

# Strategic RISK

Risk and corporate governance intelligence

- > WORD FROM THE TRADE WAR FRONTLINE
- > NO OFF-THE-PEG RISK SOLUTIONS FROM THE ICONIC'S SARAH MCNAMEE
- > THE LATEST TOUGH TRUTHS FROM OUR #CHANGINGRISK CAMPAIGN
- > ETHICS: EVERYONE IS ACCOUNTABLE
- > WARREN BLACK ON RISK 4.0

ASIA PACIFIC EDITION [Q2] 2019 | Issue 24 US\$25



## SPRUNG AN ASSET LEAK?

Your intangible assets – your intellectual property, data, branding – are the precious value-drivers you may not know are ebbing from your organisation until it's too late. Time to tighten up. >



**XL Insurance**



# Get answers

Have questions about insurance? A claim? Or new and emerging risks? Wherever you are, you'll get direct access to the right experts – underwriters, claims professionals, or risk consultants that can help. So, if you need answers, we're ready to talk.

**Know You Can**

[axaxl.com](https://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.

Q2 2019  
ASIA PACIFIC EDITION

**StrategicRISK**

www.strategicrisk-asiapacific.com

**EDITOR**  
Asia-Pacific  
Lauren Gow

**PUBLISHER**  
Europe, Middle East and Asia-Pacific  
William Sanders

**COMMERCIAL DIRECTOR**  
Europe, Middle East and Asia-Pacific  
Adam Jordan

**HEAD OF EVENTS**  
Debbie Kidman

**MANAGING DIRECTOR**  
Tim Potter

**HEAD OF FINANCE**  
Paul Carey

**CONTENT DIRECTOR**  
Kin Ly

**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@  
strategic-risk-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

#### HEADING FOR BURN OUT?

You are one of your organisation's greatest intangible assets. So take care of yourself.

### ANALYSIS /VIEWPOINTS >P4

**We are the antidote > Sell insurers your story > Let's get radical > Still surprised by a crisis? > Let's push things forward > Before it's too late**

### PROFILE >P11

#### FINDING THE PERFECT FIT

THE ICONIC's Sarah McNamee discusses risk priorities for the fast-expanding online retailer.

### RISKS >P15

#### COMBAT FATIGUE

US versus China, UK versus Europe – how can companies navigate the political battle lines being drawn around the globe?

### SPECIAL REPORT >P19

#### IT STARTS WITH YOU

Asia-Pacific regulators are honing in on individual accountability for ethical conduct in businesses.

#### SIMPLE ETHICAL RULES

Complex systems fail in complex ways. These actionable guidelines show companies how to stay in the light.

#### IS YOUR WORKPLACE TOXIC?

Data from the Ethics & Compliance Initiative reveals sexual harassment, discrimination and abuse are still prevalent in many organisations.



The #ChangingRisk revolution continues >P23

### RISK FOCUS >P23

#### LEADING THE RISK REVOLUTION

This second installment from our #ChangingRisk campaign finds a risk profession galvanised to effect real change.

### SPECIAL REPORT >P31

#### COVER: THE VALUE YOU CANNOT GRASP

Loss of intangible assets like intellectual property, brand and data is a huge risk for businesses, so why is it rarely flagged on risk registers?

#### TAKE CONTROL OF LEAKING ASSETS

We take an in-depth look at the key ways an organisation could lose its grip on those precious intangible assets.

### FUTURE THINKING >P35

#### WHAT WILL RISK 4.0 LOOK LIKE?

As the Fourth Revolution rolls in, business as usual will never be the same. To handle this, risk managers must add critical items to their to-do list.

#### COMPLAINTS - WHO TO CONTACT

StrategicRisk adheres to the Editors' Code of Practice (which you can find at [www.ipso.co.uk](http://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](mailto: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](mailto:complaints@ipso.co.uk) or by post at IPSO, c/o Halton House, 20-23 Holborn, London EC1N 2JD.*

# Heading for burn out?

Risk is inherently stressful and, most likely, you are absorbing that stress every day. So I offer up a genuinely difficult challenge: take better care of one of your company's greatest intangible assets – you.



EMAIL > [lauren.gow@nqsm.com](mailto:lauren.gow@nqsm.com)

**A**t the moment the ink is drying on this issue of *StrategicRISK*, I will have completed a 25-day journey of more than 21,500 miles, across 22 time zones, three continents, with two pieces of luggage and countless double macchiatos. The jet lag is horrendous and I find myself working at odd hours and, often, on little more than a few hours' sleep.

Don't get me wrong – I am not complaining. This is all part of my job as a magazine editor on an international publication and travelling is something I genuinely love. But the personal toll this takes on me, and anyone else who travels like this for work, cannot be underestimated. According to *Psychology Today*, prolonged sleep deprivation is an especially insidious form of torture because it attacks the deep biological functions at the core of a person's mental and physical health.

I have spent a lot of editorial this year, and in fact dedicated much of this issue, to highlighting the often-missed intangible asset risks within organisations. However, what had not occurred to me until my most recent trip is that I am neglecting to risk manage the most important intangible asset – myself.

Like everyone, my ability to perform my job to the highest standard possible relies on my mental stamina. Protecting and nurturing mental health is becoming more important in every workplace and it has long been a passion of mine. And yet, how quickly I forget this when I am under pressure. The need to do more, to say yes to everything, be everything to everyone and an overwhelming burning desire for perfection often leaves me on the brink of burning out.

As risk managers, your job is inherently stressful. The very definition of risk means 'exposing someone or something of value to danger, harm or loss.' You are

dealing with crises or trying to predict and stop a crisis before it occurs. Every day, you are pulled in multiple directions across your organisations and must manage multiple stakeholder expectations within often unrealistic timeframes.

There is no doubt in my mind that this pressure must take its toll on you as individuals. Especially when you feel this hard work is undervalued by your organisation. One risk manager in Singapore recently said to me: "Sometimes I wonder why I bother. Management don't even read my reports." To this person: you are not alone, trust me. I hear this much more often than I care to.

As you read through our special report on protecting intangible assets or check out Warren Black's latest piece on preparing for the Fourth Revolution, I want you to consider your own value as an intangible asset. Your value to your organisation should not come at any cost. Whether it be the long hours you work in the office sandwiched by a long commute, or checking your phone for emails while also trying to reading your kids a bedtime story or enjoy time out with friends, all of this takes its toll on you.

We all need to get better at risk managing ourselves. I don't know one person who does it well. As a collective, we need to put more value on ourselves and our time. I am sure, like me, most of you love what you do, but that doesn't mean it always loves you back. Take care of yourself because unless you do, everyone loses and how will we risk manage our way out of that one?

I have a challenge to you, my readers, for the remainder of 2019. Sure, work your hardest. But go for that run. Take an afternoon off because it is sunny. Sleep. Don't check your phone at the cinema. From this I can guarantee, we will all manage our intangible asset risk better. What organisation wouldn't want that kind of experience?

**"I AM SURE, LIKE ME, MOST OF YOU LOVE WHAT YOU DO, BUT THAT DOESN'T MEAN IT ALWAYS LOVES YOU BACK."**



# yes.

WE CAN TAILOR THAT  
COVERAGE FOR YOU.

**Berkshire Hathaway Specialty Insurance is pleased to bring underwriting flexibility, claims handling excellence, and financial strength to the Asia Pacific region. Our experienced team is committed to providing the customised coverage you need.**

Property | Casualty | Executive & Professional Lines | Healthcare Liability | Accident & Health  
Cyber | Marine | Energy | Surety | Terrorism | Construction

*All products may not be available in all countries.*



**Berkshire Hathaway  
Specialty Insurance**

[www.bhspecialty.com](http://www.bhspecialty.com)

Australia | Hong Kong | Macau | Malaysia | Middle East | New Zealand | Singapore  
Canada | Germany | Ireland | UK | USA

# We are the antidote

A survey by insurer QBE quantified businesses' concerns over our unpredictable future. The remedy? Risk management and strategic planning.

**B**usiness leaders see the world becoming less predictable, posing a threat to revenue. A survey by Australian insurance giant QBE found that solid risk management and disaster planning was the "antidote" to concern over the future.

The insurer's annual predictability index tracks a set of business, economic, environmental, political and societal indicators to understand how easy it is to forecast future events at any given time.

QBE's study found that in the immediate future, businesses were facing unpredictability from Brexit and global trade wars. But looming in the distance is the threat from climate change, an aging population and new technology.

Ongoing uncertainty over Brexit is thought to explain why only 42% of UK business leaders surveyed said the business landscape over the next year was predictable. That compares to two-thirds of bosses globally who said they knew what to expect from the future. Of those in big businesses, 82% said they considered unpredictability to be a bad thing for their company.

## UNPREDICTABLE TIMES

The index, which looks at a set of indicators dating back to 1978, illustrates that the world has become more unpredictable. In fact, almost all of the "least predictable years" in the index have occurred in the past 20 years, with the majority falling during the past decade.

"This increase in unpredictability is largely driven by deterioration in political stability since the millennium, compounded by the economic and political fallout from the 2008 financial crisis," said QBE. "Politics stands out as the biggest driver of unpredictability. Political instability started to rise following the 2001 terrorist attacks in the US and has continued over the last decade with a huge rise in electoral and policy-related instability."

Meanwhile economic factors are the biggest concern for businesses looking three to 10 years into the future. However, this unpredictability affects different companies in different ways. Manufacturing companies and retailers, for example, are vulnerable to disruption in trade or their supply chains, while service companies are more likely to be concerned with regulation and cyber.

"According to the index, the biggest impact of unpredictable events is loss of revenue, unexpected

**THE STUDY FOUND THAT BUSINESSES WERE FACING UNPREDICTABILITY FROM BREXIT AND GLOBAL TRADE WARS, PLUS THE THREAT FROM CLIMATE CHANGE, AN AGING POPULATION AND NEW TECHNOLOGY.**

costs and decreased demand," QBE said.

It noted that the further forward businesses look, the less confident leaders feel about being able to predict what will happen. However, many of their companies have to plan more than a decade ahead.

QBE said: "Companies may have to invest in new business models at a time of fast-changing technology and consumer trends. AI and automation, for example, will have huge implications for the workplace and wider society, while political and environmental factors could lead to big changes in demand for goods and services. Yet predicting the how and when is beyond most companies."

The insurer said that increased unpredictability compounded the issues for business planning and strategy setting, but noted that could be minimised if those organisations focused only on the most critical factors to them. "There is a lot of noise surrounding issues like Brexit and global trade disputes, and this is likely to continue for several years to come. But companies should step back from the media headlines and not get bogged down with the issues of the day – there are likely to be long-term trends out there that are more relevant to the future success of a business."

## RISK TO THE RESCUE

The insurer said the antidote to unpredictability is likely to be found in the development of risk management and scenario planning. It argued that better information would be the key to managing unpredictability in the future.

"We already see an increasing number of companies spending time on risk modelling and scenario planning, thinking about unexpected or difficult-to-predict events," QBE said. "However, the collection of risk data is often not as comprehensive and as structured as it could be."

The survey found that fewer than two-thirds of respondents used economic data to help plan for their future. Nevertheless, three-quarters said that they felt prepared for unforeseen events.

To combat those events, QBE said "what-if" thinking could help businesses prepare for the worst by identifying risks to critical services and supply chains. "Whether it's an unexpected election result or an extreme weather event, businesses are clearly operating in unpredictable times. More sophisticated risk management and scenario planning could be the antidotes to growing unpredictability."

# Sell insurers your story

You will be best-placed to navigate your organisation through this hard market if your insurer knows who you are and what you need. Allied World Asia Pacific's Carolyn Shreeve offers practical advice.

**R**electing on renewals in the first half of 2019, there is no doubt the insurance market is hardening across most lines. For many, this may be their first experience of tougher market conditions as the market has been relatively soft since 2001. The Asian market has seen more than 15 years of favourable market conditions for buyers.

One of the most important things insurance buyers need to be doing is selling their story to insurers. Insurers are making assumptions about your business, so remove any ambiguity. Work with your broker to ensure all of your submission information is up to date, evaluations have been done on the assets you are seeking to have insured and that your claims records are all current.

By doing this you are building a relationship with your insurer, which is critical in a hard market to ensure you are receiving the best possible coverage and value. By building a relationship with your broker and insurer, you can be sure that the right story is being sold. To do this, you need to have a full understanding of what your insurance needs are and whether other risk mitigation

**“BUILDING A RELATIONSHIP WITH YOUR INSURER IS CRITICAL IN A HARD MARKET TO ENSURE YOU ARE RECEIVING THE BEST POSSIBLE COVERAGE AND VALUE.”**

Chief underwriting officer,  
Allied World Asia Pacific  
**Carolyn Shreeve**



strategies can be employed (see boxout 'Know what you need').

Once you have built a clear picture of your internal risks and have your C-suite on board, then it is time to look at the picture externally. Below is a checklist of the questions and steps you need to take to get the best from your insurers (see boxout 'Get the best from your insurer').

