor/significant/catastrophic are often used. These are essentially useless as they do not help any decision making or handling.

Furthermore, most risks are traditionally quantified using a single-point estimate. “If risk A materialises, it will have an impact of B.” Well, yes or something less, or more likely, something more. Single-point estimates do have a ring of authenticity around them, but they are not much more valuable than a qualitative assessment.

The problem is, if you assume a risk has an impact of 100, you inherently assume the distribution around this is bell-shaped whereby the average outcome will be 100, and also assume the likelihood of 50 is as high as that of 150.

Unfortunately, this is not true in real life, where impact distributions are skewed, and more likely look like a curve, where the most likely value is smaller than the median (50/50 case). The average impact is higher than the median. And the 10% worst case, which does happen from time to time, is much larger – often more

than twice the most likely value. If you are in charge of managing a project, and just one risk materialises with an impact more than twice what you expected – you are suddenly unlikely to meet your target.

HOW TO FIX IT:

Systematically analyse risks using data and facts to avoid the optimism and other biases people exercise, when assessing risks. If you cannot, challenge the quantitative assessments you get from subject matter experts. Then, insist that all assessments are based on three-point estimates enabling long tails when needed.

FAIL #5

PERFORMANCE EXPOSURE NOT CALCULATED

Traditional, and alas still common, risk management reports outcomes in terms of risk matrices or heat maps. These are useless on a good day, and even dangerous on a bad day.

Even the best-derived risk matrix/heat map will not tell you anything about whether or not you will meet your targets – which is probably the reason so few managers are truly interested in risk management. It does not help them in their decision making and management. Risk management is NOT about managing risks, but ALL about enhancing performance and thereby meeting (or exceeding) targets.

This means that we do need to take risks, but also, that this must be done intelligently. Please note that this means we take mitigating actions as deliberate means to enhance expected project/business performance, not as a means to manage risks.

HOW TO FIX IT:

Model your project using Monte Carlo simulation. Apply ranges to project assumptions and add risks (negative as well as positive) to the modelling. Simulate e.g., 10,000 times and address the outcome. You will be able to show: What is the likelihood targets will be met? What is 10% worst-case/the average/10% best-case outcome? Which are the key drivers of uncertainty to these results?

This insight will help management manage. They can address whether or not they are ‘happy’ with the calculated likelihood of meeting targets. In fact, this is their application of the concept of risk tolerance, but you do not have to tell them that. They are also helped to address key uncertainties, and ask for/drive further actions to enhance expected performance to an acceptable level.

Focus your risk management efforts on intelligent risk taking and help project managers to develop and work with plans that are adequately likely to deliver on realistic targets.

Be proactive and collaborative. Liaise with those involved in projects, offer your insights and support – and add true value to your organisation.

“RISK MANAGEMENT IS NOT ABOUT MANAGING RISKS, BUT ALL ABOUT ENHANCING PERFORMANCE AND THEREBY MEETING (OR EXCEEDING) TARGETS.”

Founder, AKTUS
Hans Læssøe

Directors beware

With corporate management under scrutiny like never before, a new report calls out five mega trends that will have significant risk implications for senior management in 2020.

The range of risks facing executives, directors and officers – and the resultant insurance claims scenarios – has increased greatly in recent years. With corporate management under the spotlight like never before, a new report by insurer Allianz Global Corporate & Specialty (AGCS) highlights five big trends that could spell trouble for the c-suite.

1 MORE LITIGATION COMING FROM 'BAD NEWS'

Bad news events, like product failures, man-made disasters and cyber attacks, are dominating the business press agenda, and when things go wrong it can cause drops in share price or regulatory investigations, which in turn be bad news for senior management.

This often results in significant securities or derivative claims from shareholders. Of the top 100 US securities fraud settlements ever, 59% are event-driven. There has also been a spike in claims resulting from the #MeToo movement, where it is alleged D&Os allowed a toxic culture to endure in companies.

Another concern is cyber. AGCS has seen a number of securities class actions, derivative actions and regulatory investigations, including from the EU's GDPR, in the last year, and expects more in 2020. "AGCS continues to see more claims against D&Os emanating from 'bad news' events not necessarily related to financial results," says Shanil Williams, global head of financial lines at AGCS. "Scenarios include product problems, man-made disasters, environmental disasters, corruption and cyber attacks."

2 CLIMATE CHANGE LITIGATION ON THE RISE

Failure to disclose climate change risks will be more likely to result in litigation in the future. Climate change cases have already been brought in at least 28 countries around the world to date. More and more cases are alleging that companies have failed to adjust business practices in line with changing climate conditions.

Environmental, social and governance (ESG) failings can cause brand values to plummet. "Directors will be held responsible for how ESG issues and climate change are addressed at a corporate level," says Williams. "Increasingly, they will have to consider the impact of these when looking at strategy, governance, risk management and financial reporting."

"AGCS CONTINUES TO SEE MORE CLAIMS AGAINST D&OS EMANATING FROM 'BAD NEWS' EVENTS NOT NECESSARILY RELATED TO FINANCIAL RESULTS."

Global head of financial lines, AGCS
Shanil Williams

3 GROWTH OF SECURITIES CLASS ACTIONS GLOBALLY

AGCS has seen increasing receptivity of governments around the world to collective redress and class actions, particularly across Europe, but also in territories like Thailand and Saudi Arabia.

At the same time, the level of filing activity in the US has been at record highs in recent years, with over 400 filings in both 2017 and 2018, almost double the average of the preceding two decades. This increased activity is impacting both US and foreign companies that have securities listed directly in the US.

With global law firm Clyde & Co, AGCS has compiled a risk map in its report that assesses the risk of a company being subject to a securities group action in a particular jurisdiction. This risk analysis takes into account the availability and prevalence of third-party litigation funding, which is regarded as a strong factor in increased group action activity around the globe.

While countries such as the US, Canada and Australia see the highest activity and most developed securities class action mechanisms, these are developing and strengthening around the world. The Netherlands, Germany, England and Wales have all shown notable development and increased activity in recent years.

4 BANKRUPTCIES AND POLITICAL CHALLENGES IMPACT

An increased number of insolvencies could translate into more D&O claims. Business insolvencies rose in 2018 by more than 10% year-on-year, owing to a sharp surge of over 60% in China. In 2019, business failures are set to rise for the third consecutive year by more than 6% year-on-year, with two out of three countries poised to post higher numbers of insolvencies than in 2018.

"Political challenges, including elections, Brexit and trade wars, could create the need for risk planning for boards, including revisiting currency strategy, M&A planning and supply chain, and sourcing decisions based on tariffs. Poor decision-making may also result in claims from stakeholders," says Williams.

5 LITIGATION FUNDERS GONE GLOBAL

All of these trends are further fuelled by litigation funding now becoming a global investment class, attracting investors searching for higher returns.

Litigation funding reduces many of the entrance cost barriers for individuals wanting to seek compensation, although there is much debate around the remuneration model of this business. Recently, many of the largest litigation funders have set up in Europe. Although the US accounts for roughly 40% of the market, followed by Australia and the UK, other areas are opening up, such as recent authorisations for litigation funding for arbitration cases in Singapore and Hong Kong. India and parts of the Middle East are predicted to be future hotspots.



Australia's green scene

A renewable energy boom is bringing new challenges and risks. Enter the insurance risk engineer – making smooth sailing of the most complex, remote projects.

Australia's renewable energy market is currently experiencing the highest pace of renewable energy changes of any country in the world. This may come as no surprise from this sea-bound island that boasts vast open deserts, relentless sunshine and high winds.

The figures speak for themselves. Australia produced 378.7 PJ of overall renewable energy (including renewable electricity) in 2018, which accounted for 6.2% of Australia's total energy use (6,146 PJ), according to the Climate Council. Renewable energy grew by an annual average of 3.2% in the ten years between 2007–2017 and by 5.2% in 2016–2017.

This increased focus on renewable energy brings with it many logistical challenges, and so, many challenges to risk management. The national or international transportation of large, heavy, often high-value pieces of equipment to the project site is expensive and complex.

SUPERSIZED PROJECTS

To use any form of natural power successfully, you need a good site – of which Australia has many. More often than not, a renewable project will be located in a remote area. It is at this point that logistics becomes key. Shipping gigantic wind turbines from factories in India or China to some of the most remote places in the world is a colossal effort. Faced with population booms, increasing urbanisation and stretched power supplies, a well-engineered renewable energy system can be a cost-effective mechanism and significantly improve the quality of life in remote areas.

But building a renewable energy plant requires a huge network, including manufacturing, distribution, transportation and construction, which is where the risks begin to escalate. As well as the remote locations of plants and shipping of enormous parts from other parts of the world, the actual turbines themselves and the associated technology have become larger and more complex with each iteration.

In January, wind turbines were unveiled that were nearly the length of a football pitch. These colossal turbines will not be on the market for three years, but when they are, the 94-metre-long blades promise to boost electricity by up to 30%. With this supersizing

of components comes the supersizing of the supplies needed to transport and install these beasts.

SMOOTH OPERATORS NEEDED

Some of the logistics risks needing to be identified ahead of a project include site access, turning circles for logistics vehicles, organising cranes at site to lift the blades into place... the list goes on. Add to this providing appropriate accommodation facilities to attract and retain the many specialist staff required to not only install these power sources but to provide ongoing maintenance, and we have a huge number of factors at play in the detailed planning and implementation of a complex operation.

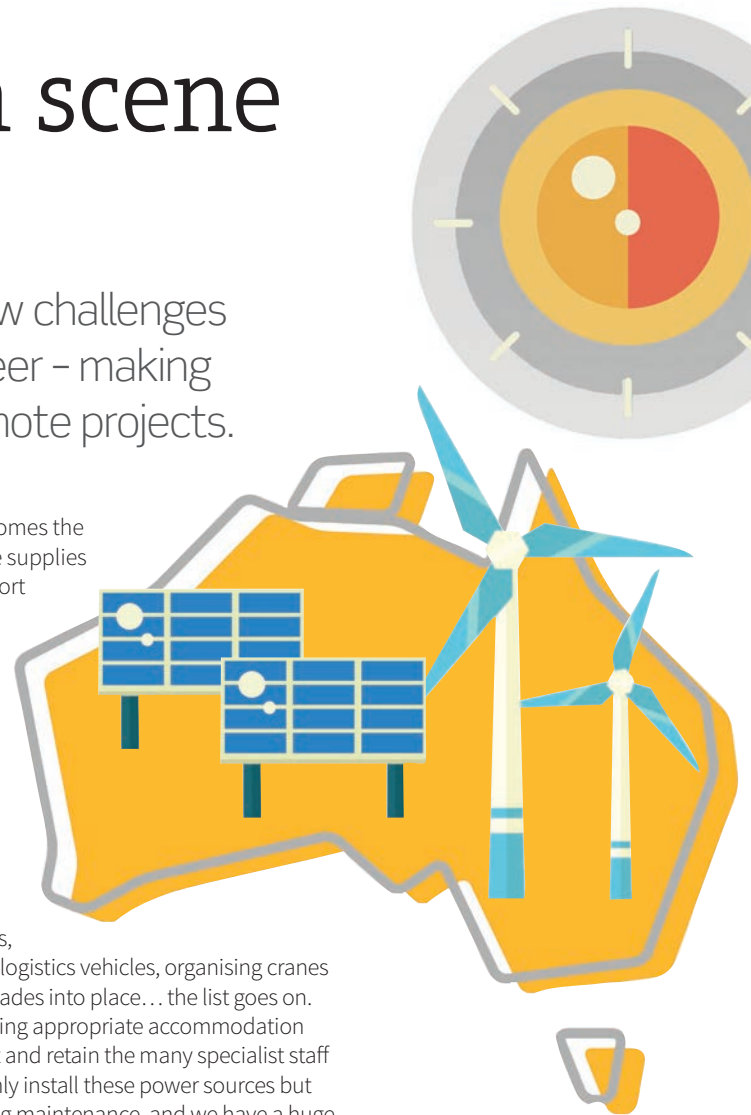
Allied World has overseen projects where trees have been cut down, bridges strengthened and electric cables rerouted to allow equipment to be moved to a site. This is no easy feat in a country where there can be 1000km between towns and just a service station for fuel.