Following these practical tips will not only help you navigate your company through difficult market conditions, but it will have the added benefits of developing a long-term working relationship with your insurance carrier – giving you the optimum risk oversight for your organisation.

## KNOW WHAT YOU NEED

Here are the three things you need to do to understand your insurance needs.

### ENGAGE C-SUITE

Ensure they understand the changing dynamics of the insurance market

RE-ESTABLISH INTERNAL RISK APPETITE and tolerance

### PLAN IN ADVANCE

Give yourself time to debate options

## GET THE BEST FROM YOUR INSURER

Follow this checklist of the questions and steps you need to take to get the best from your insurers.

### DRIVE WHAT'S IN YOUR POLICY

- Do you understand all the coverages and extensions provided?
- Does it provide the risk transfer you want?
- Are limits/sub-limits/deductibles reflective of your current risk appetite?
- Can you stress test vs realistic scenarios?

### BUILD UNDERSTANDING

Avoid any ambiguity or assumption by the broker/insurer, e.g.:

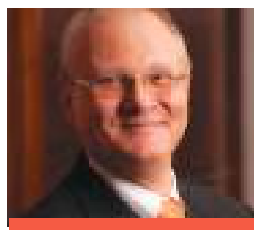
- Is the schedule/submission information up to date?
- Is your claims record up to date?

### BUNDLE PRODUCTS

Can you cross-market your insurance products to the same carriers?

# Let's get radical

Throw out the risk models, the decision-by-committee, the lines of defence – if you have an effective risk culture, you don't need them. Horst Simon outlines his radical risk management process.



**“IN THE ULTIMATE RISK CULTURE, EVERY PERSON WILL CONSTANTLY EVALUATE, CONTROL AND OPTIMISE RISKS TO MAKE INFORMED DECISIONS AND BUILD SUSTAINABLE COMPETITIVE ADVANTAGE.”**

Risk Culture Builder  
**Horst Simon**

**I**f you are still trying to identify all the risks you are exposed to within the context of your business, or spend endless hours converting historic data into useless risk reports in an effort to mitigate as much risk as possible for a green light on the road to taking less risk (for less reward), or spending a fortune on controls and the digging of trenches for your lines of ‘defence’... Fear no more!

The radical risk management process is here and the future is bright for those who choose to go through the disruption of dumping outdated thinking, concepts, models and processes. These are things like risk management ‘process’, based on the assumption that it is possible to identify all the risks you are exposed to and then follow a dedicated process of mitigating all those risks, as well as ideas like ‘green is good’ and the three, four, or even five ‘lines of defence’.

The management of risk is not a technical process of data gathering, evaluation and reporting at consistent intervals, with an expectation of a different outcome; or even ‘improvement’.

## FOUR KEY ELEMENTS

This radical process involves only four components:

- Situational awareness – perceiving elements in the environment and projecting their future status.
- Mental simulation – imagining taking a specific action and simulating the probable result before acting. This improves our ability to solve new problems.
- Naturalistic decision-making – how people make decisions and perform cognitively complex functions in demanding, real-world situations.
- Response execution – once these steps are complete and a response has been selected; the response, or action, must be executed.

These are built around key elements of an effective risk culture:

- Risk intelligence gathered from everywhere (not just last quarter’s outdated risk report).
- A risk nervous system through which this

information can flow everywhere in the business (not a process of sanctification where reporting gets better the higher it goes).

- Competencies and skills in all employees to manage the risks associated with their jobs daily and ultimately build sustainable competitive advantage for the organisation (no levels of assurance, squadrons of policemen or lines of defence; there is nothing to defend against).

In the ultimate risk culture, every person will constantly evaluate, control and optimise risks to make informed decisions and build sustainable competitive advantage for the organisation.

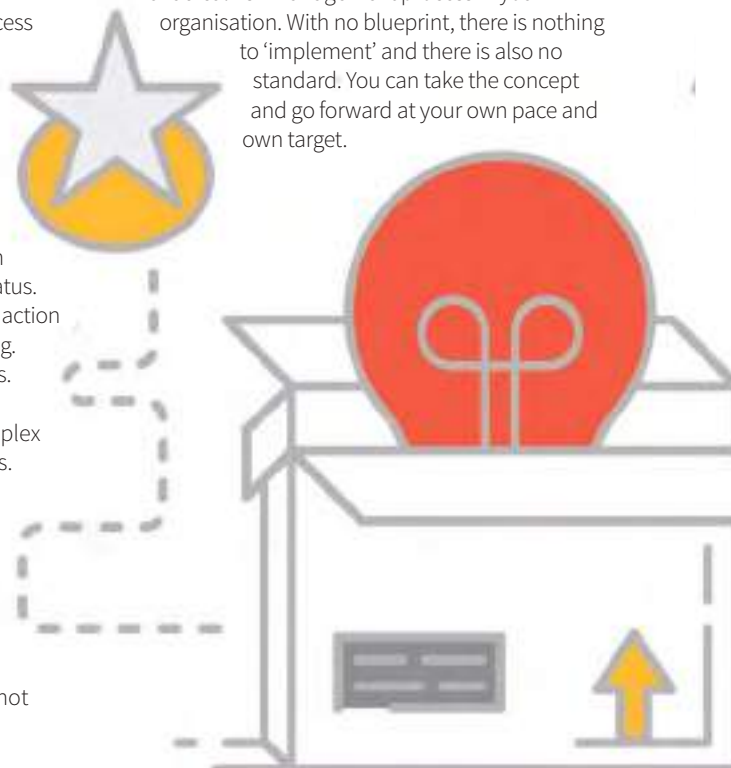
Success depends on the levels of accountability you drive in your organisation. Do not even attempt this if you are going to keep a process of making risk decisions in committees where these decisions are ‘syndicated’ without anybody taking any accountability.

## IF YOU BUILD IT

There is no blueprint – you have to build the unique process in your organisation, based on the underlying corporate culture and organisational structure, and focus on driving the behaviours you want to encourage and those you want to avoid.

You need to take each of the four components and develop these within the context of your business strategy, goals and objectives. If a risk will not prevent you from reaching your business goals, don't worry about it; you can never identify all the risks you are exposed to. The key factor is how your employees will respond to a situation of risk in ‘real-time’. Business is not a game and business decisions based on last quarter’s risk report are not such a good idea in real-life.

You have to research each of these four components and apply your learning to your organisation to build a radical risk management process in your organisation. With no blueprint, there is nothing to ‘implement’ and there is also no standard. You can take the concept and go forward at your own pace and own target.





# Still surprised by a crisis?



The myriad of disasters that can hit are nothing new, yet companies are still often caught under-prepared, marvels risk specialist Gabriel Souza.

**W**e all know that we are living and working in a more volatile, uncertain, complex and ambiguous world.

So why, then, do we still underestimate the necessity

to prepare our businesses and tackle the challenges of a volatile environment in a structured way? Why do businesses continue to struggle to address the same problems, like floods, hurricanes and diseases outbreaks? Why do companies continue to lose billions of dollars every year as a result of cyber attacks, facilities damage, security? Why do the executive management of so many companies continue to ignore the fact that unexpected events can destroy their companies?

In Deloitte's 2018 Global Crisis Management Survey, 84% of the companies said they had crisis plans in place, as well as continuity plans and incident management plans. But, if we asked them how their plans are structured, we would likely see inconsistencies, out-of-date procedures, and stakeholders ill-prepared to deal with events that could harm the company.

Creating and enacting an effective and structured plan for crisis management is not simple. It should involve the following:

**Establish a crisis committee** with all the required personnel. It is important to mention that the committee can vary depending on the breadth of the crisis. And, of course, the C-level management has a reserved seat in all events.

**Understand the possible outcomes** using risk management. It is essential to identify all the potential events, as well as the impact and consequences.

**Develop structured procedures** to tackle each possible event. Steps should be mapped precisely, and responsibilities defined. It is essential to then define the recovery time objective for the event and then simplify this against the steps that have been mapped out.

During a crisis, personnel will likely feel high levels of stress, which can complicate a crisis recovery. People must feel supported by a practical document/system that is to the point and avoids overthinking.

**"IF WE ASKED COMPANIES HOW THEIR CRISIS PLANS ARE STRUCTURED, WE WOULD LIKELY SEE INCONSISTENCIES, OUT-OF-DATE PROCEDURES, AND STAKEHOLDERS ILL-PREPARED TO DEAL WITH EVENTS."**

Risk management specialist,  
**Gabriel Souza**

**Treat business continuity separately.** Many combine the concept of crisis management with business continuity. It should be treated and seen as two separate perspectives – after all some crises may not interrupt a company's operations. But it is important to understand how a crisis can impact the operations.

**Effective communication** with employees, customers, public agents, insurance companies, shareholders and any other stakeholder that must be involved in the crisis is critical. The Achilles heel in most crises lies in a failure to communicate effectively. But worse is a failure to be transparent with all stakeholders, particularly customers. Best practice requires you to:

- Identify and detail all stakeholders that should be involved in any crisis management. The document must inform the roles, responsibilities description, names, contacts and any other relevant information.
- Define the face of the company in a crisis, who will speak to the press, employees and suppliers. They must have in-depth knowledge of the company, be confident and have undertaken media training.
- Define a 'hot line' through which all external agents can communicate. A big mistake is in not creating open lines of communications between external and internal crisis management personnel. Identify all communications channels, including social media, press, intranet, etc, and define how to communicate through these channels during and after the crisis.

**Learn from mistakes.** Unfortunately, crisis management is not always performed as we planned. Thus, after every crisis, it is vital to have an assessment and create a database of lessons learned to be used to enhance plans and mitigation for future events.

**Prioritise people's safety** in every plan. This must be followed by the kindness and altruism to provide the support and infrastructure required for victims and their families.

This is just a glimpse into how we need to be structured and respond to harsh scenarios and guarantee that infrastructure, money and people's lives are not lost owing to a lack of preparedness.

# Let's push things forward

This year's Risk Forum APAC in Singapore inspired delegates to bust through silos, build bridges with the C-suite, and think strategically about the risk tools they use.

**“COMPANIES WITH PURPOSE PERFORM BETTER.”**

**KURT MEYER, FORMER CHIEF RISK OFFICER, SWISSGRID AND CO-CEO, RISK TALK**

Meyer said it was critically important for organisations to make sure that employees are aligned with a company's values, both for the good of the company's performance and in order to manage risks effectively.

He said: “You need to monitor how cultural values are understood in the firm. These are often at the heart of the problem, so if you are able to manage values then you are also well placed to manage risks.”

The most obvious way to do this, he said, is to walk around a company asking people how they perceive the risks an organisation faces and the values they stand for.

Of course, in larger organisations this is nearly impossible and that's where technology comes in. Using simple tools, everyone in your organisation can make suggestions for improvement, identify risks and you can track how they perceive company values.

“So you don't just have a handful of people reporting to the CEO but hundreds of people reporting with this tool,” said Meyer.

Once you have the data, you then need to make sure it is acted on. The outcome of measuring values is a successful business, according to Meyer. He gave the example of Johnson & Johnson.

“Johnson & Johnson have a marble stone in their entrance with their credo engraved on it. It says that at the core is not profit but the well-being of the patients, and profit is just a natural outcome of adhering to this credo. If you look at the share price of J&J, it does not only outperform S&P but also the benchmark. Companies with a purpose perform better.”

But how can risk managers embed this thinking in their own employers' businesses? Meyer recommends asking the following question: Do the actions of the company correspond to

its espoused value and priorities as per the board's strategic intent and the firm's corporate purpose?

The benefits of knowing the answer to this question, he explained, include:

- Corporate integrity – actions of the company are defensible if aligned with core values and priorities
  - Motivation – employees are more willing to work in a firm where they have integrity, especially Gen Y and Z
  - A holistic picture – risk managers can produce top-down, bottom-up lateral and outside risks
- All of which leads to risk management at the core of an honest dialogue about things that really matter.

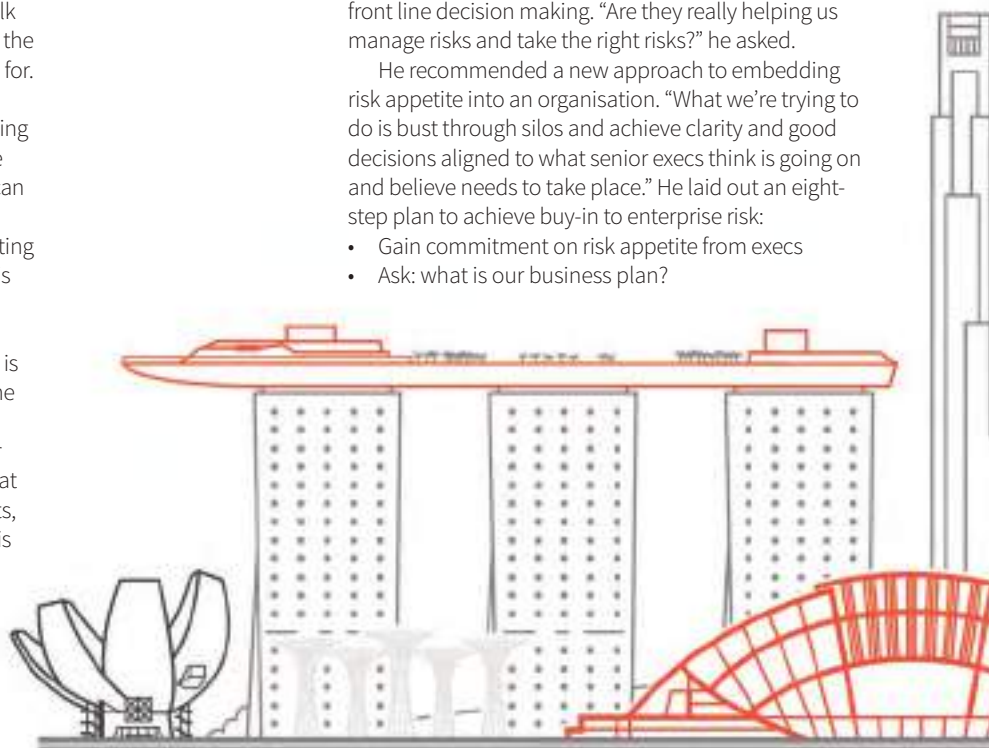
**“YOU HAVE TO USE RISK APPETITE STRATEGIES WELL.”**

**GARETH BYATT, PRINCIPAL CONSULTANT, RISK INSIGHT CONSULTING**

Risk appetite strategies can be a great way of taking risk to a strategic level, but only if they're used properly, said Byatt. He argued that while they are a good process, too often they are not part of the business strategy, not really used in operations and not used for front line decision making. “Are they really helping us manage risks and take the right risks?” he asked.

He recommended a new approach to embedding risk appetite into an organisation. “What we're trying to do is bust through silos and achieve clarity and good decisions aligned to what senior execs think is going on and believe needs to take place.” He laid out an eight-step plan to achieve buy-in to enterprise risk:

- Gain commitment on risk appetite from execs
- Ask: what is our business plan?



- Ask: what are our risks?
- Ask: what's your appetite for those risks?
- Then try to describe this appetite for risk
- See if you can quantify the appetite
- Collect and review with management
- See if adjustments need to be made

You need to keep it simple, use it as an excuse to connect with people and make sure that what you produce is honest. Byatt emphasised the importance of change management practices. "One of the things I often find with risk appetite is that change management is an important piece. If you are implementing something new, be aware of some implications of change."

## "WE MUST MOVE BEYOND HEAT MAPS."

**PATRICK ADAM K. ABDULLAH, VP, ENTERPRISE RISK MANAGEMENT, ASTRO OVERSEAS LTD**

### Are current risk management tools fit for purpose?

According to Abdullah, probably not. While such tools are a good way of registering risks, they have severe limitations, he told delegates.

They do not act as an information management tool that is used to track KPIs, metrics and other key data points relevant to a business by simplifying complex data into digestible chunks. They do not gather data from multiple data points to provide a single reporting interface. They do not offer instant access to information on various parameters such as financials, valuations, risks, etc.

They cannot carefully structure various data points to highlight areas that need improvement. They don't enable the board to act on events as they occur.

They don't help with quick decision-making. They can't help organisations to be more efficient in managing strategic initiatives and operational targets. And they do not provide the right indicators that allow businesses to address key strategic needs.

Instead, Abdullah argued, risk managers should be considering a shift towards risk dashboards, which are designed to give real-time reporting that can help businesses meet KPIs,

make growth decisions and identify core risks and opportunities. Such tools could save time, provide snapshots of how a business is performing and easily spot ongoing trends, so the C-suite and board can see where the challenges lie and decide how to deal with them.

"We talk about change and a more futuristic way of reporting risk. But the most important thing is the maturity of the company. Can the organisation and board accept the new way of reporting risk that infuses parameters into one dashboard and gives a snapshot of how the business is doing? You need to sell that idea to the board and the senior leadership team."

## "THE OLD MODEL IS BROKEN."

**SUCHITRA NARAYANAN, FORMER HEAD OF RISK AND INSURANCE, AIRASIA**

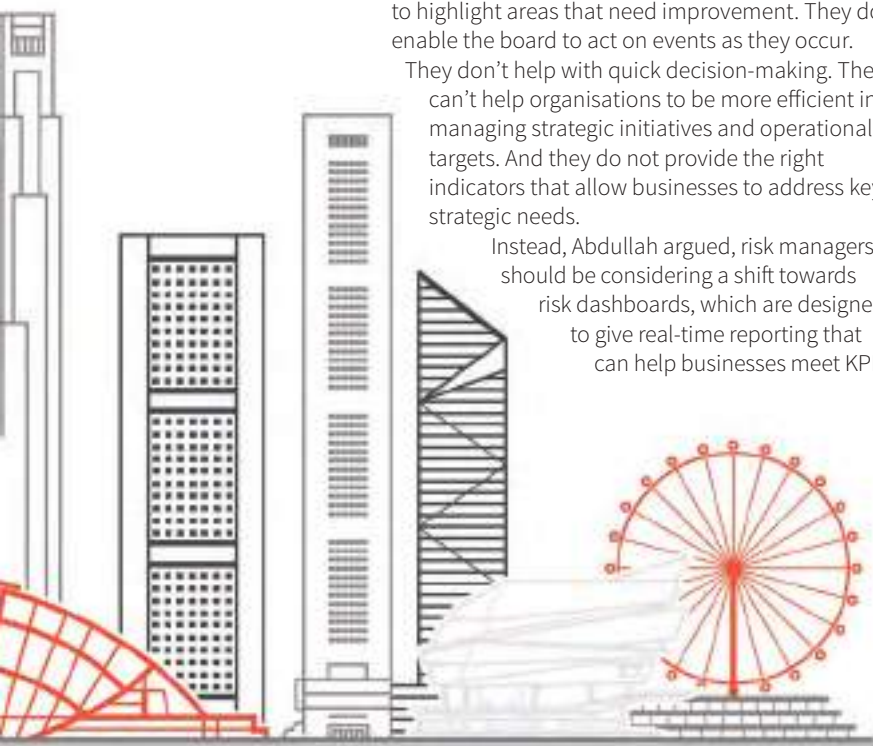
### Narayanan is an advocate for change in risk

management, believing the old model is broken and we must become more relevant. She highlighted several core issues:

- Value and relevance: "Where should risk management sit and how does it truly add value?" she asked. "I am often amazed when I ask risk managers who they report to. It's just fascinating that sometimes risk management doesn't have a place in the organisation where it has visibility. That's one thing that should change in a lot of organisations."
- Competencies and skill sets: "Doctors, lawyers and accountants have a body; they have to do exams. I think about what we really need from risk managers and if we're not sure ourselves then how do we expect our CEOs to know?"
- Strategic decision-making: "Risk information often doesn't feed into strategic decision-making. When you don't get the feedback, it causes a lot of frustration. We're providing research and information and we need to know how it is being factored into the real decisions that boards make."
- Confusion about the role: "People think risk, compliance and audit are the same thing. We need to communicate how they are different."
- Out-of-date tools: "The tools we use can be sometimes archaic, ineffective and don't communicate to management what they need to know. If you can't communicate what they must know in two minutes then you've lost them. They want to know: 'What do I need to worry about today, how do I deal with it and how can you help me get there?'"

To change all of this, Narayanan argued that risk management needs to change. Risk managers need to challenge senior managers, add value and be more strategic.

She added: "We need to think about larger issues. Reputation, brand and shareholder values – these are real issues that affect organisations and we need to be part of that."



# Before it's too late

Reflecting on April's devastating terrorist attack in Sri Lanka, Suchitra Narayanan explains why risk managers must demonstrate care, conviction and courage to ensure their warnings are heeded.



**“IT’S EASY TO BLAME MANAGEMENT FOR NOT BEING COMMITTED TO THE DISCIPLINE OF ROBUST RISK MANAGEMENT BUT IS THIS BECAUSE THE MESSAGE IS NOT STRONG ENOUGH?”**

Former head of risk and insurance, AirAsia  
**Suchitra Narayanan**

**O**n Easter Sunday, I sat glued to my phone and the television, horrified at news of the terror attacks in Sri Lanka. I ruminated upon the thought that we live in such a volatile world today. Everything seems to be constantly changing, be it politics, technology or social media.

The news reports stated that the Sri Lankan government had been warned of the attacks a couple of weeks before they took place and again hours before. The warnings were purportedly specific, which made me wonder – how often do companies ignore warning signs and, essentially, risk management?

No one likes to hear bad news, so this makes the intrinsic messaging of risk a hard one to deliver. It's easy to blame management for not being committed to the discipline of robust risk management but is this because the message is not strong enough? Relating this back to the terror attacks, I asked myself if the warnings were not acted upon perhaps because the message was not conveyed in the right way.

## MAKE YOUR MESSAGE MATTER

Messaging is such a simple concept, but probably one of the hardest things in reality to deliver as a risk manager. I draw upon my own experiences where I have sometimes struggled to convince CEOs of the importance of issues that I felt needed to be conveyed. The benefit of hindsight, of course, is that I know now what I could have done differently. This brings me to something that I affectionately refer to as the three Cs: care, conviction and courage.

For a message to matter, risk managers naturally need to care enough about the content. The most worthwhile risk-based conversations I have had with management have been those where I genuinely cared about the company that I worked for and I was able to put myself in the shoes of the CEO. People can sense care, people react positively to it and so it makes tough messages much easier to communicate and discuss.

When I first started working in risk management, I would approach each meeting, each engagement, with much trepidation. I wasn't always sure what I was and wasn't meant to say and

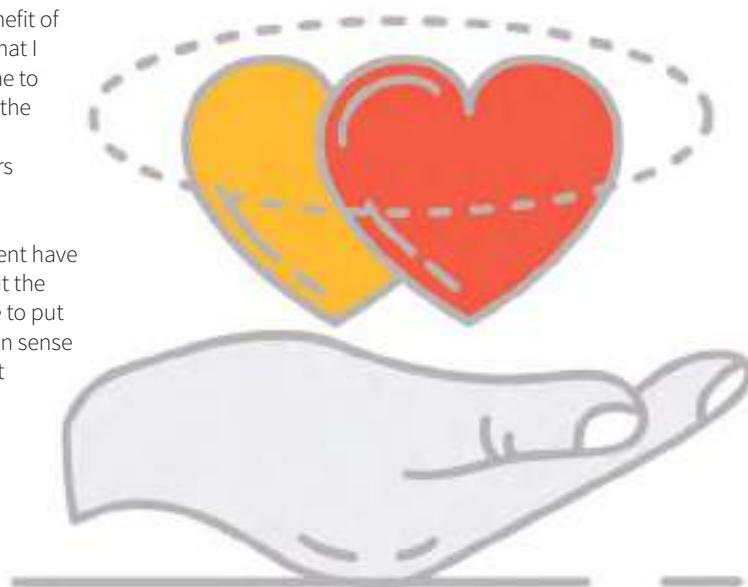
what management wanted to hear. I learnt the hard way: when questioned, I would often fumble, out of nervousness, and be met with sometimes perplexed, sometimes agitated looks.

I quickly grasped the fact that conviction is so very important. Know the content, and anticipate questions you might be asked (though it is okay to not know all the answers as long as you're honest), and stand firm in that conviction. It is a trait that gains trust and respect.

## DON'T SHOOT THE MESSENGER

Risk managers, it's no secret that we are often the most disliked messengers in the organisation. Financial risks, strategic risks, liquidity risks – we need to bear the burden of delivering the sometimes unpleasant messages. This requires courage – lots of it. I am still developing courage as I go along and the one thing that inspires me to be courageous is the glimpse of change. For it is courage that is going to take risk management to greater heights and for risk managers to be heard.

My mind wanders back to Sri Lanka. I can't help but think, if only the warnings, the unwelcome messages, had been taken more seriously. I don't have the ability to change the world but I can change the way I, as a risk manager, deliver my messages so that people listen, take note and most importantly, act before it's too late.



A portrait of Sarah McNamee, a woman with long blonde hair, wearing a light blue button-down shirt, smiling at the camera. The background is a plain, light-colored wall.

# Finding the perfect fit

---

Online retailer THE ICONIC is the very definition of a maturing start-up. Its head of risk & controls, Sarah McNamee, is dedicated to ensuring the board sees risk management as a must-have staple.



**P**aris, Berlin, London, Stockholm. Sarah McNamee has worked in some of the world's most glamorous locations in her risk, compliance and audit career to date. So taking on the role of head of risk & controls at Australia and New Zealand's fastest growing online fashion and sports retailer, THE ICONIC, was a natural fit.

Sydney native McNamee's impressive career has already spanned a number of continents and industries, taking in some of the world's biggest companies along the way.