Making light work of your logistics project is achievable if you choose the right provider. Allied World looks at all elements of an energy project to create the correct logistical solution. Its team of underwriters, risk engineers and claims handlers are located in Asia-Pacific – helping them to remain close to partners, clients and renewable energy assets.

POWERING THE FUTURE

Creating wind farms is an immensely complicated task, but with the right logistical planning, even the most challenging project can be successfully delivered.

In 2017, 17 countries generated more than 90% of their electricity with renewable energy. Despite having world-class solar and wind resources, Australia was not one of them. Only 15% of Australia's power comes from renewable energy sources like solar, wind and hydro, meaning we have a long way to go before we can label ourselves as truly world class. Well-managed logistics will be absolutely key to success.





How's it going?

In our 2019 Survey, we took a dive into Asia-Pacific risk managers' greatest concerns and what tops your to-do lists for the coming year. With more reporting increased risk engagement and team size, the stage is set for real progress in 2020. Your priority number #1? Risk culture.

In partnership with



TOP TEN: RISKS OF GREATEST CONCERN

Comparing this and last year's responses, supply chain risk no longer makes the cut, replaced in the top 10 by project failure or delay.

2018

- 1 **STRATEGIC:** Increasing/changing competitive landscape
- 2 **EXTERNAL:** Macroeconomic change (trade wars, tariffs, currency, interest rates)
- 3 **PREVENTABLE:** Targeted cyber attack
- 4 **EXTERNAL:** Economic slowdown/slow recovery
- 5 **STRATEGIC:** Failure to innovate
- 6 **EXTERNAL:** Change to regulation
- 7 **PREVENTABLE:** Maintaining a talented workforce
- 8 **PREVENTABLE:** Failure of critical infrastructure
- 9 **STRATEGIC:** Damage to company reputation/brand
- 10 **OUT for 2019 PREVENTABLE:** Supply chain risk

2019

- 1 **EXTERNAL:** Economic slowdown/slow recovery
- 2 **EXTERNAL:** Macroeconomic change (trade wars, tariffs, currency, interest rates)
- 3 **NEW to 2019 PREVENTABLE:** Project failure or delay
- 4 **STRATEGIC:** Increasing/changing competitive landscape
- 5 **PREVENTABLE:** Targeted cyber attack
- 6 **EXTERNAL:** Change to regulation
- 7 **PREVENTABLE:** Failure of critical infrastructure
- 8 **STRATEGIC:** Failure to innovate
- 9 **PREVENTABLE:** Maintaining a talented workforce

Welcome to the 2019 *StrategicRISK* Asia-Pacific Risk Benchmarking Survey. As you will see, this year's results show an increasing maturity in many areas of risk management in the region.

Risk culture was identified as the number one focus for risk managers over the coming year, reflecting greater understanding of the impact it has on risk management within organisations. It is up to you to spread the word and foster awareness.

Another area of note is the change in top risk rankings. The results show that non-strategic areas are now outranking other areas of focus, with the top strategic level risk – the changing competitive landscape – being bumped from the number one spot last year to fourth place in 2019. External risks – economic and macroeconomic fears – rose to the top of the list.

It is hardly surprising that technology risks are ranked some of the highest concerns for risk managers in the region. However, the low ranking of climate change is surprising given the current increased global focus on this risk area, particularly from younger generations.

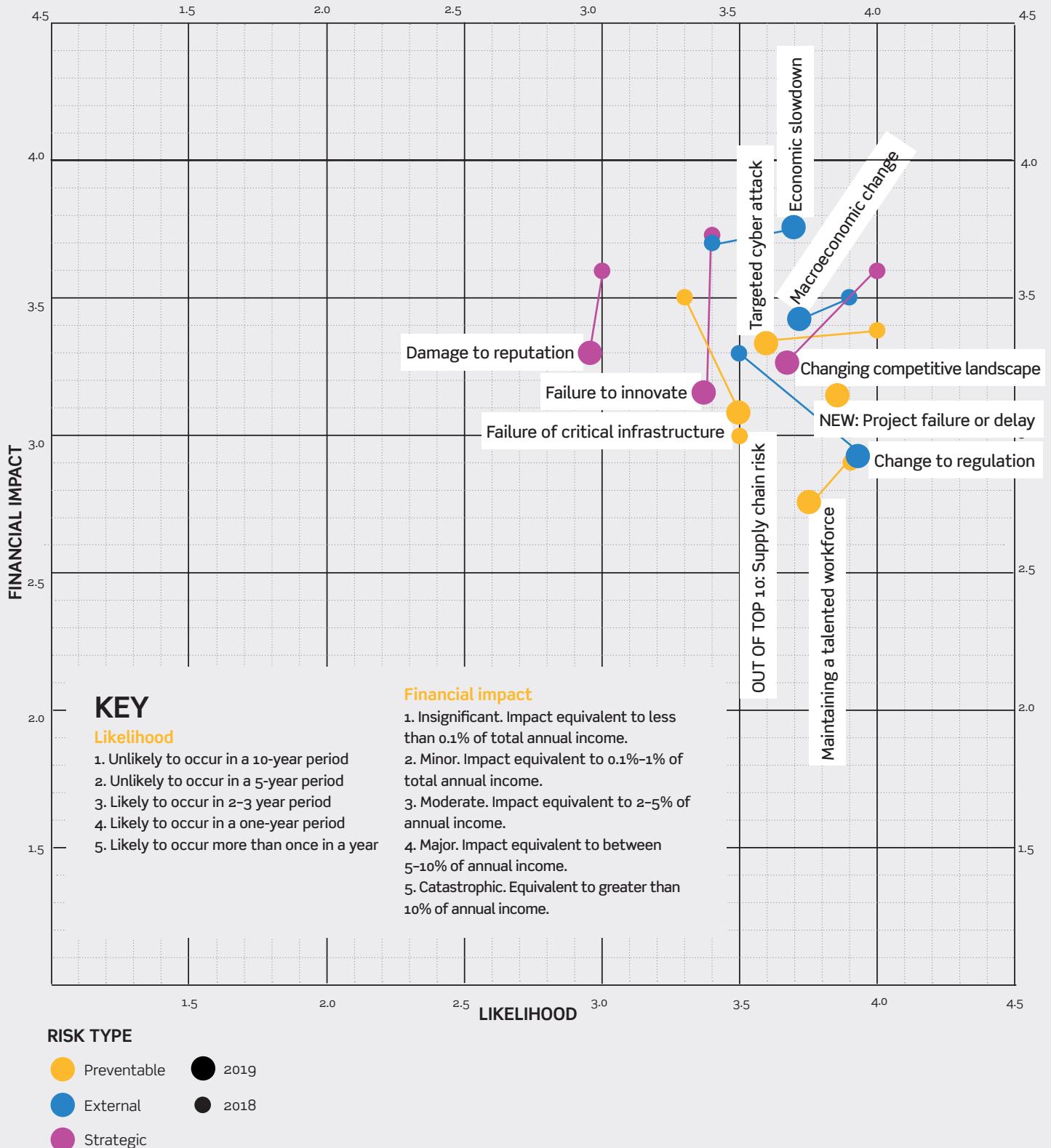
Increased board and senior management engagement is encouraging given the low ranking this has received in other surveys and shows Asia-Pacific risk managers are making real inroads in terms of engaging the right levels within their organisation.

“I AM SURPRISED TO SEE CONCERNS ABOUT SUPPLY CHAIN AND CYBER ATTACK RISKS REDUCE OVER THE PERIOD, GIVEN THE LARGE NUMBER OF WELL-PUBLICISED LOSSES IN THESE AREAS.”

SUSIE JONES, CEO AND CO-FOUNDER, CYNCH SECURITY

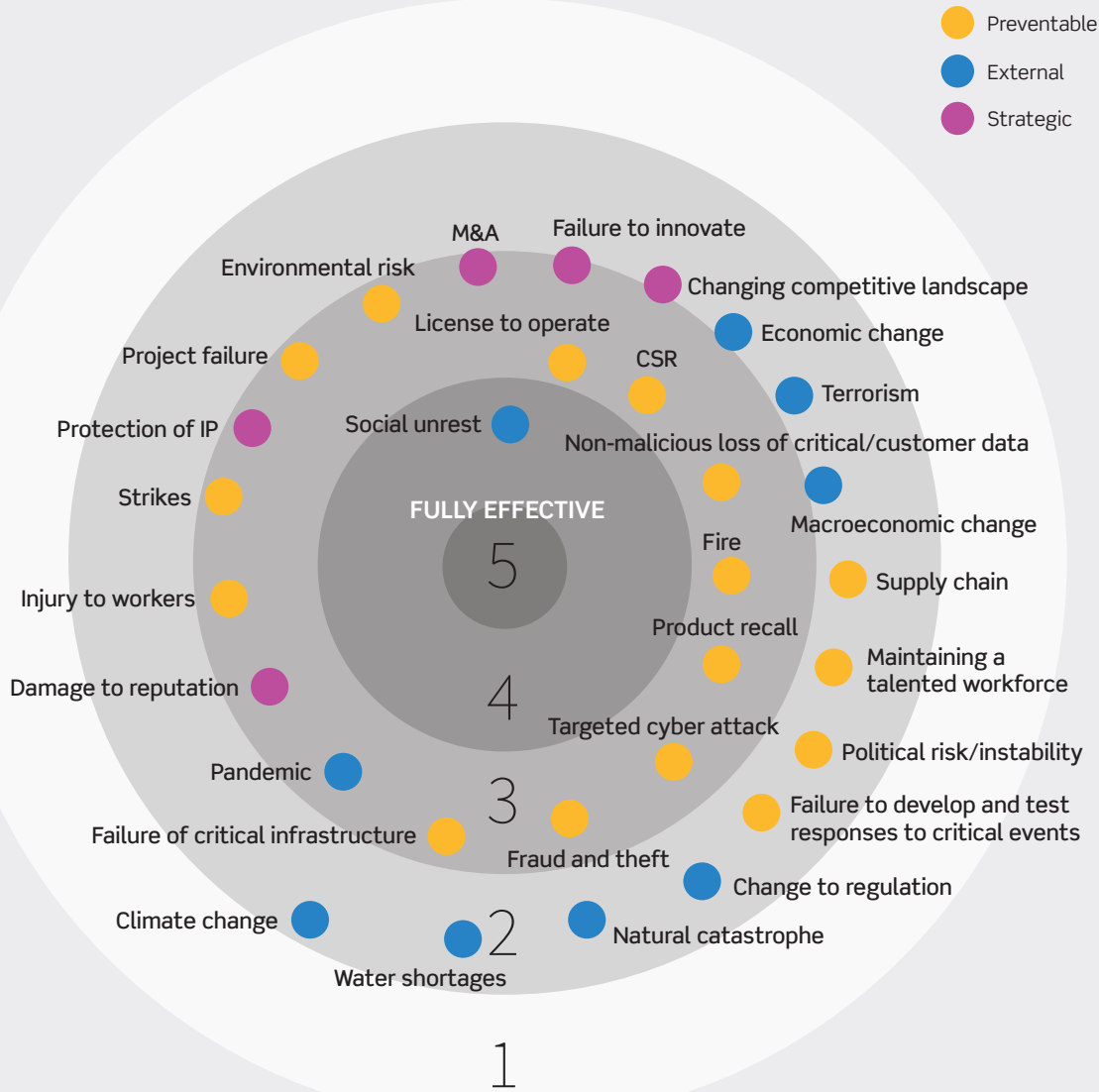
TOP RISKS BY LIKELIHOOD AND FINANCIAL IMPACT 2018 VS 2019

From a list of 31, respondents were asked to select 10 risks that are of greatest concern to their business. They were then asked to rate the risks they had selected by likelihood and financial impact.