She graduated in 2008 from Macquarie University in Sydney, holding a double-degree in Commerce Accounting and Business Administration Marketing.

McNamee began her career with advisory firm Deloitte, picking up a graduate role covering process improvement and some elements of risk. Like most in the industry, she did not set out for a career in risk management, but quickly grew to appreciate the analytical nature of the work.

In 2013, she relocated to London to work for consultancy firm Protiviti, providing advice to fast-moving consumer goods companies, media and pharma businesses.

Moving back to Sydney with Protiviti, McNamee's risk career took off with a role focused on risk governance and risk consulting. Helping clients plan and execute risk management strategies piqued her interest in spotting risks and operational challenges on the horizon.

"That's where I stepped away from audit and fully into risk work, and where I started to see the value in risk management as part of businesses' wider strategies," she says.

McNamee then became risk and audit manager at Coca-Cola Amatil, the regional division

of the global drinks giant, helping the company focus on competition, adapting to a changing regulatory environment, and managing operational risk. She reported to board committees about present and future challenges, such as the global trend away from sugar and its impact on the beverages market.

"The company had a traditional but effective risk management approach, and it was about bringing conversations to the board and trying to influence decision-making," she says.

#### FAST FASHION

McNamee joined THE ICONIC in July last year, taking on the newly created role of risk & controls manager. The position, covering strategic risk and controls and insurance coverage responsibilities, was handed to McNamee as the company sought to formalise its risk management operation.

McNamee's risk function sits separately from other areas of the business, giving her a "helicopter" view of the company.

"In order to be effective, you need independence for your controls framework," she says. "I report to the CFO, and in a dotted line to our parent group, Global Fashion Group."

THE ICONIC, which sells everything clothing, from designer shoes to luxury sportswear, for women, men and kids, was founded in 2011. The retailer has grown quickly, from boasting just five employees at its inception to more than 950 today.

The company generated more than \$267 million in sales in 2017 and has a goal for revenues to hit \$1 billion in the next three years. This growth comes as consumers, particularly younger shoppers, continue to abandon the high street in preference for making selective and savvy online purchases, with the greater convenience and choice it offers.

---

**"AT EVERY LEVEL AT THE ICONIC, RISK MANAGEMENT IS SOMETHING WE'RE KEEN TO PROGRESS. THINGS ARE MOVING SO QUICKLY, AS ARE THE RISKS."**



McNamee describes THE ICONIC as a “maturing start-up”, with an established footprint in its field. With any fast-growing start-up comes challenges, however, particularly in the tech-driven online space. Growth, new markets and competition are “part and parcel” of the issues growing companies have to focus on, she says.

McNamee is responsible for implementing the retailer’s risk management and control framework, and “establishing it across the business”.

“At every level at THE ICONIC,” she says, “risk management around our processes and systems is something that is hugely important to us and we’re keen to progress. With our high-growth environment and the evolving nature of our company, things are moving so quickly, as are the risks.”

So what risks does a growing online retailer think about? McNamee says remaining relevant, having the best and most inspiring assortment at the best price, the flexibility to scale in line with our growth and the agility to respond to changing preferences, ultimately creating a seamless experience for our customers.”

Of course, being an online business, safeguarding data also poses a unique challenge. “Data governance is a big issue. Data is core to our decision-making and, increasingly, we’re using big data. The way you collect, manage and use data is hugely important to

support accurate and effective decision-making,” she says.

Data privacy is also front of mind. “With global best practice development, such as [the EU’s] General Data Protection Regulation, it’s about ensuring we treat customers’ data correctly, and make sure it is safeguarded.”

THE ICONIC is focused on keeping information safe and secure, in a world where even global heavyweights have been brought to their knees by malicious attacks. “Cyber security is an inherent risk,” McNamee says.

“There’s a new issue almost every week and a new article about a breach somewhere. Fraudsters are always trying to be one step ahead of the game. It’s about protecting our customers, managing reputation and mitigating the damage as well.”

#### TAILORED APPROACH

So how different is the approach to risk in such a maturing start-up?

“Everyone is on the journey and believes in the values of the company. The principles of THE ICONIC are core to its decision-making. It’s my challenge to make risk management relevant to key stakeholders. The number of hours I have with which to do that is limited, so my job is to articulate how decisions impact the risk management framework, and how they fit in with our values.”

McNamee says it is her role to help senior executives understand risk in a practical sense, and

**“CYBER SECURITY IS AN INHERENT RISK. THERE’S A NEW ISSUE ALMOST EVERY WEEK. FRAUDSTERS ARE ALWAYS TRYING TO BE ONE STEP AHEAD OF THE GAME.”**



how issues might impact customers, the company's most important commodity.

"If the customer is core to our decision-making, how do I represent this risk in terms of our customers to key stakeholders and our executive team. It comes down to knowing your audience and making it relevant to them. It's making sure they are aware of the key risks facing our business and having the right tools in place to effectively mitigate these risks," she says.

As THE ICONIC continues to grow, McNamee's risk role will continue to evolve. She loves the changing nature of the job, as new risks emerge for the business.

"No two days are the same. But the ability to effect change, and deliver on initiatives as a risk manager is much greater in a high-growth environment. I see the future of my role as helping support the business in taking the right risks to support our continued growth."

McNamee has learned a lot about start-up risk management over the past year. Her biggest piece of advice to risk managers in smaller companies? That risk is not a one-size-fits-all function.

She adds: "Listen to your stakeholders, understand what's important to them. Develop a framework that supports their needs as well as delivering a risk management function."

"Don't try to emulate a standard approach. The tried and tested risk management model may work for a larger company, but for a start-up, the nature of decision-making and the pace of change requires a framework and approach that's practical and resonates with the culture of the business."

**"I SEE THE FUTURE OF MY ROLE AS HELPING SUPPORT THE BUSINESS IN TAKING THE RIGHT RISKS TO SUPPORT OUR CONTINUED GROWTH."**

## THE ICONIC: VITAL STATS

The fashion retailer is growing fast as customers abandon the high street for the convenience and choice of online shopping.

 **5** → **950**

employees when founded in 2011... and in 2019

**1,000**

name brands on offer



**3hr**

Available delivery within Sydney

**\$267m**

sales generated in 2017

**\$1bn**

Revenue goal for 2021



**60,000**

items stocked at any time

**200+**

new arrivals land daily

**12m**

website hits per month



# Combat fatigue

---

From China and Trump to Brexit and Brussels, the world in 2019 is one political battleground. As global companies live in fear of impending economic catastrophe, what can they do to avoid becoming a casualty of trade war?



**U**S president Donald Trump began Monday, 6 May in typical fashion. Taking to Twitter in the early hours of the morning, he kicked off the day by making public threats against China – escalating the high-stakes trade war between the two global superpowers that has left economists fearing a global economic downturn.

He proclaimed to his followers: “The United States has been losing, for many years, 600 to 800 billion Dollars [sic] a year on trade. With China we lose 500 Billion Dollars [sic]. Sorry, we’re not going to be doing that any more!”

The US president has shown no sign of backing down after launching an aggressive trade war against China in early 2018. Trump has outlined plans to double tariffs on \$200 billion of Chinese goods, while China has introduced its own tariffs since the beginning of 2018.

The trade war has left global companies and risk professionals scrambling to assess the impact on supply chains and consumer demand. Like so many

**“THE RIPPLE EFFECTS OF THE CURRENT CHINA-US TRADE RELATIONS ARE BY NO MEANS CONFINED TO CHINA... DISRUPTION IS ALREADY PLAYING OUT AROUND THE GLOBE.”**

Risk report  
PwC

other political risks in 2019, market observers are unsure whether things will get better or worse.

#### ON THE EDGE

The US-China trade war is one of several global political risks facing multinational companies in 2019. Nearly every global company has deep connections with the US and China, and the trade war has already damaged political relations between China and allies of the US. The ongoing friction is yet to cause an economic catastrophe, but multinationals are on alert.

The recent furore over Chinese telecommunications company Huawei competing to build 5G networks in the UK and Australasia has further fanned the flames, raising the prospect of retaliation and obstruction of free trade. A host of other political risks continue to haunt risk managers, including lone-wolf terrorism, recessionary political instability, Brexit and state-sponsored cyber attacks. Many of these issues have been on the horizon for several years, but are tough to mitigate.

According to advisory firm PwC, 2019 has marked

a “risk realignment” for global businesses. Policy uncertainty, trade conflicts and cyber threats have given CEOs cause for anxiety over the course of the year. US-China relations, rising nationalism and geopolitical tensions were cited as some of the biggest political risks facing companies right now. According to PwC, 88% of CEOs expressed concerns about the US-China trade conflict.

According to PwC in a recent risk report, global companies have adjusted their supply chain management during the trade war. “The ripple effects of the current China-US trade relations are by no means confined to China... Disruption is already playing out around the globe, as companies diversify their customer and supplier bases, accelerate procurement schedules, and turn inward in search of growth.”

“Nowhere are these trends more apparent than in China, where, according to the CEO survey, local businesses are shifting their focus to the domestic market, where the middle class is burgeoning, and to markets in Africa, the Middle East and Southeast Asia.”

## WE WILL ALL FEEL IT

Martin Baghdadi, a director at Control Risks, says the US-China trade war has impacted different countries in different ways, with a notable impact on Canada following its arrest of a Huawei executive. He believes the trade tensions mark an “ideological” shift in US politics. “Where Obama was frustrated with China, we now have Trump enforcing tariffs, from a government that is deeply suspicious of China and not just from a trade perspective.”

Baghdadi fears the trade wars will have a significant and detrimental impact on global economic growth. “The IMF has said if Washington and Beijing continue like this, it will push US GDP down by 0.6%, and China’s GDP by 1.5%. Those are scary statistics.”

Baghdadi says Asia-Pacific companies have begun to adapt to the new trade environment by channelling goods and services through Vietnam. “Some countries are benefiting as companies try to untangle economic links.”

He predicts some US allies with strong links to China, such as Australia, will be forced “to choose their alliances” as the trade wars intensify. He believes the trade wars will cause particular upheaval for Asia-Pacific businesses. “There is concern at board level. Companies want to know where they stand and where their business stands in China,” he says.

Risk consultant Eamonn Cunningham believes the US-China trade war will damage the global economy. “They say that if the US retail sector gets the flu, China gets a heavy flu. The miners in Australia will get pneumonia. There is a lot of brinkmanship going on. People are playing poker with some very big chips on the table.”



**“THEY SAY THAT IF THE US RETAIL SECTOR GETS THE FLU, CHINA GETS A HEAVY FLU. THE MINERS IN AUSTRALIA WILL GET PNEUMONIA. THERE IS A LOT OF BRINKMANSHIP GOING ON.”**

Risk consultant  
**Eamonn Cunningham**



Cunningham says the trade war has prompted risk managers to “think twice” about their strategic plans. “If you’re a rational business owner, you’re looking at this and saying: ‘The outcome here could be disastrous.’ The likelihood of a not so pleasant outcome might be quite low, but risk managers must multiply the impact by the likelihood. It’s a very large impact we are talking about. You can’t help but sit up and take notice.”

Cunningham says risk managers need to think about “the risk of uncertainty”. “It puts a dampener on the future, and that is certainly evident in the retail sector, with low consumer confidence,” he says. “It also impacts the industrial levels, and companies are putting brakes on capital expenditure.”

## POLARISING FEARS

Cunningham says risk managers should not view political risk in isolation. “You can’t just talk about the old-fashioned suite of political risk. If you look broadly, clearly terrorism has reared its ugly head and that has major ramifications. In the context of this, there is a resurgence of advocates promoting an ultra far-right philosophy and greater acceptance of populist parties, in Germany and Italy, for example.”

Baghdadi is also concerned about potential “lone-wolf” terrorist attacks across the globe, following the recent devastations in New Zealand and Sri Lanka. “I would not be surprised if there was an uptick in lone-wolf attacks following the disbanding of Isis fighters in Syria and Iraq,” he says.

Cunningham adds that polarising politics and the emergence of nationalist governments have made it a more challenging business environment. “There’s a greater acceptance of populist parties gaining momentum in Europe,” he notes. “The impact of all this isn’t always clear. It is difficult for large multinationals trying to plan and mitigate risk.”

Risk consultant Chris Corless thinks the rise of protectionism should be viewed as a key political risk. “Politically, the continued rise of protectionism and its impact on the various elections globally is a concern, because of its potential impact on global trade. The continued growth of separation between the haves and the have-nots and the broader ‘us versus them’ will continue to drive further populist agendas, and a further reduction in global growth.”

## BREXIT: NO END IN SIGHT

In Europe, Brexit remains the focal political risk. While risk managers expected the issue to be finalised this year, there is still no end in sight. Britain has extended its deadline to leave the EU to October 31, but the British government's exit plan has been rejected several times by cross-party politicians.

The British economy has slowed, forcing businesses across Europe to revise their plans. Risk managers fear further chaos in the months ahead, with the distinct possibility of a 'hard' Brexit, in which Britain would leave without a European trade deal.

Hans Læssøe, founder of Danish risk consultancy AKTUS, says Brexit is one of the leading political risks on the continent. "Both sides of the [UK parliament] focus on party politics with little or no inclination to find common ground, which they should have done years ago."

"I fear a hard/no deal Brexit will have a huge impact on business – plus the consequences of a significant decline in GDP over the coming years," says Læssøe.

**"I FEAR A HARD/  
NO DEAL BREXIT  
WILL HAVE A  
HUGE IMPACT  
ON BUSINESS  
– PLUS THE  
CONSEQUENCES  
OF A SIGNIFICANT  
DECLINE IN GDP  
OVER THE  
COMING YEARS."**

Founder, AKTUS  
Hans Læssøe

Cunningham believes political tensions also influence cyber risk, following a series of state-sponsored cyber attacks in recent years. "We're in a whole new ball game with politically motivated cyber hazards. I'd expect companies to be looking at this, and they will dismiss this concept at their peril."

## ECONOMY WOES

While political stalemates are unwelcome enough, concerning economic trends could also influence political risk in the coming year. Global central banks from the US to New Zealand have abandoned plans to raise interest rates amid weak economic growth and inflation. The risk of a global downturn has increased over the year.

Economic issues are known to impact political stability, and Baghdadi of Control Risks believes we could see greater political upheaval if the economy worsens. In 2017, when global GDP hit 3.8%, Control Risks raised its political risk rating on seven countries. So far in 2019, with global GDP set to fall to 3.3%, the firm has raised the risk rating of five countries already.

Cunningham says it would be difficult for central banks to support economies, and agrees with Baghdadi that slow growth could heighten political risks. "The capacity of central banks to use monetary policy is more limited. The risk of an economic downturn needs to be on the register of every risk manager. That needs to be connected to potential political fallout, particularly when a country is in the middle of an election."

# It starts with you

As Asia-Pacific countries focus in on individual accountability for unethical behaviour, it is critical for risk managers to embed a code of conduct that everyone must live by.

**I**n February, Australia's Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry published its damning indictment of corporate culture across the country. The report highlighted endemic greed and an absence of accountability at Australia's biggest corporations. The Commission prompted the Australian government to put a focus on the actions of individuals, a trend seen across the region.

The Reserve Bank of New Zealand is turning its focus on corporate misconduct and culture. In Singapore, financial regulators have drafted laws to identify the responsibilities of employees in material risk functions. In Hong Kong, the Manager-in-Charge regime is set to enforce greater individual accountability for corporate executives and organisations.

## **WE'VE ONLY JUST BEGUN...**

As scrutiny on conduct and culture increases, risk managers face more pressure to implement a strong



risk management culture in their organisations. Risk managers need to ensure the tone is set from the top and practised throughout their business. So how can risk managers ensure their company has a strong risk management culture? What obstacles stand in the way?

Thomson Reuters' 2018 Culture and Conduct Risk Report found that conduct risk continues to influence boardroom decisions. A total of 28% of respondents said they had turned down business opportunities due to culture and conduct concerns in the past year. Over 70% of companies expected regulators to increase their focus on conduct this year. The report concluded that most companies have just begun to tackle risk culture. "There is a sense that firms are now at the end of the beginning phase of coming to grips with culture and conduct risk, and that the concepts, approach and practices have entered the mainstream of business practices."

Advisory firm Aon Hewitt says a strong risk culture allows a business to operate within its risk appetite and maximise market opportunities.

Deloitte lays out seven key characteristics of a risk intelligent culture:

- A commonality of purpose, values and ethics
- Universal adoption
- A learning organisation
- Transparent communications
- An understanding of risk management value
- Individual and collective responsibility
- Expectation of a challenge

The firm says there is "no one-size-fits-all approach" to risk culture, and that companies should align their risk culture with their business model and risk tolerance.

### FROM THE TOP AND THE BOTTOM

According to senior risk consultants, executives at the top of an organisation, such as chief executives and senior management teams, should set the tone for risk culture. Ryan Tan, vice-president of M&A and corporate planning at Singaporean telecommunications company StarHub, believes there are three main components to setting a risk culture. The first, he says, is support from the top level. "You need a top-down approach, and you need management to buy into it," Tan says. "Because risk management doesn't have a direct association with the P&L of a company, it may be deprioritised, and that needs to be addressed."

The next step is a bottom-up approach, Tan says. "Risk managers need to engage different junior to mid-level risk associates – through risk training programmes or other practical applications. Not only to train them but to educate them about how risk makes a difference."

The third step is to gain an "external perspective", and identify areas of improvement by looking at rival businesses and organisations outside of their sector. "Risk managers should be thinking about best practices and benchmarking outside of their industry," Tan says.

He says the perception of risk as an independent function, rather than a profit driver, can make it difficult to embed risk culture. He believes companies need to emphasise that risk is integral to profits. He says mindset is the biggest obstacle to embedding risk culture, and companies must stress the value of risk. "You need to identify cases where risk management has made a difference to profits," he says.

Nor Adila Ismail, head of group risk management at Petronas, agrees that senior management should set the tone for risk culture. She says: "Both positive and negative behaviours, especially displayed by role models and senior management, to me will instil values on the importance of risk management."

### WE'RE NOT JUST POLICING

Like Tan, she believes risk has to be viewed as an integral profit driver. Ismail believes employees at all levels can play their part in creating a risk culture: "Encourage staff to express concerns and upholds processes to elevate concerns to appropriate levels. Emphasise this to the business, and change the perception of risk management as a policeman. We are not just concerned with the downside, but also seeing the upside."

Ismail believes practical steps can be taken to embed risk culture, such as working closely with human resources departments and ensuring clear internal communications on risk matters.

Victoria Tan, head of group risk & sustainability at Philippines conglomerate Ayala Corporation, has conducted research into risk appetite and awareness of employees. Ayala uses this data to identify weaknesses and make improvements to the corporate risk culture.

She says: "We first did a risk culture survey in 2015, involving managers and senior officers, the results of which were used to help us understand where we are. Last year, we did another survey across all positions within the organisation. The results will be used to develop strategies that will enhance the risk culture of the organisation."

Tan advises Asia-Pacific corporates to conduct company-wide analysis. "The best start is a survey. Use any framework that will suit the organisation's culture. At Ayala, we started with Aon's Risk Maturity Index, which includes questions related to risk culture. Then we moved to Deloitte's framework for a deep dive."

Tan says the onus is on chief risk officers to "establish risk-aware culture" and "strengthen it in the years to come". She adds: "So we always ask the question: 'What is the impact of our risk program to the risk-aware culture of the organisation?' We also encourage other functional units to include risk awareness in their activities, such as HR for employee health and safety."

Overall, Tan believes business functions need to work together to create and maintain a risk intelligent culture. She says: "Truly, ERM should be a collaboration platform and should let us break down silos. After all, risk's interconnectedness is real, and only a collaborative solution will manage it effectively."



# Simple ethical rules

The business that stays on top is the one that puts ethical conduct front and centre, and remembers these risk maxims, says Risk Cooperative's Dante Disparte.

**W**ith the growing number of firms falling prey to governance failures, cyber risk and market forces, there is a need for greater agility in how risks are confronted. Heeding lessons from the likes of Volkswagen's emissions scandal or the warning signs that could have prevented the Germanwings disaster, it is time for businesses to change the way they think about and respond to risk.

Complex systems fail in complex ways. Many failures are created by or missed within the Byzantine maze that is the modern enterprise. Addressing these organisational blind spots means equipping people with risk awareness, codes of conduct and value systems. These risk maxims reduce complex enterprise risk management principles into actionable guidelines:

## 1 VALUES MATTER MOST WHEN THEY ARE LEAST CONVENIENT

When confronted with challenging situations, value systems are there to guide behaviour and decision-making. After 9/11, the Geneva Convention took on an entirely new meaning in the US, just like Johnson & Johnson's Tylenol recall in the 1980s was informed by the firm's credo to put the people they serve first.

## 2 SUNLIGHT IS A GREAT DISINFECTANT

In the age of rampant cyber risk and unwanted disclosure, privacy is a luxury. The negative effects of the Sony Entertainment hack were amplified by inconsistent behaviour among top officials.

## 3 MAKE IT EVERYONE'S BUSINESS TO STAY IN BUSINESS

Firing the whistleblower breeds indifference. The notion of skin in the game helps create both a sense of loss aversion and preservation that is critical to firm survival.

## 4 THERE ARE NO CONSTRAINTS

Like in weather patterns and market forces, there are no constraints in risk management. It is safe to assume high degrees of variability over time and

therefore dynamic approaches should be applied to managing risk rather than passive ones.

## 5 TONE (AND DISTANCE) AT THE TOP MATTER

Attitudes towards risk are informed by tone, tenor and remoteness at the top. Leaders who practice what they preach, have conviction and lead by example are better at managing risks than those that merely pay lip service to risk, compliance and codes of conduct.

## 6 RISK LIES BETWEEN CHAIR AND KEYBOARD

In the era of man-made risk, internal and external threats emerge from human behaviour. Unlike naturally occurring risks, man-made risk has agency and therefore a greater degree of planning. Incentive systems and deep stakeholder engagement can help reduce the incidence and severity of these risks.

## 7 YOU CAN'T DECOUPLE THE FORTUNES OF COMPANIES FROM COUNTRIES

Firms are finding it increasingly difficult to shelter themselves behind their fortress balance sheets, protect their supply chains, people, systems and market access from global risks. At the same time, they have a unique duty to invest in slowing down the decline of the global business commons on which they depend.

## 8 BAD THINGS HAPPEN IN THE DARK

Moral hazards arise when people do not bear the downside of their behaviour. Combating these hazards begins with having transparency, accountability and clear guiding principles that hold economic, social and environmental impacts in balance.

## 9 SIMPLICITY IS KEY

Just as David was able to slay Goliath with a simple instrument – a slingshot – complex risks are best addressed with simple measures. Encouraging bounded risk taking and reducing fear of failure can help hone an organisation's broad senses – muscle memory – on how to respond to emerging threats and complex risk relationships.

## 10 EMBARK ON A ZERO-FAILURE MISSION

The airline industry boasts of one of the best-performing risk management records. The reason is that the consequences of failure are dire and all parties typically have skin in the game. This zero-failure approach should be adopted across all industries.

Firms should not embrace risk agility out of fear of failure or mere compliance. Risk agility is a source of lasting competitive advantage. When the competitive landscape is littered with the tombstones of firms that failed to respond assertively to risk, the agile enterprises will inherit the spoils.

**“MORAL HAZARDS  
ARISE WHEN  
PEOPLE TAKE RISKS  
BUT DO NOT BEAR  
THE DOWNSIDE  
OF THEIR RISKY  
BEHAVIOUR.”**

Founder and CEO,  
Risk Cooperative  
Dante Disparte

# Is your workplace toxic?

The #MeToo movement has begun to help bring interpersonal misconduct in the workplace to task. But latest survey findings suggest it's an even bigger problem than many anticipated.

**A**busive behaviour, sexual harassment and discrimination in the workplace have joined data privacy as critical issues of our time. #MeToo and #TimesUp have given names to the larger effort to shed light on the issue and to find a path towards more respectful workplaces.

Efforts to expose these issues have uncovered patterns of interpersonal misconduct in organisations around the world. Our newly heightened awareness of interpersonal misconduct and the toll it takes on individual employees and organisations is a positive development. But more needs to be known about the nature of the issue, the scope of the problem, the factors that exacerbate problems and strategies for fostering respectful workplaces.

As part of its Global Business Ethics Survey (GBES), the Ethics & Compliance Initiative gathered data to inform the conversations taking place in workplaces and to suggest a constructive path forward. The report asked:

- What does interpersonal misconduct (abusive behaviour, sexual harassment and/or discrimination) look like in the modern workplace?
- What is the frequency of these behaviours?
- How does interpersonal misconduct occur in the workplace?
- What are the greatest risk factors?

Data from the GBES revealed that 27% of employees have observed at least one of the three types of interpersonal misconduct (abusive behaviour, sexual harassment, and/or discrimination) in their workplace. Further,

5% of employees have observed all three types of misconduct in 2018.

Most problems happened on multiple occasions (62%) and were deemed “serious” or even “very serious” by observers (61%). Equally troubling, many of those seen to be perpetrating the misconduct were middle or senior managers. When it came to discrimination, employees indicated that more than half of the observed misconduct (56%) was committed by those in leadership.

Some industries seem to be particularly perilous for its workers: nearly two out of every five employees (39%) in the accommodation and food services industry have observed at least one type of interpersonal misconduct, compared to fewer than one in five (17%) employees in professional services saying they had witnessed an incident of misconduct.

## WHY PEOPLE STAY SILENT

According to the GBES, about one in three of those who observe interpersonal misconduct do not report it—leaving problems unsolved and putting employees and companies at greater risk. Raising reporting rates for interpersonal misconduct can be particularly difficult.