HOW EFFECTIVE ARE YOUR CONTROLS?

We asked survey respondents to let us know the level of controls their organisations have in place to manage those risks rated of greatest concern. Over all, external risks, perhaps understandably, proved the most difficult to manage.



KEY

Effectiveness

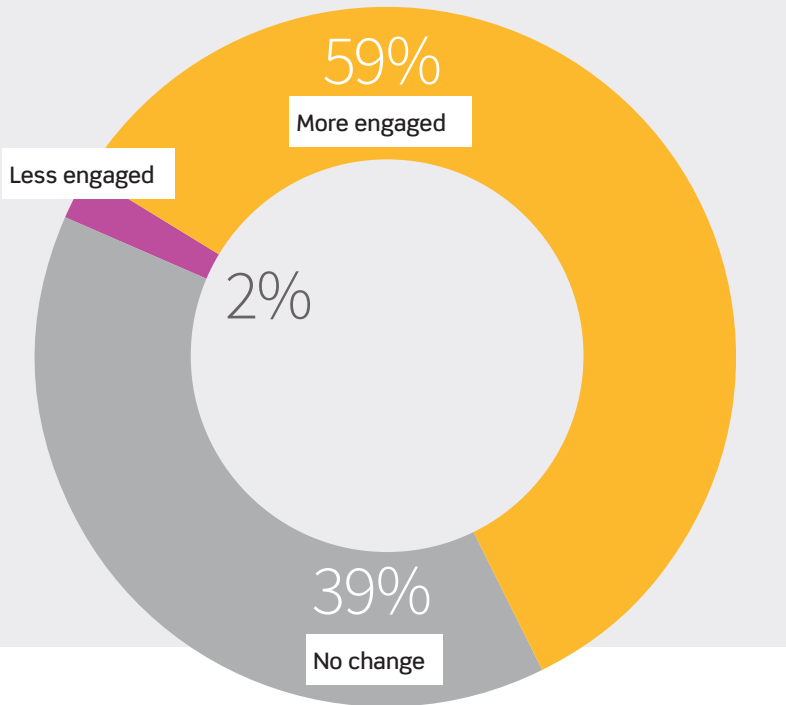
1. INEFFECTIVE: No confidence in the control design or its effectiveness.
2. MOSTLY INEFFECTIVE: There are significant control gaps.
3. PARTIALLY EFFECTIVE: Some controls are effective, others are not.
4. MOSTLY EFFECTIVE: Most controls are designed correctly and are in place and effective.
5. FULLY EFFECTIVE: Nothing more to be done except review and monitor existing controls.

“IT IS NOT SURPRISING THE MACROECONOMIC ENVIRONMENT IS STILL TOP OF MIND THIS YEAR. THE CHALLENGE WILL BE HOW WE LOOK AT OPPORTUNITIES AND RISK HOLISTICALLY.”

RYAN TAN, VICE-PRESIDENT, M&A, CORPORATE PLANNING, STARHUB

SENIOR MANAGEMENT: MORE OR LESS ON BOARD

We asked survey participants: In the past 12 months, how has senior management's engagement in risk management changed at your organisation? Responses show a positive picture of increased support for risk thinking

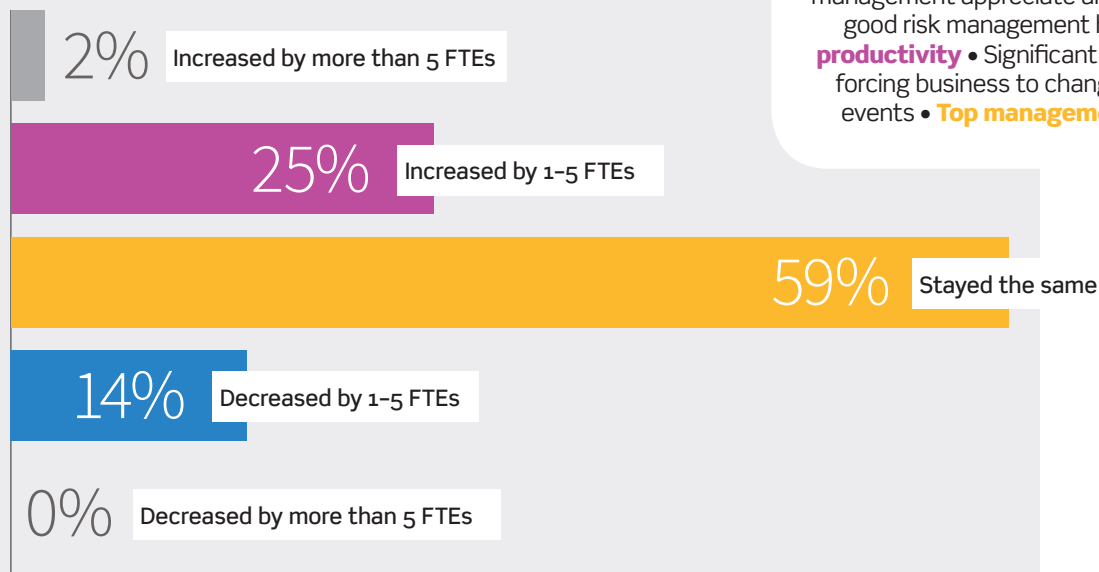


WHAT ARE THE DRIVERS BEHIND ENGAGEMENT?

Complying to **BNM regulations** • **The board** • Change in **ERM processes** • Change in the **government** • Changing regulatory and economic **landscape** • Board interest • Evolving company **maturity** • Focus and involvement on risk profiling activity • More engagement by risk team • **Governance** • Changing **economic landscape** • Greater awareness of risks as rising from several major **cyber incidents** and attacks • Improved governance • Key risk indicators reported to the board of directors • Larger team, **more integrated** • Less time talking about controls, more time about risk • **M&A**, due diligence • Materialisation of risks exposing **gaps in organisation** • More awareness and more **regulatory requirements** imposed • Ongoing discussion and dialogue with them • Alignment to **strategic priorities** • Ensuring **value protection** and creation is at the heart of decision-making • Recent adverse events experienced by the organisation **impacting bottom line**, share price and market perception of the organisation • **Regulation** and **political** changes • New engagement approach with **board of directors** • **Risk culture**, risk awareness and embedding of risk management into operation • Senior management appreciate and value the impact good risk management has on **business productivity** • Significant **external impacts** forcing business to change • **Threats** and events • **Top management** involvement

YOUR STRENGTH IN NUMBERS?

Respondents were asked: How has the size of your firm's risk management team changed in the past 12 months? Results reveal a modest increase for some, but an underwhelming growth over all.



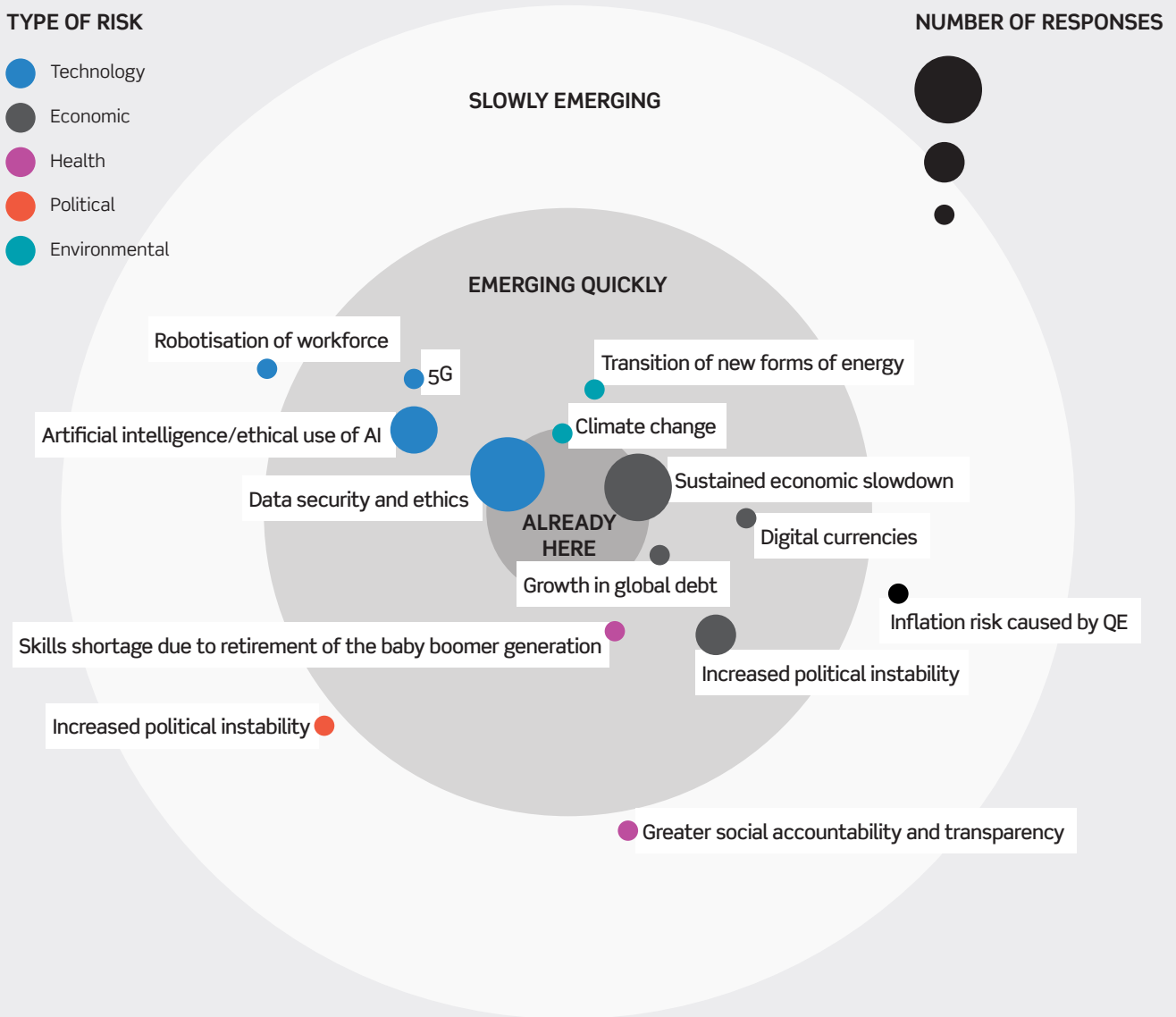
TOP EMERGING RISKS

From a list of 28, respondents were asked to select the emerging risks that are of greatest concern to their business. They were then asked to rate the risks they had selected by speed of emergence.