A report by the Equal Employment Opportunity Commission Select Task Force on the Study of Harassment in the Workplace describes how harassment claims that are made are frequently ignored and trivialized and how the victim often ends up being blamed for causing problems. While the #MeToo and #TimesUp movements have drawn attention to workplace harassment, it is still extremely difficult for victims to bring forward such claims.

Increased reporting of interpersonal misconduct will require focused efforts to provide support and reassurance to potential reporters that their allegations will be investigated without repercussions.

## WORK ABUSE: THE NUMBERS

**27%**

of employees have witnessed a form of interpersonal misconduct



**56%**

of observed misconduct was committed by leadership



**39%**

of accommodation and food industry workers have witnessed workplace abuse

Ethics & Compliance Initiative's Global Business Ethics Survey



RISK FOCUS > #ChangingRisk

# #ChangingRisk

LEADING THE

RISK REVOLUTION

As our #ChangingRisk campaign continues to gain momentum, we gather the latest opinions, impassioned views and harsh truths on where the industry must go from here.

## CONTENTS

---

Everyone is talking about  
#ChangingRisk p24

John Ludlow  
It takes two p26

Brigitte Bouquot  
The world is watching p27

François Malan  
Work on your soft skills p28

Gaëtan Lefevre  
Stop thinking like risk managers p29

Patrick Smith  
What's in a name? p30

# Everyone is talking about #ChangingRisk

We surveyed risk managers from across the world for their views on what really needs to change in our industry. They pulled no punches.

**I**n the industrial era, a company's business model didn't change much. The way in which businesses developed, delivered and captured value would remain static for decades. But in today's technologically advanced and globalised world, traditional business models are being disrupted and reinvented – at an exponential pace.

The velocity of change – and its breadth and sheer impact – is being felt in almost all countries, sectors and markets. Its impact extends to entire systems of production, supply chains, distribution and to areas of management and governance. And the risk landscape is changing like never before, posing new and complex risks for risk managers. To keep pace, remain relevant and add tangible value to business, risk management needs to change.

In our #ChangingRisk survey, we asked what you want to see changed. At the time of writing, more than 50 risk managers have taken part. Their views are a candid and passionate portrayal of the state of risk management and the challenges that need to be addressed to ensure a risk-mature future. There are some harsh truths – and not all that you'll agree with. And while we review these findings, let's do so with thought to the innovative work of many risk managers. This isn't about throwing out the old. It's about enhancing the strength of risk management.

In three events this year, we will place a microscope on some of the common themes that come out of our study to aid our #ChangingRisk manifesto, which we will launch at the end of this year.

So, while we continue collecting your views, we've summarised the interim data to give you a snapshot. The full report will be available at the Ferma Forum in Berlin, 17–20 November.



## WHAT ELEMENTS OF RISK MANAGEMENT ARE OUTDATED AND INEFFECTIVE?

### A FALSE SENSE OF RISK MANAGEMENT

"The preoccupation of catering to the board and audit and risk committees' expectations of risk management – i.e., production of governance documents – gives a false sense that risk management is effective. I don't mind if an organisation feels it must start the risk conversation with a flawed risk heat map and/or risk register, but it's a real problem if that's where risk management stops (which is often the case)."

### OVER-COMPLICATED ERM

"Many companies over-complicate ERM and focus a lot on capturing risk data in a non-consistent fashion and in cumbersome risk registers. The information is not used to drive risk-informed decisions."



## WHAT WOULD YOU CHANGE TO IMPROVE RISK MANAGEMENT?

### REDUCE TIME SPENT ON RISK FRAMEWORKS

“Yes, we need tools, but it is ridiculous when the development of frameworks, methodologies and heat maps consumes most of your role. Our role should be considered as risk/opportunity advisory services. We do not ‘manage’ risk, and nor are we solely focused on ‘risk’.

Aren't we also there to help from an opportunistic perspective, i.e., helping business protect what they have, and helping them make informed decisions to maximise growth? Yes, we need a profile to understand where an organisation is – profiling is the cornerstone – but we need to be strategic advisors and a conduit to pull the right stakeholders together to help make informed decisions.”

### CHANGE ROLE, RESPONSIBILITIES AND JOB TITLE

“I would start at a higher level and transform the name, role and responsibilities of the risk manager. This requires a disruptive ‘start again’ strategy.

With the ever-increasing focus on risk and strategic achievement at board and executive levels, I would start from that perspective and answer the following question: ‘What role and/or function is required to assist the company in developing strategies that are achievable, resilient and flexible; mindful of the opportunities that are available and internal and external risks to strategic success?’

Then, ‘How does this role/function align to the current or future organisational structure?’

Thereafter, the following can be considered:

- What are the skills, attributes and experience required to deliver the role and responsibility?
- What tools, structures and methodologies are required to be successful and to really add value to the organisation, exec and board; including the three topics above – tools, standards and risk model?”

### ONE SIZE DOES NOT FIT ALL

“The concept that one approach to risk management works for all organisations. Risk management needs to be bespoke to the business and consider the current stage in its business lifecycle, the strength of the company’s leadership and the maturity of governance by the board. Pedalling a one-size-fits-all approach is naive at best and damaging at worst.”

### CHANGING PERCEPTIONS

“Risk management is only considered a compliance requirement, with no bearing in strategy setting or decision making.”

## WHAT DO YOU THINK IS SLOWING CHANGE IN RISK MANAGEMENT?

### GETTING THE RISK STORY WRONG

“Auditors, insurance and consultants telling management different stories about what risk management is. All say they do it, all have different solutions and approaches and all have different underlying motives.”

### WHEN WE DON'T HELP TO MAKE DECISIONS THAT MATTER

“Those who are deemed ‘risk managers’ or equivalent not having the ability and skills to create real value by helping the business make decisions that matter. I believe that an enhanced skill set, above and beyond what has been necessary for some of the traditional risk work, will be required, but for this there is a considerable amount of content already available – decision science, psychology, risk analysis and modelling techniques.”

### OUR JOB TITLE

“The concept of ERM and titling most risk functions and individuals as ‘risk managers’ – particularly when we do not manage the risk as we do not own it.”

### THE INDUSTRY'S UNDERSTANDING, OR LACK THEREOF

“The first thing that is slowing down change is the insurance industry (brokers, insurers and reinsurers) not understanding that risk management is more than buying insurance. The second thing is when risk managers only concern themselves with downside risk instead of risk = uncertainty, and include upside (strategic) as well as downside (tactical).”



# It takes two

We need to create two distinct and defined roles in risk management to drive new solutions in a changing world, writes John Ludlow, chief executive for Airmic.



**F**our words – *New world. New solutions* – and the theme of this year's Airmic annual conference sums up, succinctly, the state of business, the state of risk management and, crucially, our role within it.

The new world is perpetuated by several trends. Most notably, the advancement of new technology, which underpins the depth and velocity of the business transformation that is so prolific today. Then the acceleration in globalisation connecting businesses from the Atlantic to the Pacific into a global ecosystem of trade, distribution and supply chains. There are also new economies in the on-demand, sharing and intangible markets, initiated by so-called unicorn start-ups, which are driving competition and change faster than we have ever witnessed before.

The last trend is new solutions. This encapsulates the risk community's ambition to pioneer new thinking in risk so that we can ensure the success and resiliency of our businesses in the face of this brave new world.

As business continues to shift and evolve, risk management will need to adapt and play a more significant role in helping the board of directors and C-suite develop a more risk-intelligent organisation. So, from a risk perspective, what does this need to look like?

## A FRAMEWORK

Risk management, by and large, operates on two or three main levels – operational, tactical and strategic. In other words, bottom-up (operational) and top down (strategic and tactical).

Operational is all about optimising the efficiency and effectiveness of an organisation. At the strategic level, risk management is about creating a defined model for identifying, assessing and managing risk and uncertainties. It is the 'what' – what is your business model? 'Why' – your purpose and value; 'when' – your priorities; 'where' – the internal and external contexts; and 'who' – the capabilities.

Tactical risk management drives the delivery of this strategy, this relates to change management –

anticipating the internal blockages and resistance to risk management and unblocking them.

It is about taking stakeholders on a journey and helping them recognise the true value of risk, as well as its business enablement potential, and its capability to support intelligent risk-taking.

It is about getting into the same mindsets of the board and using this to drive change.

And within these two pillars – strategic and tactical – is where we need to effect the biggest change so that we can drive risk management further up the risk maturity curve and respond to the risks of the new world.

Indeed, the concept and theoretical parts of risk management are in good shape – we are very good at working bottom up. We are the experts in compliance and operation risk. And we have a healthy community of professionals who drive strategic and tactical risk management.

But change is a question of elevating the number of professionals who can confidently lead – who can shape and enhance strategic and tactical risk management – an area that Airmic is working hard to support its members to do.

## TWO MINDS

So, my vision for #ChangingRisk is to create distinct roles of the risk management function – splitting out the strategic and tactical from the operational. These functions – equally as important as the other – are different mindsets and would not be combined into one meeting or one role in larger teams, as is the case in many organisations. They should, instead, be considered as two distinct jobs.

Take the finance profession as one example. In a large company we would not expect a financial accountant, who conducts general financial management, to also be the management accountant, forecasting the financial health of the company's future. These are two different disciplines – so, why should one risk manager always be expected to be able to conduct all three disciplines of risk management?

Combining these job roles confuses the risk conversation and the understanding of risk management among the c-suite and board. Strategic and tactical; and operational risk management are two different occasions to talk to the business. And when approaching the board, we must be clear on what perspective we are giving – the operational or the strategic and tactical?

These disciplines within business are simply referred to as 'risk management', and technically they are. But one is bottom-up and the other is top down. Yes, they are both risk management, but they must be orientated differently, so the value of each is clear.

Finally, we need to support risk managers to develop the competencies that they need to help their organisations become risk intelligent. We are well-versed in the theory. The next step is to build on the knowledge – strategic-influencing skills, change management and team building.

For me, #ChangingRisk is about developing capability and capacity within the risk management community so we can respond to the new world with new solutions.

# The world is watching

We are facing a paradigm shift, as society expects more from businesses, says Brigitte Bouquot, Amrae president and risk manager for Thales.



**T**he risk manager's role is fast-evolving to meet the changing needs of businesses. And this change is driven by two trends. The first is digital disruption. Globalisation coupled with greater interconnectivity are changing the way companies operate and so risk managers will need to assess the risks associated with these new models.

For example, many companies are moving away from being a sole-manufacturer to being service or platform providers. But when businesses make this transition, they suddenly develop global connections. This is creating a rupture in the way we manage risk.

Technology might be global, but regulations are not global. This means that there is an increase in the compliance burden on organisations. Keeping pace with the changing regulatory environment is critical. Large global companies must be fully compliant with the law, otherwise they put their top directors at risk.

This leads to the second trend: digital disruption and the added regulatory burdens. This adds a new layer of risks, which are closely linked to business strategy.

Risk management cannot be defensive anymore. You must be at the root of organisational strategy. At the same time, risk managers must still manage the traditional historic risks like fire, flood, storm and staff health. And they need to be closer to the C-suite.

Risk managers must ensure that when a company decides to go in a new direction, this is done after balancing risk and knowing what is at stake in terms of liability, supply chain and skills. To achieve this, risk managers need to be connected to board members. If a risk manager is too far below the board or if they are isolated, they cannot assess strategic risks until after decisions have been made – which is often too late.

## WE NEED INVESTMENT

This changes the risk manager role. Being connected means that risk managers don't necessarily need to be an expert in all risks, but they do need to be able to interface with senior management and build a relationship. The best way to achieve this is to increase the resources of the risk team. This means you can keep all the experts but introduce a

management position at a higher level whose job it is to communicate the risks to the board.

Before going to the board, it can be useful to create a governance committee where experts evaluate the risks that a business is facing. Then, when risk managers go to the C-suite, they can say: here are the top five risks, and we've worked out the priorities and actions required.

This kind of model is not always in place. We're seeing more progress, but creating this structure requires understanding from senior management of the real value of risk management. The C-suite needs to know that they must invest in risk management.

## SOCIETY EXPECTS

One thing that is driving better understanding of risks on boards is the societal expectation across the world that companies will do good. This has created a climate of corporate responsibility, which is giving risk management a new lease of life.

The education of board members has changed so much – now there are rating agencies and CSR and all

**Risk management cannot be defensive anymore. You must be at the root of organisational strategy.**

this dynamic is pushing for better risk management. But this can't be just communication about the importance of risk, it has to have real budget behind it. And as society expects that a company will not create risk, there are rewards for businesses with strong risk management even if the end product becomes a little more expensive.

It's important to understand the world globally and to match the expectations of the young people that own society. People expect companies to be fair and not only making money. This is something which helps risk management to be embedded in the whole of the company.



# Work on your soft skills

Want to make a real difference? Risk managers need to develop the way they communicate with their organisation and with the C-suite, says François Malan, chief risk officer at Nexity. But that can take courage.