TYPE OF RISK

- Technology
- Economic
- Health
- Political
- Environmental

NUMBER OF RESPONSES



RANKED: TOP 10 EMERGING RISKS

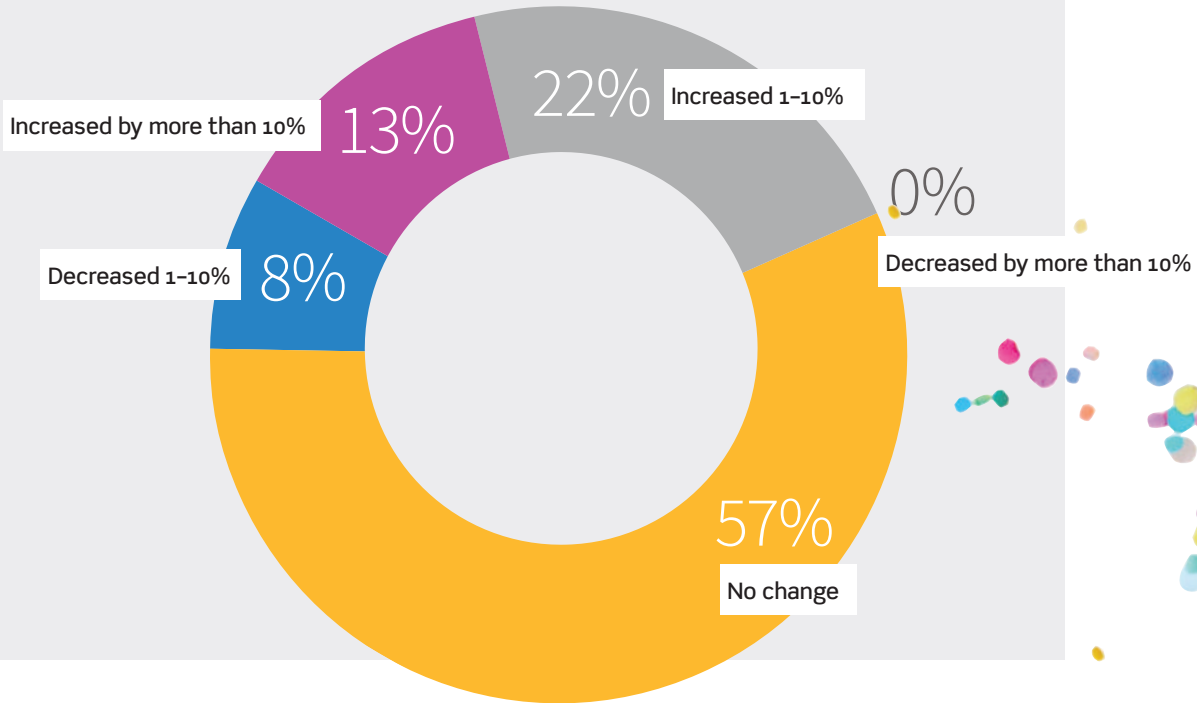
- 1 **TECHNOLOGY:** Data security and ethics
- 2 **ECONOMIC:** Long-term global economic slowdown
- 3 **TECHNOLOGY:** AI/ethical use of AI
- 4 **POLITICAL:** Increased political instability
- 5 **TECHNOLOGY:** 5G
- 6 **ECONOMIC:** Increasing protectionism/trade wars
- 7 **ENVIRONMENTAL:** Climate change
- 8 **ENVIRONMENTAL:** Move to new forms of energy
- 9 **TECHNOLOGY:** Robotisation of workforce
- 10 **ECONOMIC:** Digital currencies

“TECH RISKS FEATURE IN THREE OUT OF THE TOP 5 EMERGING RISKS – THIS IS NOT SURPRISING.”

EAMONN CUNNINGHAM, DIRECTOR AND RISK MANAGEMENT CONSULTANT AT 15B PTY

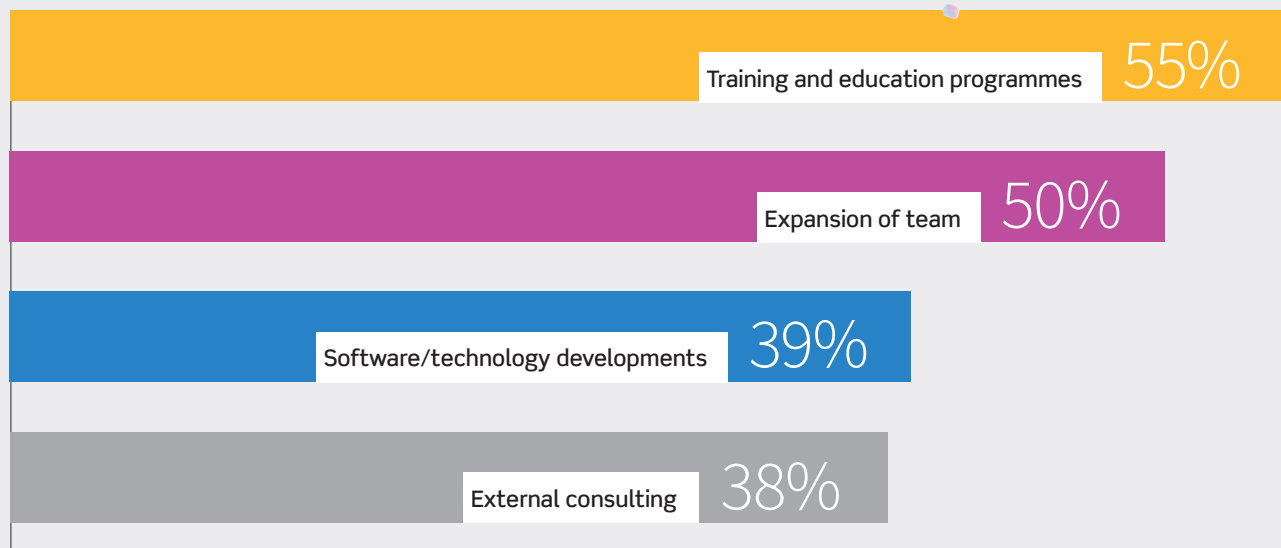
IN THE MONEY: HOW HAS YOUR BUDGET CHANGED IN THE PAST 12 MONTHS?

When it came to investment in the risk function, it was business as usual for most survey participants, though over one-third (35%) did see their budget boosted to some extent.



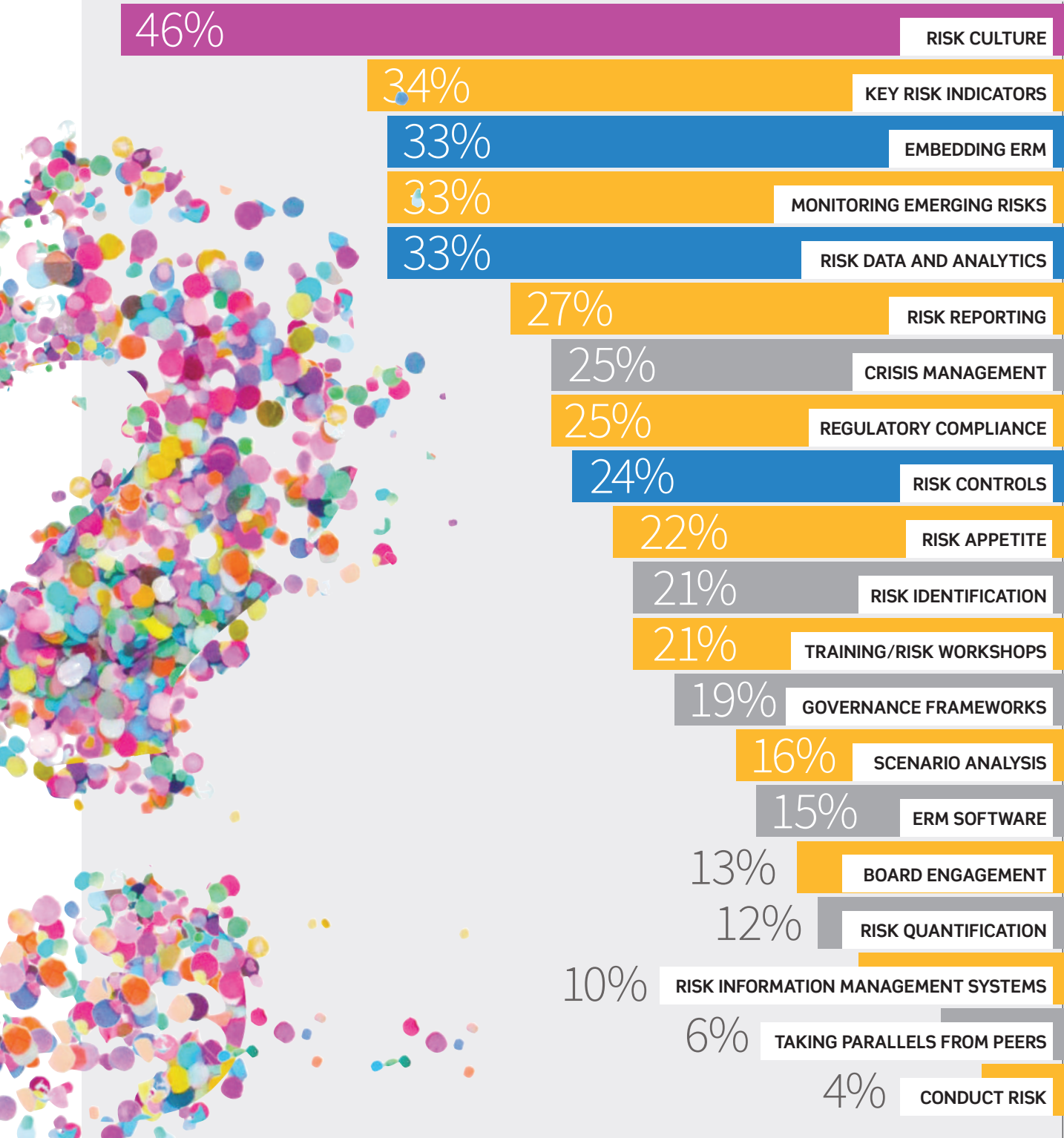
WHERE ARE YOU FOCUSING ANY ADDITIONAL INVESTMENT?

Survey respondents reported a fairly even spread of spending choices, with over half choosing to invest in training and education and adding to their numbers.



FUTURE THINKING: WHAT'S YOUR RISK PRIORITY?

Our respondents were asked: Where will you and your team be focusing your efforts in the next 12 months to improve your company's risk management programme? With respondents able to choose up to five options, focuses were diverse but a clear winner emerged, being chosen by almost half of respondents. Risk managers know: culture is king.



The dream team

The lure of the start-up may be great, but so are the risks. Adam Selwood and Susie Jones, the hearts and minds behind Cynch Security, took the gamble, emboldened and inspired by one thing – a great idea.

There are four reasons start-ups fail: neglect or fraud, lack of experience, a lack of managerial experience and general incompetence. Combine this with the fact that 50% of all start-ups fail in the first five years, and you might wonder why anyone would even try.

It usually comes down to knowing you have a really good idea, and for Melbourne-based Cynch Security co-founders Susie Jones and Adam Selwood, both formally in cyber risk management roles with Australia Post, that idea was just too good not to take forward.

Another interesting fact about start-ups is that 70% of entrepreneurs come up with their idea while working for someone else, which is precisely where the Cynch seed was sown.

Selwood begins the story: “About three years ago, I had started to learn about and get a little bit more exposure to the start-up world and start-up culture, which was around the same time Australia Post was running these things called ‘Hack Days’, an internal initiative. The concept was that you’d come up with an idea, spend 24 hours working on that idea and then compete against a bunch of other teams doing the same thing to see if you could come up with something that was viable and interesting to the business.”

He goes on: “Around the same time, I was away for Christmas break and was continuing to research start-ups and came across havebeenpwned.com, which is a service that allows you to check if your email address has been hacked. I thought this would be a great idea to adapt for the Hack Day.”

Selwood says that, while the idea was kicked around, Australia Post ultimately decided it wasn’t for them,

“YOU FIND A PROBLEM AND YOU DEVELOP A PASSION FOR THAT PROBLEM AND FOR SOLVING IT. ONCE YOU SEE THAT NO ONE ELSE IS OUT THERE SOLVING IT, YOU CAN’T FORGET ABOUT IT.”

Director and co-founder,
Cynch Security
Adam Selwood





meaning he didn't become one of their "intrapreneurs", as they are dubbed.

LET'S DO THIS

Fast forward a few months and Selwood was invited to move into Australia Post's Accelerator Programme. "I was essentially given an opportunity to go off and see if we could create a commercial opportunity around an idea. I wanted to find a way to help small businesses when they discover that they've had a data breach."

"We were looking at that as an internal initiative and during that process, I met Susie. Susie was introduced to me by someone in that programme who basically said: 'Hey, you should see if cyber insurance can play a part in this space. And if I know anything about cyber insurance, it's that you should go talk to Susie because she knows absolutely everything about cyber insurance.'"

"That's true," Jones shrugs, laughing. "We met over coffee and I agreed to join Adam. We spent another six months toying around, working with a non-profit up in the Sunshine Coast called IDCare, who provide free counselling service for anyone who was hit by a data breach. But ultimately, we just helped Australia Post realise they didn't want to be a cyber security company."

They were unfazed. Selwood says: "They closed down that initiative unfortunately. By that point, both Susie and I had had first-hand experience with a number of different small businesses in that space. As a result of that, we just kind of caught the bug and felt the need to solve for that problem."

"That is kind of the catalyst for many businesses in these spaces. You find a problem that you fall in love with and you develop a passion for that problem and for solving it. Once you see that no one else is out

there solving it, you can't forget about it or leave it alone. We didn't get the opportunity to continue with our idea at Australia Post, so we created Cynch Security to solve it instead."

THROWING THE LADDER ASIDE

Jones is the more pragmatic of the duo; something that is clear from their respective routes into the notoriously difficult world of start-ups.

"My path was a little bit different because Adam had discovered start-up land and was interested in that. That's how he then created the opportunities within Post to go up and play in that space. For me, I had no intention of doing any of that. I was climbing the corporate ladder determinedly and I was doing everything I could to keep on going."

"It just happened to be when I had that coffee with Adam that my secondment was coming to an end and I didn't want to go back to being a risk manager. I just didn't want to go back to my day job. Then he told me what he was doing, that he was getting paid to play a co-founder essentially, and I thought: 'Okay, that's totally a thing that I need to go off and do.'"

In the end, it was the tantalising prospect of decamping from corporate bureaucracy that sold Jones to the idea of tackling Cynch full-time.

"So much of being in a large corporate is just working within the machine. Even when you're really amazing at your job, does it really actually impact somebody else's life? After the project got shut down, we went back to our day jobs. I was living with a split personality because I spent nights and weekends working on Cynch with Adam but every other day in risk management and corporate bureaucracy."

"I WAS LIVING WITH A SPLIT PERSONALITY BECAUSE I SPENT NIGHTS AND WEEKENDS WORKING ON CYNCH WITH ADAM BUT EVERY OTHER DAY IN RISK MANAGEMENT AND CORPORATE BUREAUCRACY."

CEO and co-founder,
Cynch Security
Susie Jones



“YOU HAVE TO BE HONEST WITH YOURSELF ABOUT YOUR STRENGTHS AND WEAKNESSES, BECAUSE THERE’S NO HIDING WHEN YOU’RE BUILDING A START-UP. IF YOU’RE BAD AT SOMETHING, YOU GET FOUND OUT EMBARRASSINGLY FAST.”

Director and co-founder,
Cynch Security
Adam Selwood

After 15 months of working on Cynch as a side project, Jones had had enough.

“Some months we didn’t get to touch Cynch at all. Some months life got too busy and it was too hard. We’d come back two months later and then have to figure out where we were up to, which was incredibly frustrating. Eventually, I was getting a massage and I actually allowed myself to think about what life would be like if I was working on Cynch full-time. By the time I’d got off the massage table, I decided I would quit, and that was that.”

“I messaged Adam and said: ‘Hey, pretty sure I’m going to resign on Monday to work on Cynch. How do you feel about that?’ Then I went home and had a three-minute conversation with my husband, who said, ‘Sure.’ And off I went.”

ONTO A GREAT THING

The next step for this double act was gaining a place on the CyRise Accelerator (a cyber security venture accelerator program, powered by Dimension Data/NTT and Deakin University); something Selwood attributes wholly to Jones’s fearlessness in leaving her day job.

“The programme that we were applying for at the time, we didn’t know if we’d been accepted but Susie said: ‘I’m going to go do this regardless.’ Ultimately, I think that was possibly the thing that got us into the programme – you actually just stating: ‘I’m doing this whether or not you’re involved, guys.’ And they said: ‘Okay, someone who’s got the balls to do that should really get involved in this.’”

Conversation easily flits between Selwood and Jones, sometimes to the point where you feel like a third wheel, but it is clear their natural rapport is one of the key reasons for the incredible success of the business.

Cynch was one of just two international finalists in the NYCx Cybersecurity Moonshot Challenge. The event, run by the NYC Mayor’s Office of the Chief Technology Officer, was launched in late 2018 to tackle how to make every small and mid-sized business in New York City and beyond as resilient to cyber security attacks as the Fortune 500 companies. Despite ultimately not winning the challenge, the team are undoubtedly onto a good idea.

WHAT’S THE WORST THAT CAN HAPPEN?

With failure always looming on the doorstep of start-ups, it is of little surprise that Selwood and Jones have a laundry list of mistakes they’ve made along the way, lessons they are keen for other entrepreneurial risk managers to learn from.

“Save money,” says Jones. “Save as much as you can before you make the leap, because it will give you more of a runway to take off from.”

“I also didn’t gain as much empirical evidence before I made the decision as I probably should have. Thankfully, it turned out all right in the end anyway. But what is going to be right for one person is not necessarily going to be right for somebody else, and you’ve just got to be flexible and make it work the best you can.”

Selwood is quick to echo Jones’s thoughts on saving money and adds timing as a huge factor in the success or failure of start-ups. “The reasons we took the jump to Cynch full-time were about timing

and the external factors affecting each of us. In the 12 months prior to the CyRise programme, there was no pressure from any direction. In every instance, where we’ve made that call to do this full-time, there’s been some sort of external pressure – be it the market has matured or there are a lot of customers talking to us.”

In true risk manager style, Selwood ponders aloud whether he would have changed the timing on his leap to Cynch.

“Ultimately, timing wise and when to do it – it’s not really an option to be honest. It was then. It was then or never, and so if the alternative was never, then I don’t regret it. You see something, you jump towards it. The other side of the calculation has always been if I don’t do this then I’m going to forever regret not having done this. I would have been really disappointed in myself if I hadn’t taken the leap.”

Jones sees things a little differently. Turning to Selwood, she remarks: “It’s funny that you say you think about regrets because I never do. I probably should sometimes but I never do. What was the worst that could happen? The worst case was that we couldn’t afford our rent for a while and had to move in with friends and I had to get another job. Once I’d settled that in my mind, then I allowed myself to go off and have the big audacious daydreams of: ‘How big could this get?’ And in my head it can get really, really, really big, so that makes it a much easier decision.”

IN THE SAME CORNER

Selwood is the natural dreamer of the two, having come from a family of entrepreneurial business owners, while Jones is evidently, unmistakably the mouthpiece of the business. This balance is nice but there will always be disagreements, even in the best partnerships. How are they solved at Cynch?

“Cage fighting,” says Selwood, with a deadpan expression.

“I would totally win,” retorts Jones. Jokes aside, Jones says: “Both of us are really bad if we let anything bottle up. It’s also really obvious if we do, so there’s no point even trying to – we just talk it out.”

Selwood adds that the focus of their combined mission helps keep them from all out war. “We have different ideas, which we present in different ways. Sometimes we deviate from each other but we always find our way back via our shared mission.”

Before our conversation can become too ‘smiles and rainbows’, Jones quickly points out one of the hardest facts about working as a partnership in a start-up. “You have to be really honest with yourself about your strengths and weaknesses and what do you need to be able to overcome these weaknesses. Because there’s no hiding when you’re building a start-up. If you’re bad at something, you get found out embarrassingly fast.”

And when you are both bad at the same thing? “We go and have a beer together and find a way to suck it up,” laughs Selwood.

There is no stopping this whirlwind pair as they gear up for the next stage of Cynch – organic growth of their team and their footprint over the coming year. It’s something they are both understandably excited about. As for any talk of failure, that simply isn’t the plan.





On a bear hunt

As some market experts report hearing the distant, but undoubtedly chilling, growls of an approaching global downturn, we ask how much risk managers can really do to protect their businesses from being savaged.

It is now more than 11 years since Lehman Brothers bankers packed their belongings into cardboard boxes and left their Wall Street offices for the last time. September 2008 saw the collapse of the US investment banking institution that marked the onset of the Global Financial Crisis and Great Recession, the worst global economic downturn since the Great Depression of 1929.

From Singapore to Sydney and London to Lisbon, no global economy was immune from the effects of the global financial crisis, sparked by the collapse of the US subprime mortgage market. Credit was withdrawn overnight, and global economies turned to monetary and fiscal stimuli to prevent a full-scale economic collapse.

Banking crises in Iceland, Ireland, Portugal and Britain echoed the turmoil seen in the US, as governments grappled with falling house prices and damaged consumer confidence.

Eleven years on from the biggest economic crisis in our lifetimes, there are fears another global downturn could be around the corner. Months ago in the US, an inverted bond yield curve, a key indicator

for an imminent recession, caused market experts to ring the alarm.

The yield curve has since returned to normal, but recent market activity indicates investors are skittish about the prospect of the global economy. There is a looming feeling we are approaching the end of the upturn.

A WORLD IN TURMOIL

While it hard for economists to pinpoint the date or year of the next downturn, global organisations have begun to raise concerns about a combination of geopolitical and economic factors. Rating agency Moody's has highlighted fears of rising political instability and a fragile global economy heading into 2020. It says the global economy is on track to record the lowest level of growth since 2009. It does not, however, believe we will enter recession in 2020.

In a November 2019 note, Elena Duggar, Moody's associate managing director, said: "Growth in advanced economies will slow toward potential as labour markets continue to tighten, while growth in many emerging market countries will be below

"GLOBAL GROWTH IS SLOWING. THE WORLD ECONOMY NOW LOOKS EVEN WEAKER THAN THE BANK'S JUNE FORECAST FOR 2.6% GROWTH IN 2019, HURT BY BREXIT, EUROPE'S RECESSION AND TRADE UNCERTAINTY."

President, World Bank
David Malpass

average as a result of China's slowdown and as global trade growth grinds to a halt."

Moody's believes rising trade tensions between the US and China, and Britain's exit from the EU, will exacerbate wider problems in the global economy: "Risks will centre around US-China trade disputes, Brexit-related uncertainty and the escalation of other bilateral disputes. At the sector level, spillover effects from trade frictions will drive shifts in global supply chains and weigh on investment decisions."