**T**he risk management profession is changing because companies are facing a lot of new and complex threats – cyber, climate change and other business interruption risks.

No longer can risk managers assume the role of ‘expert on risk and insurance’. This is still very important, but they must also develop the right soft skills. And how easy this is to do will depend on the personality of the risk manager and their willingness to adapt and learn.

One of the most important of these skills is the ability to oversee and manage various departments, finding ways to break down silos and get teams working together.

## ONE TEAM, ONE VISION

There will often be several departments in one company who have some responsibility for dealing with these complex risks – from legal, compliance and health and safety to human resources. Risk managers need to act as co-ordinators, bringing together several functions so that they can obtain a truly holistic view of the company’s risk profile.

Risk managers need to get an overarching view of the risks, co-ordinate the various teams, not just for the purpose of effective risk management, but so they can present one clear picture to the top management. It’s vital that risk managers create a risk aware culture throughout the business.

And to successfully achieve this goes back to my first point of developing the right soft skills.

Risk managers need to get better at marketing and communicating risks. They must find ways to convince stakeholders that they’re not just the owners of risk but they exist to also improve risk management throughout the organisation.

Risk managers need to be courageous with this. They need to monitor and evaluate risks but also challenge stakeholders and top management.

Dealing with the C-suite is rapidly becoming one of the most critical components of a risk manager’s job, particularly given the high-profile of emerging risks.

So, risk managers need to be more strategic and to find ways to present granular risks in a way that’s



holistic, relevant and useful to the board. They need to build a dashboard or create something simple, clear and then market and promote it in the right way.

Good key risk indicators could help. But risk managers can’t just follow other companies. They must adapt existing indicators to match the risk profile of their organisation and use them to develop and report on their risk management strategy.

And these top-level discussions need to happen regularly. It is not enough to meet with the board once a year. Risks evolve rapidly and so risk managers should be updating senior executives at least quarterly to show the changing threats the business is facing.

## TWO TO TANGO

For their part, the C-suite also need to consider risks more seriously because they are liable when something goes wrong.

And we’re starting to see this happen. Risk management is increasingly seen and discussed at board level. Senior management want to know how the organisation is dealing with these risks. They don’t want to go into all the details, but they need to have the reassurance that risks are being well managed. They’re asking questions about cyber risk, business continuity, and we can’t forget the old risks – fire, flood and other traditional risks.

Senior managers are more aware of the importance of risk management and want to be kept informed, partly because they understand the business costs if things go wrong. Most of all, risk managers need to evolve to ensure they are ready for these questions and prepared to answer them in a way that makes sense at board level.

# Stop thinking like risk managers



Start thinking like the C-suite. Risk management can't just be about evaluating risks, but the strategic direction of a company, says Gaëtan Lefevre, group risk and insurance manager at Cockerill Maintenance & Ingénierie.

**T**he risk manager role needs to evolve to better support business. That means that risk management cannot just be about evaluating risks, it must also be about understanding the strategic direction of a company and – critically – adding value.

For this to happen, it is critical that risk managers report into high level management, the chief executive or CFO for example. They must communicate with those at the top of a business and have regular contact with decisions-makers.

## CREATE A ROLE FOR RISK MANAGERS

Ideally, with this contact comes the creation of a new senior level role, such as chief risk officer. Risk managers are not yet at the top of the maturity curve and the challenge is to develop a specific role in the company.

Creating such a position is not easy because there are internal challenges from other departments, but a CRO needs to have oversight of all the risks whether it is reputation or cyber risks.

Some industries are ahead of the curve on this, namely insurance or finance, where it's mandatory to have a CRO. But for other sectors, fundamentally, it's up to the company whether to employ or develop the CRO role. So, if an organisation doesn't understand the strategic importance of good



**If you can't show how your advice and support will create value in the company you are completely missing the challenge.**

risk management – they're unlikely to see the value of a C-suite risk role.

## CHANGE THE LANGUAGE

It is critical that risk managers start speaking the language of senior managers. They need to understand the business and in particular the company's strategic direction.

To rise up the maturity curve, risk managers need to develop new activities that clearly demonstrate how risk management can add value to an organisation. They need to make sure that they are giving the right support and the right advice to the right people.

This means a change in the way that risk is communicated. You can no longer just say: "We need to do this (or not) because it avoids a risk, and I'm the risk manager and this is my job."

## CREATE VALUE

You need to create your position even when you have the title and to convince your management that you add value. This is so important. If you can't show how your advice and support will create value in the company you are completely missing the challenge. You're not framing your advice in a context that your C-suite and board will understand.

This is a huge change for many risk managers, who will need to develop the right skills and confidence to communicate this way. They'll need to understand finances, corporate strategy and to balance risks holistically against opportunities.

In the future I'd like to see more risk managers reporting to the chief executive with access to the board. My dream is that all risk managers will play a central role in supporting the business. But to achieve this, risk managers need to stop thinking like risk managers and start thinking like the C-suite.

# What's in a name?

Juliet may have disagreed, but a lot can, in fact, be achieved from changing a name, writes Patrick Smith, director of Acumen Advisory, and principal of Airmic Academy.



**T**here is no doubt that the risk landscape is changing faster than ever before. As trade continues to shift and grow in complexity; and technological advances accelerates transformation in business – from tangible to intangible assets – the role of risk management is evolving. It is becoming more strategically important and if the risk management community is to continue adding value to business, it also needs to change and enhance its capabilities.

There are three things that need to change to ensure that the risk community continues to advance up the risk maturity curve and benefit the organisations it serves

First, risk must be placed in the centre of strategy creation and strategic decision-making. Risk managers must be at the forefront of and be the experts in collating and analysing data relating to any strategic constraints or accelerants in the management of risk and opportunity. They should be responsible for horizon scanning and drive forward both resilience and developments for the near and longer term.

## TRUSTED ADVISORS

The second change I would like to see, which is a derivative of the first, is for risk managers to be regarded as trusted advisors to senior-level management and exercise their full potential to inform and guide strategy and strategic decision-making. This will cement their place at the top table. For this to happen, risk managers may no longer be called 'risk managers'. In the

future, their job titles could take on a new name, the 'chief strategy officer' or 'business resilience officer', for example. The point is that change is needed.

Risk management has a very bright future, but we must disrupt and transform ourselves and drive risk to be positioned more strategically within an organisation. Given that the role, as I see it, should be central to the achievement of strategic objectives, rather than on responding to headwinds and incidents, we need a more 'transformative' job title.

The issue with 'risk' in the job title is that, rightly or

wrongly, the word can have negative connotations. 'Risk' can be regarded in some industries as a blocker to commercial or strategic progress. And herein lies one of the challenges that we must overcome – changing the perception that our stakeholders, C-suite and the board of directors have of risk management. Sadly, our value in aiding strategy isn't always recognised. Unfortunately, perception is often reality.

Risk management is often regarded as being overly technical and academic. Over the last 50 years, risk management has developed into a 'science' because the evaluation of risk and the governance around it can appear to be overly complicated and removed from core business objectives.

Equally, risk management frameworks can often provide output that is difficult to understand and, most importantly, hard to use in the practical sense. There is no questioning the significance of risk output, but it must be displayed in a way that provides practical answers – and answer the real question: "What should we do next?"

Of course, all of this can be changed – and collectively we can truly affect the future of risk management.

## REWRITE THE RULES

If I were to write the #ChangingRisk manifesto for the future, I would rewrite the risk management rules and transform both job titles and the specification of our roles. I would create a career that realises the vision of what we hope risk management to be: the strategist or futurist of the businesses that we represent.

Effective engagement with the recipients of risk management is critical to changing common and embedded perceptions. It would be a mistake to produce a manifesto that does not have the support and influence of the users of risk management – risk management stakeholders, executive managers and boards of directors. Creating a "top down" pressure for change is as important as "bottom up" transformation.

The final item I would place in the manifesto is, 'change the risk conversation'. We must stimulate discussions around new questions – so, rather than asking the usual questions around what risks might prevail, we should rather ask "given the risk landscape, what is the right strategy and how can we execute it?" As risk professionals, we will naturally assess, mitigate and prevent the risks to strategic success.

So how about it? Let's nudge at the future of risk management so we become the strategist and futurist, and critical to organisational sustainability and success.





# The value you cannot grasp

Intangible assets like intellectual property, brand and data are key value-drivers. Yet companies are in danger of allowing them to slip through their fingers. What protections can you put in place in case of loss?

**I**ntangible assets are the value-drivers we cannot touch or see. While most companies consider their property, manufacturing facilities or equipment as their prized possessions, intangible assets represent significant value. From intellectual property to computer code and branding, intangible assets are often the hidden foundation for profit and growth.

While the loss of intellectual property might not appear as obvious as conventional risks, intangible asset loss can be a danger for any company. Intangible assets are a growing risk for companies, yet many risk



**“WE’RE WORKING WITH RISK MANAGERS TO FIGURE OUT WHAT INTANGIBLE ASSETS EXIST, HOW LOSSES MIGHT COMPARE BETWEEN THE TYPES OF ASSETS AND WHAT IS INSURABLE.”**

Head of cyber and professional indemnity APAC, AIG  
Liam Pomfret

professionals believe the subject is overlooked.

AIG’s head of cyber and professional indemnity APAC, Liam Pomfret, says: “It’s become apparent that much of an organisation’s value is in its intangible assets. You only have to look at how the top five global companies by market cap have changed over the past 40 years to understand where value lies today. The difficulty is in identifying and categorising the types of intangible assets and the impacts they could have on a business if disrupted.”

**STILL OFF BALANCE SHEET**

“The most common risk is the failure to identify intangible assets at all,” says Paul Adams, CEO of EverEdge Global, a New Zealand-based intangible asset advisory firm. The company has worked with companies from Coca-Cola to Air New Zealand. “If you fail to identify these assets, you fail to identify the risk to those assets.”

Adams says intangible assets are typically “off balance sheet”, and of less importance to finance managers and risk teams. “You have these tremendously valuable assets that aren’t captured in P&L, aren’t on the risk register and generally do not make the risk register. Yet they represent so much of the value and earnings growth of that company.”

The biggest intangible risks vary from sector to sector, Adams says. “For companies like Google, it may be data. For SAP, it would be their software code. For drug companies, it would be their patent holdings and approvals. For industrial companies, it might be technical know-how.”

Adams believes that cyber risk, one of the most significant threats facing global companies, is a “subset” of intangible risk. He says cyber insurance products do not protect against the loss of intangible assets. “Most [cyber] insurance products do not deal with the issues. The average cyber policy is a business interruption policy, but it doesn’t compensate if someone steals data or information.”

**WHAT PRICE BRANDING?**

How can companies value their intangible assets and the associated risks? Adams says risk managers need to take a new approach using different methodologies. “The risk industry can be very creative. If they can come up with the damage a hurricane might cause, they can come up with the costs associated with not being able to use their software, or if someone rips off their brand.”

Adams says quantitative modelling – measuring the relationship between cost and value – is not an efficient way of valuing intangible assets. “Often, there is no correlation between their cost and value.”

He adds that the “income approach” – valuing an asset on how much income it earns – does not capture the value of intangibles, as intangibles often represented new ideas and innovation.

AIG’s Pomfret believes insurers can help risk managers understand what they need. “We’re working with risk managers to shift the mindset of an enterprise

from only managing and insuring tangible assets to figuring out what intangible assets exist, how losses might compare between the types of assets and what is insurable.”

“Historically, intangible asset value has been associated with patents, trademarks or brand equity. However, more recently cyber incidents have shown us the risks associated with loss of information or the reliance on access to data and networks.”

While solutions are needed, there are options, he adds. “The market will likely develop further as the knowledge economy evolves. It also depends on the category of intangible asset. For example, is there an integrity, confidentiality or accessibility issue? Then cyber may be a solution. Is there a dispute over ownership or the use of something, such as software? Then a legal defence policy may be required.”

**TURN UP THE HEAT**

Companies across the Asia-Pacific region have begun to elevate the importance of intangible asset risk. Victoria Tan, head of group risk management at Philippines conglomerate Ayala Corporation, says the company has made brand and reputation a “top five risk” on its register. “In Ayala, we regularly conduct an annual risk assessment while employing different methodology, so we always have a fresh and relevant view of risks,” Tan says. “In 2014, we did a Black Swans approach in our risk assessment, where we focused more on the value-drivers of the holding company. During that workshop, the group, composed of the senior management team, concluded that Ayala’s brand and reputation were its most critical value-drivers.”

Tan says intangible assets such as brand and reputation drove economic benefit through better access to capital markets, a lower cost of financing, better access to talent and greater business opportunities.

Yet most companies underestimate their intangible assets, according to Eamonn Cunningham, an Australia-based independent risk consultant. Cunningham says companies tend to take “an informal approach to their management”. He adds: “As a consequence, their approach to protection is undercooked.”