And fears of another global downturn extend beyond the US and Europe. Investment banking giant JP Morgan's recent survey of Asia-Pacific chief financial officers found a global recession was the main risk for their business over the next six to 12 months. A total of 30% of the 150 respondents from 130 corporations said a global recession was their top risk, 27% pointed to the impact of global trade tariffs, and 24% said an emerging markets slowdown was their top concern.

US economists predict the world's biggest economy will enter recession by 2021 – a survey conducted in August by the National Association for Business Economists found 72% of leading economists believe the US will slide into a downturn within two years. About 38% of economists expect a recession next year.

The International Monetary Fund (IMF) is more bullish on the global economy's near-term prospects. It is "far" from forecasting a global recession, but has cut the world's forecast for growth in 2019 and 2020, due to the "negative impact" of the US-China trade war and increased protectionism. The IMF warns that when the next recession comes around, central banks will have little room to manoeuvre, as they have already cut interest rates to record lows.

The World Bank, on the other hand, warns of "substantial risks" to the global economy. It forecasts weaker-than-expected 2.6% growth during 2019, and says "economic momentum remains weak". Growth will slow in both developed and emerging economies through next year, the World Bank says, with softness in trade and domestic demand.

"Global growth is slowing," World Bank president David Malpass said in a speech in October. "The world economy now looks even weaker than the bank's June forecast for 2.6% growth in 2019, hurt by Brexit, Europe's recession and trade uncertainty."

FOREWARNED IS FOREARMED

As risk managers across the globe watch financial markets for the next big risk indicators, how can risk teams prepare their organisation for a global economic downturn? What role should risk managers play in protecting their business, and can anything really be done? *StrategicRisk* spoke with some of the world's leading risk managers to get their views on how to tackle recession risk.

Eamonn Cunningham, an independent risk consultant, was the chief risk officer for shopping mall group Westfield when the 2008 crisis hit. With operations in the US, UK and Australasia, the company was directly impacted by reduced spending as consumers tightened their belts in the wake of the crisis.

Cunningham, who is now based in Australia, says it can be difficult to predict the outcome for your business, and organisations should consider all eventualities when considering the impact of a recession.

"In the retail landscape, you would think customers would have reduced spending on luxury goods, and the more expensive stuff. You would expect discount brands to be more resilient. However, the opposite happened, and the high-end proved more resilient, at least in the initial period after the recession hit. The message here is, you have to check the facts and not assume."

Cunningham says risk managers can help guard their company against the risk of recession by having a "robust" enterprise risk management (ERM) system in place. "That needs to cover all areas of enterprise activity, at the strategic decision-making level. If you're just employing ERM for the operational stuff, you're going to be caught short if we have a major market-changing event like the 2008 recession."

Cunningham says risk managers should regularly test their ERM processes to ensure they can withstand a major economic event.

"You might have a robust ERM system, and it might go from boardroom to factory floor, but unless you're stress testing it, and have a regular regime of robust scenario planning, you're not testing the ERM system to ensure it will deliver as intended.

"What we found was, testing needs to be sophisticated so that it also considers the impact of multiple factors that may cause an adverse impact.

"FOREWARNED IS FOREARMED. IT'S AMAZING WHAT DEGREE OF CONTROL YOU CAN HAVE. YOU WON'T BE ABLE TO INFLUENCE MACROECONOMIC POLICY, BUT THERE ARE THINGS YOU CAN DO."

Independent risk consultant
Eamonn Cunningham

GREAT RECESSION: BY THE NUMBERS

10.1%

Peak level of unemployment in the US after the recession

20%

Subprime mortgage lending as a proportion of overall US lending, 2004-2006

\$400bn

Greek national debt in 2010

\$787bn

Stimulus package delivered by the US government as part of the American Recovery and Reinvestment Act

127%

household debt compared to income in the US, 2007

£500bn

Bank rescue package unveiled by the UK government in October 2008

4,485

In Q1 of 2008, credit rating agencies downgraded more than 4,000 collateralised debt obligations

-1

Australia bucked the global trend by avoiding recession, only suffering one quarter of negative growth

41%

House price drop in Ireland following the crisis

“IN THE UK, THE MOST OBVIOUS TRIGGER EVENT WILL BE BREXIT. IT COULD HAVE A SEVERE DIRECT EFFECT ON THE UK AND EUROPEAN ECONOMIES, WHICH COULD TRIGGER THE NEXT GLOBAL RECESSION.”

Founder,
GOAT Risk Solutions
Danny Wong

You have to look at areas that are highly correlated. So ‘A’ might have an impact of 1, ‘B’ might have an impact of 1, but together they might have an impact of 3.”

Cunningham believes risk managers can help their organisations guard against the risk of recession by highlighting the potential effects and helping companies consider strategic changes, such as which markets to remain in, which products to sell or which currencies to move into.

“Some [risk managers] may feel they have no ability to influence the outcome, but I always refer to the old adage, which is, ‘forewarned is forearmed’. If you’ve done the homework and identified it as an issue, and get that message through, that is something.”

“If it is on the register and decision-makers see it as a risk, they might think they can impact it by 2% or 5%. It’s amazing what degree of control you can have. You won’t be able to influence macroeconomic policy, but there are things you can do.”

He says it is important for risk teams to “position yourselves so that when you speak, all the relevant people listen”. “You may be coming to the table with a dire warning, so you need to come with facts and back up what you say.”

Risk managers should not underestimate the impact they can have in preparing for major global events, he says.

“Any risk manager worth their salt shouldn’t just throw their hands up and say there’s nothing we can do about it. It’s even worse to leave it off your company’s risk register. You must put it on. There must be a grown-up debate on what can be done, even if you don’t think anything can be done. Don’t accept the premise there’s zero that can be done. Knowledge is power, and forewarning is useful.”

GO BEYOND YOUR IMAGINATION

Danny Wong, the founder of GOAT Risk Solutions, a UK-based risk management business, says the UK has struggled to recover during the Great Recession.

“Although the credit crunch of 2007–09 originated in the US, the impact in the UK was far-reaching. The collapse of Northern Rock, the government bailout of HBOS, liquidity in the markets collapsed, equity market plummeted, interest rates dropped, and governments pumped

money into the financial system through quantitative easing, house prices collapsed, millions of jobs were lost, and the value of sterling has never recovered – all indicate its lasting effects.”

Wong says macro-economic risks “are ones that could have a significant impact on the business but are almost entirely out of our control”.

He adds: “As a risk manager, we can still help the business walk through the scenario, ensuring that we are as resilient to economic shocks as possible. This might mean introducing policies to hold cash, reduce investment capital and spending, cut costs, reduce financial commitments and secure access to credit. The important thing is to monitor and manage cashflows, communicate expectations, have plans of different levers to pull and at what point. These aspects are all wholly within our control.”

Wong believes Brexit poses the biggest risk to a recession in his home market. “In the UK, the most obvious trigger event will be Brexit, which has been looming since the 2016 referendum. Brexit could have a severe direct effect on the UK and European economies, which could trigger the next global recession.”

Wong says risk managers learned a valuable lesson in the Great Recession: that events “could be longer and have more far-reaching effects than imaginable”.

He added: “We really shouldn’t have been surprised if we stepped away from it and used some common sense – we should now be able to see bubbles from a mile away. We must not be complacent.”

We need to pay attention to the systemic or macro-risks. It’s not just relative to your competitors; it could permanently affect entire sectors. It will happen again.”



Keep pace with connectivity

The Internet of Things is blazing trails like nothing before. But as data privacy and safety concerns set in, regulation is hot on its heels. Our industry must be up to speed with this fast-moving new world.

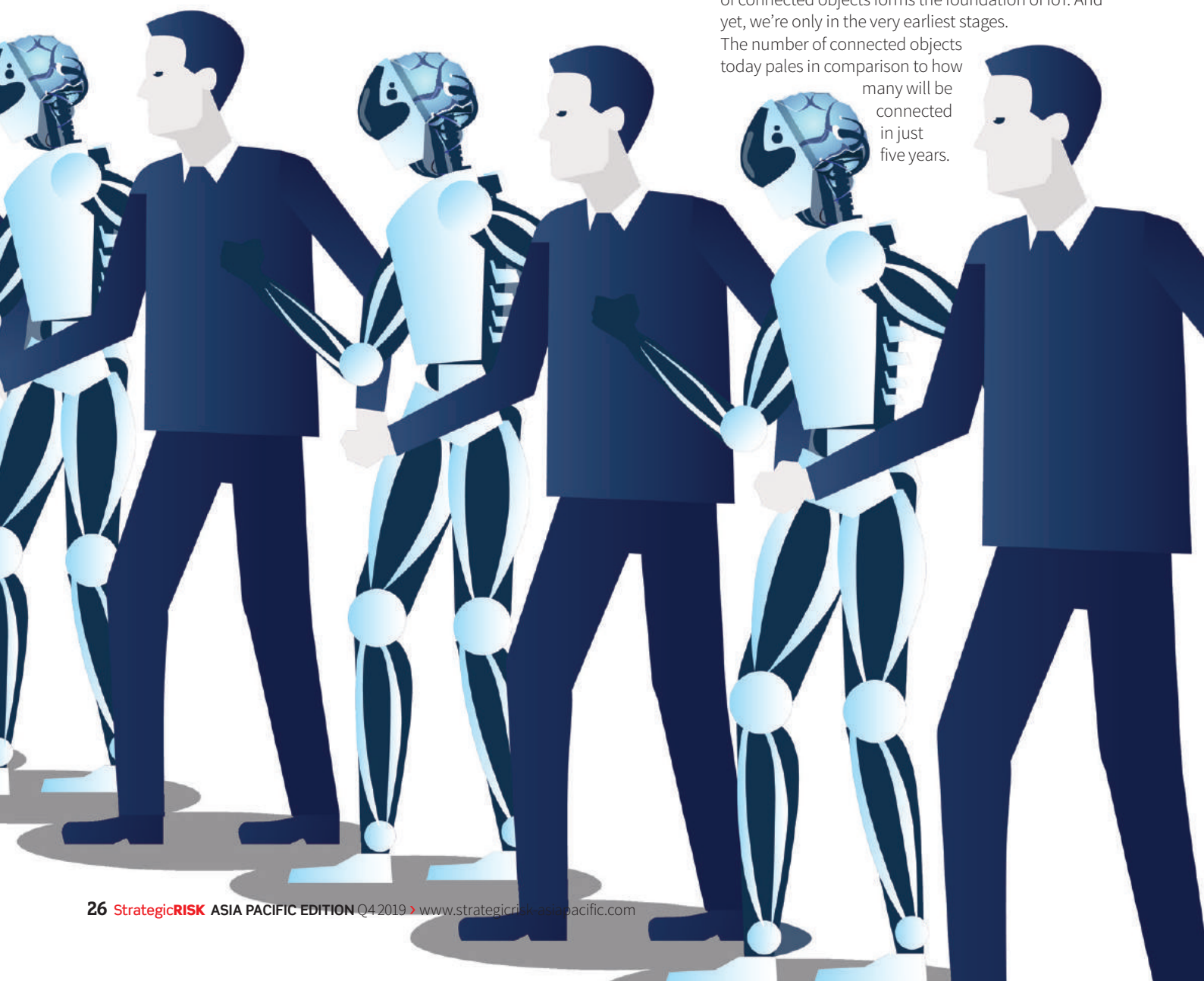
Your business has been redesigned to incorporate 'smart' devices that constantly monitor the operations of the business. One device, a thermostat, collects data and sends it to the device's company, including your premises' temperature. One day, a fire occurs and the thermostat registers a dramatic spike in temperature. The thermostat is not designed to work as a smoke detector and the manufacturer claims it has no obligation to inform you of danger. However, just because it doesn't have to, does that mean it shouldn't? Here in lies one of the most serious risks clouding this tech revolution.

A GIANT STEP FORWARD

The Internet of Things (IoT) is a data-driven revolution that could rid us of many of the inefficiencies and unsafe practices of modern business and domestic life. The transformation deals with the steady but inexorable rise of connected and sensorised objects in our home – in short, the online digitisation of our physical world.

According to industry analysts, there are 10–20 billion things connected to the internet today. This ecosystem of connected objects forms the foundation of IoT. And yet, we're only in the very earliest stages.

The number of connected objects today pales in comparison to how many will be connected in just five years.



THE ETHICAL DILEMMAS OF IOT

Autonomous vehicles present serious questions of liability. When they are the decision makers, who is at fault in a crash?

When it comes to autonomous vehicles, we are faced with an ethical dilemma: In the seconds before an accident, should an autonomous vehicle do anything it can to protect the passengers, even if it means harming other motorists or pedestrians?

When humans are behind the wheel, collateral damage, as terrible as it is, doesn't pose much of an ethical problem. A human being in danger can't be faulted when its survival instincts make it swerve its car into a pedestrian. But when machines are the decision-makers, does a pedestrian harmed in an accident have a case against the car manufacturer? Does a driver have a case against a car manufacturer following an accident in which they were injured?

As a European Commission report on ethical dilemmas inherent in IoT technology stated: "People are not used to objects having an identity or acting on their own, especially if they act in unexpected ways."

\$2.5tr
projected sale of
connected devices and
services, 2020

RISE OF THE SMART CITY

The IoT is giving rise to pervasive digital networks within the physical space - the networked lifeblood of the 'smart city'.

Not just a network of municipal services, such as electricity and water, truly 'smart' cities combine elements from all urban

stakeholders, including citizens, government and businesses. A broad spectrum of implementation models is emerging in different parts of the world.

In South America, Asia and Europe, all levels of government are identifying the potential benefits of building smart cities, and are working to unlock significant investment in that area. Rio de Janeiro is building capacity at its Smart Operations centre; Singapore is about to embark on an ambitious Smart Nation effort; the EU's Horizon 2020 program has earmarked €15 billion in 2014-2016 - a significant commitment of resources to the concept of smart cities, especially at a time of fiscal constraints.

While China is the biggest player in the IoT market, the entire Asia-Pacific region stands to gain greatly from recent IoT technology. The research firm IDC estimates that the IoT market size in Asia-Pacific, excluding Japan, will grow from \$250 billion in 2013 to \$583 billion in 2020. Meanwhile, the number of things connected to the internet in the Asia-Pacific market will grow from 2.59 billion in 2013 to 8.98 billion in 2020.

Estimates vary, but the range of connected objects by 2020 will be 40-50 billion, and includes everything from cups and pens to homes, cars and industrial equipment.

Combined with other technological developments such as cloud computing, smart grids, nanotechnology and robotics, the world of IoT we are about to enter represents a giant stride towards an economy of greater efficiency, productivity, safety and profits.

Autonomous objects can constantly acquire, analyse and transmit reams of data captured from their surroundings. In turn, economies, cities, businesses and people will respond to this flow of information - opening an unprecedented array of opportunities, and challenges, for risk managers.

REGULATORY CRACKDOWN

AIG Asia's head of financial lines, David Ho, explains why risk managers globally need to get up to speed on this issue quickly. "Data privacy and use has come squarely into focus with the implementation of GDPR. Many IoT devices may collect, store and use personal data such as auto telematics, smart speakers, health biometric data, among others. Producers of IoT devices, and the software they run on, need to ensure that they meet the regulatory requirements to avoid costly fines and penalties."

"In the US, California is leading the charge on the regulatory provisions for collection and use of personal data. The California Consumer Privacy Act was signed into law in June 2018 and companies will need to meet the requirements by January 1, 2020. Further, California passed SB 327, which is specific to the collection and use of data from IoT devices."

"Risks can extend beyond data privacy. Failure of IoT devices may cause property and bodily injury risks. The very concept of securing a facility or business, with respect to the protection of people and property, now has a cyber security component because of the proliferation of IoT devices and equipment."

"IOT PROVIDES VALUABLE DATA THAT CAN BE USED TO MORE EFFECTIVELY ASSESS AND PRICE RISK. FOR THE INSURER, THE VALUE LIES IN MORE CUSTOMISED AND ACCURATE PRICING."

Head of financial lines, AIG
David Ho

\$775m
How much China has
earmarked for IoT
investment

HOW MUST INSURERS RESPOND?

The insurance industry's response to any emerging challenge is key to how businesses can optimise and manage this risk to their advantage, or disadvantage.

Ho says: "IoT provides valuable data that can be used to more effectively assess and price risk. An example that is quite dated now is the use of telematics in personal auto. We expect that more 'telematic-like' applications will emerge in other sectors - for example, heavy industry and manufacturing- to provide insureds and insurers with 'real-time' data on risk levels.

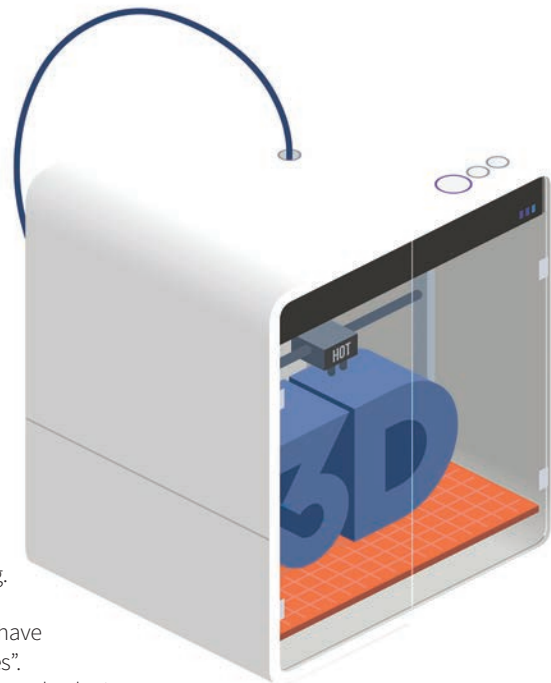
"For the insured, the value of the data lies in improving safety and thus reducing accidents and the cost of risk. For the insurer, the value lies in more customised and accurate pricing that relies on hard data rather than more qualitative reports. Data collection through IoT should eventually provide a more effective underwriting process than heavy reliance on human-answered questions with limited data collection."

One area of concern Ho notes that requires more significant adaptation is cyber security of IoT used in critical infrastructure. "Increasingly, sensors are used in sectors that provide critical and life-impacting services, such as power and energy, aviation, transportation and medical treatment. As such, insurers are faced with assessing the potential risk shifts from introducing connected technology and adjusting policy pricing, terms and conditions, and underwriting."

"AIG's strategy to move to affirmative cyber coverage in all products was in part related to the proliferation of connected devices and the potential for failure in such devices to result in physical and non-physical damage."

Is 3D printing dangerous?

It represents a huge breakthrough in the way companies manufacture goods. But are companies brushing worker health fears over 3D printing under the rug as they race to embrace the new technology?



3D printing has revolutionised the way manufacturers design, create and produce goods, leading to increased efficiency for companies across the world. From Adidas designing new shoes to surgeons creating custom-made implants, each sector can benefit from the groundbreaking technology.

3D printing heralds a shift in the way companies manufacture goods. It will enable companies to customise production and make parts in local markets, reducing the reliance on timely, costly, overseas supply chains. While 3D printing brings huge advantages and opportunities, it also presents emerging risks, particularly concerning worker health and safety.

The global 3D printing market is expected to reach \$41 billion in value by 2026, according to Acumen Research and Consulting. The technology is growing at an annual compound growth rate of more than 20%, according to the advisory firm's latest study. In the automotive, manufacturing, industrial, consumer and aerospace sectors, 3D printing has been transformational. Insurers argue that organisations are slow to recognise the potential risks.

DUST EXPOSURE

In a recent white paper, global insurer AIG outlined some of the key risks facing companies using the technology. The insurer believes the issue of worker safety has received "limited attention", as companies race to use the new technology, also known as additive manufacturing, to their advantage. The AIG paper warns that 3D printing presents "new angles on existing worker risks, such as raw material exposure, the use of new machines, and the handling of in-process and finished goods".

AIG believes organisations should consider these unknowns as they embrace the new technology. Risk managers will need to consider several emerging risks as their organisations use 3D printing technologies. "In our discussions with leading additive manufacturers, some note that workers are exposed to 'significant amounts of dust' via newly designed manufacturing processes. Risk managers are wrestling with this new exposure and seeking information and practices to reduce uncertainty and manage risk," the insurer says.

AIG is working with Praedicat, a tech company specialised in spotting harmful substances, to identify health risks from 3D printing. Its research indicates that some materials used in additive printing "have the potential to cause worker injuries".

The firm implores risk managers to take the issue seriously. AIG's report states there are several potential health risks associated with 3D printing. Inhalation of ultrafine metal and other nanoparticles, along with volatile organic compounds, have the potential to cause "adverse health impacts" such as lung and nervous system injury, mental impairment, various forms of cancer and hearing loss.

Amid these early findings, AIG has urged caution among the risk management community. "While the science is in different states of maturity, some exposure and disease combinations are well-supported while others continue to develop."

WHAT CAN YOU DO?

AIG wants organisations to take "a proactive approach" to managing worker safety, and has called on companies to "review the science" and "adjust manufacturing processes accordingly".

It said: "For example, elimination or substitution might be considered when the scientific evidence indicates the risk of using a specific agent is particularly high. For all agents, common worker safety processes and engineering controls can be applied to additive manufacturing, such as proper ventilation, system enclosures, rotating worker shifts and using proper respirator equipment."

While organisations should take steps to mitigate production risks, they must also consider the ecological and environmental impact of waste products from the 3D printing process.

AIG says businesses must "utilise proper disposal techniques to avoid environmental contamination, and protect those workers charged with the disposal and removal of residue or equipment". They should also "have a broad worker safety programme, and address common worker safety risks".

"IN OUR DISCUSSIONS WITH LEADING ADDITIVE MANUFACTURERS, SOME NOTE THAT WORKERS ARE EXPOSED TO 'SIGNIFICANT AMOUNTS OF DUST' VIA NEWLY DESIGNED MANUFACTURING PROCESSES."

An AIG white paper

Staying as smart as 5G

Connected devices are transforming our lives, and our risk landscape. As some risks are eradicated, new concerns are coming to light. We sat down with AIG's David Ho to discuss how insurers must adapt.

HOW ARE INSURERS ADAPTING TO THE NEW RISKS OF 5G?

To respond to these trends, insurers are actively assessing the risks of transition to a 5G world and partnering with clients. For example, AIG has worked with several manufacturing companies who are exploring the potential of 5G to optimize manufacturing processes.

This includes moving to "Industry 4.0", in which smart factories are leveraging connected technologies such as industrial robots and smart software to drive more efficient and automated manufacturing processes.

Further, the growth of cyber insurance will continue given the dramatic increase in exposure as more devices come online. The potential for data theft and integrity is highly in focus; increasingly more insurers will assess the potential for other types of damage including bodily injury and property damage from the failure of 5G technology.

Insurers are also exploring the potential for liability shifts as accidents move away from 'human' or 'driver' error into the realm of 'machine', 'software', or 'algorithm' error. It is likely that software errors and omissions coverage will grow in importance and size as liability will emerge when technology fails.

HOW WILL 5G CHANGE THE RISKS ASSOCIATED WITH SOCIAL LICENCE TO OPERATE?

Data privacy and security has taken a prominent role in recent regulatory and consumer discussions. This relates to a number of large data privacy events and concern over the types and volume of data collected, stored and used by companies.

This trend has led to

"A 5G WORLD WILL BE CHARACTERIZED BY EVEN GREATER RELIANCE ON CONNECTED TECHNOLOGY, AND MOST IMPORTANTLY, IN AREAS THAT ARE CRITICAL TO HUMAN HEALTH AND SAFETY."

Head of financial lines, AIG
David Ho

more stringent data regulatory requirements, including GDPR in Europe and CCPA in California, US. We expect that these regulatory requirements will continue to advance as more governments and regulators adjust to the new data-rich industrial landscape.

Further, companies will continue to be challenged by managing the multitude of regulatory requirements in all of the markets in which they operate.

Increasingly, companies will be required to go beyond regulatory compliance and provide transparency on the types of data collected, how they are used, stored and protected.

As technology becomes more and more embedded into critical life-impacting processes such as medical procedures and transportation, the risks need to be aggressively managed to foster widespread acceptance and adoption.

WHAT ARE THE POTENTIAL DISRUPTIONS ASSOCIATED WITH 5G?

It is quite clear that we will become more and more dependent on connected devices. This is already evident in our reliance on digital banking and ATMs, GPS-enabled navigation tools and voice-assisted technology for ordering consumer products. A 5G world will be characterized by even greater reliance on connected technology, and most importantly, in areas that are critical to human health and safety.

On one hand, the rise of autonomous vehicles will usher in an era of much safer roads as human error will be dramatically reduced. On the other, the potential for system outages or breakdowns, either accidental or purposeful, could lead to significant systemic disruption and/or injury.

It is not difficult to imagine a scenario in which the technology that supports autonomous vehicles fails – either accidentally or purposely – leading to widespread transportation disruptions or even accidents. The incidence of these events should be expected and will emerge as more connected devices are brought online.





Revealing Mr Hyde

Every organisation wants to project a nice guy image. But their shadow values – the ones employees actually follow – may uncover an alter ego that is much uglier. How can risk managers work on negative forces that wish to remain elusive?

We have all been there. First week of a new job and you are introduced to the company via HR policies and procedures. You are informed of the company values and told: “This is the way we do things.” Except... it isn’t. You meet your colleagues and are told: “*This* is the way things are actually done around here.” And that is precisely where the curse of shadow values begins.

In psychology, the dark side of human nature is often described as the alter ego. It’s what Freud referred to as the ‘id’, and Jung identified as the ‘shadow’ – the sum total of all those unpleasant qualities we prefer to hide.

“The shadow gains its power through being habitually repressed. And it manifests in a multitude of symptoms and psychological disturbances,” says The Ethics Centre director of innovation John Neil.

“Similarly, an organisation’s shadow values gain their power from being kept below the surface. At their worst, they are destructive mutations of the official values, that pose an existential threat to the integrity of an organisation’s ethical culture.”

Left unchallenged, values like these are highly likely to become the unofficial cultural values of an organisation, poisoning the mentality of the firm slowly and insidiously.

VALUE JUDGEMENT

But when companies look to create a set of values, many don’t know where to begin.

“It’s a perennial challenge for all organisations,” says Neil. “Ensuring behaviour, policies, systems and processes are aligned with that ethical framework is no easy feat. If the managers of an organisation say one thing but consistently do something else

entirely, it breeds a cynicism and disconnect that permeates the entire workforce. Customers and other stakeholders eventually figure it out as well.”

“There’s a whole typology around values, so you can have aspirational values that you need to drive your strategy, but ideally there’d be very few of those. Most of your values should describe explicitly the type of culture that you have, that’s in line with your purpose. The cookie-cutter approach is never going to work when you are designing values for a company.”

Neil notes the now infamous Enron example as a starting point. “*Respect, integrity, communication and excellence*. These are admirable and worthy corporate values – ones you’d proudly make official and put on the wall. Unfortunately, those same values also belonged to Enron. Only 12 months before declaring bankruptcy in 2001, the largest in US history at the time, Enron received plaudits for its 64-page Code of Ethics. It was named ‘America’s Most Innovative Company’ by *Fortune* magazine and received numerous awards for corporate citizenship and environmental policies.”

One of the biggest mistakes firms make when designing a value system for their firm is not taking into account the thoughts of stakeholders. “The executive group usually get together in an afternoon meeting or have a conversation. They may do a more intensive process, but rarely does it involve the stakeholders. They don’t include staff. It’s rarely a bottom-up process. Typically, it’s partly a reputation marketing function,” says Neil.

Another huge mistake is when firms opt to change their values when changing the corporate strategy – thereby missing the point of a solid value system.

The Ethics Centre senior advisor David Burfoot says: “If you change your values every time you change your strategy, it is incredibly destabilising.

“IF THE MANAGERS OF AN ORGANISATION SAY ONE THING BUT CONSISTENTLY DO SOMETHING ELSE ENTIRELY, IT BREEDS A CYNICISM AND DISCONNECTION THAT PERMEATES THE ENTIRE WORKFORCE.”

Director of innovation,
The Ethics Centre
John Neil

People don't invest in them and that's where shadow values begin to arise, because people start saying: 'These are our values but *these* are the things we actually value.'

UNDER COVER OF DARKNESS

Some of the worst examples of shadow values in recent years came out of Australia's Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry –including billing customers for no services, charging deceased citizens' accounts, lending money to the disadvantaged and unemployed, thereby crippling them, and giving executives bonuses in excess of 300% of annual salaries.

Perhaps the worst example was the Dollarmites scandal at the Commonwealth Bank, which involved fraudulent acts against children. Dollarmites savings accounts are a well-known savings system that Australian parents can utilise through the school banking system and which many take advantage of. The Royal Commission was told thousands of children's Commonwealth Bank accounts were fraudulently set up by retail branch staff as part of a widespread scam to meet aggressive performance targets within the bank and therefore earn bonuses.

The scam involved staff either using the bank's money, loose change of their own cash to illegitimately activate Youthsaver accounts for financial gain.

They did this in cases where parents had signed up their children for school banking, often referred to as Dollarmites Youthsaver, but had not deposited money into the account within 30 days, according to the *Sydney Morning Herald*. If no deposit had been made, the sign-up would not count towards sales targets and financial rewards for staff.

A Fairfax Media investigation revealed that the scam was part of a broader culture of gaming financial incentives at the bank, where staff were caught faking customer referrals to boost performance targets and earn rewards.

CULTURE OF SILENCE

Neil says identifying the existence of shadow values is where the real work begins for an organisation. "Uncovering shadow values can reveal deeper facets of an organisation's actual operating culture. By proactively identifying and monitoring its shadow values, an organisation is better placed to see any early drift in the alignment of its culture from its values and principles."

"Consider the fraudulent behaviour of Volkswagen engineers, who deliberately programmed 500,000 diesel-powered vehicles to provide false readings during emission testing. Despite the company's explicit corporate values of excellence, professionalism and a commitment to integrity, it became clear through the accounts of investigators and employees, that a number of unofficial shadow values were dominating the organisation's culture."

An insidious culture of fear, with intimidation used as a primary motivator for achieving sales targets, is what drove Volkswagen's employees to continue the market deception, according to Neil. Fear provided a bulwark against any dissenting voice being raised to

challenge decisions. These voices were kept silent by a culture that fostered internal competition and secrecy.

WE NEED TO TALK

Burfoot argues that shadow values aren't always negative but the identification and management of them is important for an organisation.

"You can articulate the kind of guiding instruction processes and articulate the values within your organisation, but then there are the ways that people work that may be absolutely contrary to that, or may just be a variation on that. I think it's important to note that shadow values are not necessarily always negative influences. They can be kind of subtle nuances of existing values. But the point is we need to have an open conversation around risk culture, and culture generally. How do you measure it? What does it look like? And what actually is the culture in this organisation?"

University of New South Wales director of risk and assurance Trudy De Vries agrees that identification is key to risk managing this issue effectively. "The danger of shadow values is that if you're not cognizant of them, if you're not aware of them, then you're not going to be able to understand where a bias might occur in rating a risk or even identifying what the risk is."

Risk managers often talk about ethical frameworks and cultural frameworks. However, by using definitions such as these, says Neil, C-suites may be missing the point of what we are trying to articulate. "Organisations don't use the term 'ethical framework'. They talk about their corporate values and their vision and mission, etc. Increasingly, we are also seeing them talk about purpose, which is really important."

He continues: "The distinctions between a purpose and a vision and a mission is not just a technical one. It's also an ethical one. A purpose is a perennial foundation for what it is the organisation does, and it needs to be evaluated against its vision, which relates to its values, so often organisations don't make that connection. They're often kept as separate entities," Neil adds.

OUT OF SIGHT

Burfoot argues risk managers may struggle to identify shadow values within their organisation because of their elusive nature. "The reason shadow values can be so powerful in conversations is that they're not supposed to exist. And because of that, it evades all the controls."

He adds: "Basically, this risk is not counted. It's not on the list in the risk register. There's no audit programme for it, there's no control set up for it, because it's not supposed to be there. What gives them so much potency is that they aren't stated."

De Vries also says a culture of fear of reprisal will mean risk managers may never really know the true risks within their business. "If your shadow values are conservative and staff are frightened to do any wrong or to raise bad news, then you as a risk manager are not going to get the real issues in risk. You have got to understand what kind of shadow values are operating and how those might sway or skew the risk information you get."

"If you don't understand what is lurking below the surface, how can you manage those risk effectively?"

"THE DANGER OF SHADOW VALUES IS THAT IF YOU'RE NOT COGNIZANT OF THEM, THEN YOU'RE NOT GOING TO BE ABLE TO UNDERSTAND WHERE A BIAS MIGHT OCCUR IN RATING A RISK OR EVEN IDENTIFYING WHAT THE RISK IS."

Director of risk and assurance, University of New South Wales
Trudy De Vries

NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

**FIND OUT MORE AT
zurich.com/my-zurich**




**ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.**



ZURICH[®]

This is a general description of insurance products and services and does not represent or alter any insurance policy. Such products and services may be made available to qualified customers through appropriately registered companies of the Zurich Insurance Group in the Asia Pacific region, including: in each of Hong Kong, Singapore and Japan; Zurich Insurance Company Ltd (a company incorporated in Switzerland) which is registered in each of these territories; for corporate life solutions in Hong Kong, Zurich Life Insurance Company Ltd; in Malaysia, Zurich Insurance Malaysia Berhad; in China, Zurich General Insurance company (China) Limited; and in Australia, Zurich Australian Insurance Limited ABN 13 000 296 640.



Do you have what you need to navigate a complex world? You can.

AIG's multinational capabilities go beyond insurance, helping you achieve your risk and contract certainty objectives. Our global network of over 215 territories is backed by over 500 dedicated multinational experts. In every country you do business, you can count on expert local knowledge and insights. Our innovative technology and unique solutions unlock benefits like expert program design, streamlined process, and global visibility of your claims trends. And our service is unmatched. Let's get your AIG multinational program going. Visit www.AIG.com/multinational

Local expertise, worldwide.



All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. or its network partners. Products or services may not be available in all jurisdictions, and coverage is subject to actual policy language. Non-insurance products may be provided by independent third parties. For additional information, please visit our website at www.aig.com.