Cunningham calls on risk managers to assess their intangible risks and address potential legal issues. “Take a hard look at what’s driving value in your business. Assess the value; it is probably more than you think. Make sure you have legal ownership of intangible assets and the right documentation in place.”

Cunningham says companies should be mindful of the internal threats to intangible assets. “You would be well-served to address this issue in-house. If you have a disgruntled employee, for example, your IP might be compromised suddenly, causing a massive loss of value. Make sure the right people in your business have a clear appreciation of intangibles and recognise their importance to the company.”

# Take control of leaking assets

There are a number of ways your critical intangible assets could be flowing out of your business, says EverEdge Global's Paul Adams.

**I**n more than 750 client engagements across both private and public companies, we have seen intangible asset risk feature on only one board's risk register. Yet, the consequences of not identifying and understanding intangible assets and their associated risks are extremely serious.

So, what are the top five intangible asset risks that companies face today and are they preventable?

## #1 CONFIDENTIAL INFORMATION IS BEING LEAKED

**Companies are constantly leaking key intangible assets, with the primary sources of those leaks being customers, suppliers or employees.**

According to research by Code 42 in its Data Exposure Report, 72% of CEOs, 71% of CMOs and 49% of business leaders admit to taking intangible assets (including information, ideas, intellectual property and data) from previous employers with them when they move to a new organisation. The reason given for this was that 79% of the CEOs and 65% of the business leaders surveyed saw their work as belonging to them – even though the policies typically said otherwise. Ouch.

We see this scenario play out every day. Take, for example, a hardware company that asked us to help it review its policies after it was badly burnt by the loss of its confidential information. The company had developed a world-leading new product category but, being unable to keep up with demand, it outsourced software development to an external supplier. As part of this, the company provided the full details of code and key confidential information.

The initial project was delivered on time and within budget, but the supplier then shut down.

Fast-forward six months, and the supplier reappeared as a competitor, utilising the intangible assets it had developed to spring board ahead of its former client. The supplier was able to grab a majority market share at a direct cost to the hardware company of \$150 million.

Unfortunately for the hardware company, the bell couldn't be unrung. We could only work to help it prevent this situation happening again in the future.

## #2 YOU CANNOT PROVE WHAT YOU OWN

**Eight out of 10 companies cannot prove they actually own their intangible assets.**

Unlike tangible assets, intangible assets are hard to inventory, are often not registered and do not appear on balance sheets or within profit and loss accounts. When you throw in issues such as joint development arrangements, joint R&D and outsourced contracting arrangements, it can be very difficult to actually pin down and establish who owns what.

We saw this when dealing with a company that was raising \$35 million in venture capital. A standard warranty that investors will require a company to sign is that it owns all of its assets. In this case, when push came to shove, this software company realised that it could not actually prove it owned its software code.

The company had been founded by three founders who worked together for over a year without being paid, and without any kind of corporate entity. Then one of the founders left, creating a split in the code, which eventually led to uncertainty around who owned what.

Add to this that they used friends and outsourced contractors to contribute to the coding, merged with another company partway through and also used a large

amount of open source code – and the result was a Gordian Knot of software code where it was extremely difficult to actually prove who owned the assets. This caused a major problem for the investment, but the issue could have been prevented if the company had taken steps along the way to clarify the ownership of its code.

### #3 HAZARDOUS USE OF OPEN SOURCE CODE SOFTWARE

**Today, 80% of all software code is open source – that is, software that has been developed by one individual that is freely (or not so freely) available for use by other individuals.**

The problem with open source code breaks down into three issues:

- Understanding who actually owns the software
- The licence terms of open source code software can be poisonous to proprietary code developed by your company
- Open source code is a very effective way of getting malicious code such as hacks or trojans into a proprietary source code base

The primary solution to this problem is to first understand where and how you are using open source code software – and it is almost certain that you will be. We work with a major open source code firm out of the US that, in 10 years and 13,000 audits, has found open source code software being used in every instance.

Once you know whether or not you're utilising open source code software, the next step is to understand whether or not the licence terms present an issue with your proprietary software code and whether or not there are also security threats as a consequence of the use of that open source code software. Once you have these things sorted, you need to ensure that you can establish chain of title to the proprietary code you have developed for your own purposes.

### #4 YOU DON'T OWN YOUR BRAND

**Many companies we see either do not own or control their brand, or face major brand infringement risk.**

A brand is often a company's most valuable asset, yet many companies do not understand trademark law or trademark strategy. We often find that companies create new markets and new products, enter into new geographies, or establish new relationships, without ensuring that their trademarks cover the new arrangements.

Likewise, we find that many companies are not putting the right measures in place when they enter a joint venture or distributor arrangement, which can create a risk that the partner will end up owning or controlling the brand.

We were recently engaged by a company that was growing very fast and that had been spending around \$1.5 million per month building its brand. The company engaged us to review its trademarks and we quickly realised that its trademark protection was completely inadequate, including in the US – a key offshore market

– where its brand was in fact owned by a competitor. The company had spent the previous 24 months (and roughly \$36 million) building a brand it did not in fact own or control. This created a massive loss for the company that would have been entirely preventable.

### #5 THREATENED OR ACTUAL IP LITIGATION

**There has been a huge increase in IP litigation in the US and Europe over the last decade.**

But IP litigation is often entirely preventable if a company has taken the time to understand its risk exposure early on and taken proactive rather than reactive measures.

A recent example in Australia comes from Cochlear, which last year had AU\$377 million in intangible asset damages (including for wilful infringement) awarded against it for patent infringement in the US. Particularly concerning was the fact the damages award was 17 times more than the contingent liability Cochlear had set aside for the case based on an 'independent damages expert assessment'.

Companies need to be very careful to utilise expert advice when assessing potential liabilities – to be out by this magnitude is extremely concerning.

At the time the announcement was made, Cochlear shares fell 3.8% or AU\$380 million – about the same amount as the damages award – creating a double blow for the company and its shareholders.

While Cochlear is appealing the judgment, it may not receive a ruling on this for two years or more. In the interim, the company has had to lodge an AU\$464 million insurance bond with the court to secure the judgment amount and any interest and costs. This process is costly both financially and also from a management perspective, as it can be expected that a great deal of management team resources will be going into fighting this case.

This issue can be prevented effectively by running through patent and trademark checks prior to launching – and preferably before developing – any products or ideas. Once the level of risk exposure is understood, action can be taken to correct or modify the product or idea, thereby avoiding that level of risk exposure.

### A SERIOUS THREAT

Intangible assets are the most important assets that companies own today, which means that they are also the primary source of risk for most companies. But, while these risks are significant, they are also in many cases entirely manageable if the right steps are taken to mitigate the threats.

It is vital that boards and management teams take a leadership role in protecting and managing a company's innovation, the first steps being to identify:

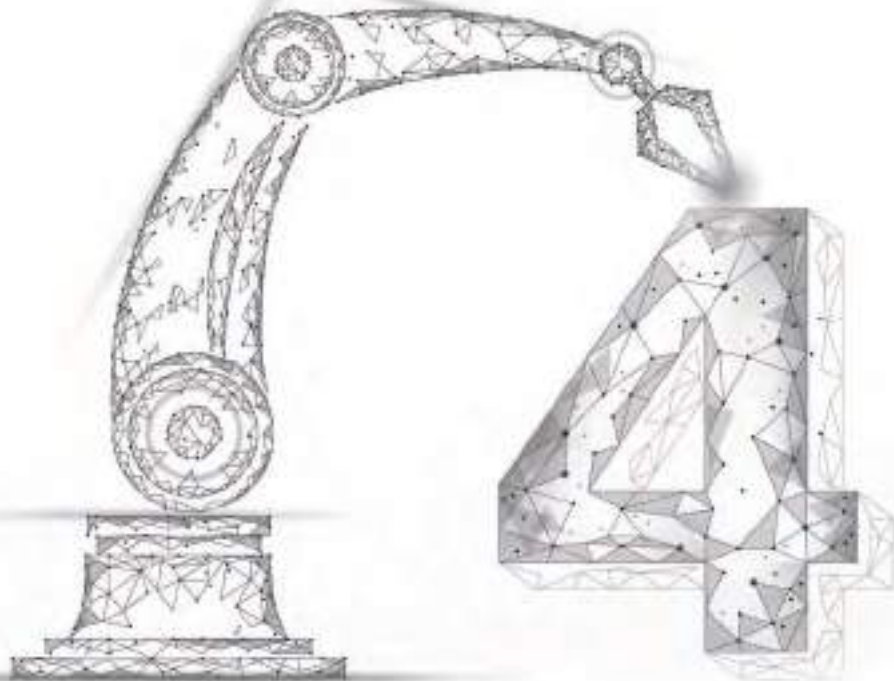
- What are our intangible assets?
- What are the impact of these assets on our business and how are they driving economic benefit?
- What risks are we exposed to through these assets?

By working through these questions, companies will be able to identify the major potential risks faced by their business and work to mitigate these issues before they have a significant negative impact.

**“COMPANIES ARE NOT PUTTING THE RIGHT MEASURES IN PLACE WHEN THEY ENTER A JOINT VENTURE, WHICH CAN CREATE A RISK THAT THE PARTNER WILL END UP OWNING OR CONTROLLING THE BRAND.”**

CEO, EverEdge Global  
Paul Adams

# What will Risk 4.0 look like?



How risk management should support Industry 4.0 is an ongoing debate for the risk community. Warren Black outlines how a modern organisation can prepare.

critical risk scenarios across their global operations. Right now, the speed the global risk management community is upskilling is much slower than the growth of cyber culture across Industry 4.0.

**R**isk management has always been about helping organisations to manage uncertainty, protect value and avoid disruption. So with this in mind, there are a few quick wins that modern organisations should plan for:

## #1 GO CYBER

Cyber represents how humankind interacts with and embraces such modern technological enablers as big data, predictive analytics, AI, the Internet of Things, digital systems, cloud-based applications, data streaming and altered reality. The Fourth Industrial Revolution is a cyber revolution and so the risk profession is going to have to embrace the threats and opportunities of a greatly enhanced cyber culture.

The ability to improve risk-related decision-making within highly complex and data-saturated environments is going to become a particular requirement of Risk 4.0. In turn, cyber (enabled) risk management has the potential to allow modern organisations to significantly improve their risk-related data gathering, storage, quality, analytics, visualisation, reporting and the like. For example, the growing number of hand-held, live data shaping platforms offer modern organisations the ability to evaluate their emerging risks in real time, based on live data sources, on an enterprise-wide scale. Equally, large-expansive organisations might consider adopting a Wikipedia-style approach to collaborating, verifying and continually updating their documented

## #2 USE COMPLEXITY SCIENCES

The ever-increasing complexity of Industry 4.0 can already be felt on a daily basis. The sheer volume of interdependent data, systems, technologies and shifting stakeholder relationships that need to be controlled in order to succeed is becoming insurmountable.

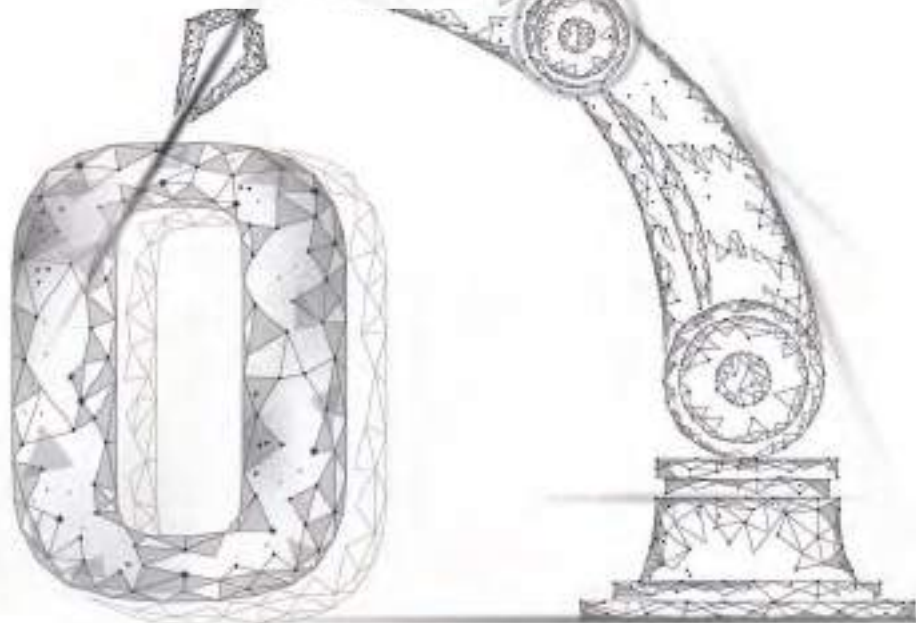
The invested risk management community must start looking at organisational risk management with a complex systems mindset. It is inevitable that modern organisations will need to better understand how disruptive phenomena (aka risks) emerge from within highly inter-connected and co-dependant working systems, relationships and interactions.

For this reason, it is almost certain that many of the future advancements required by Risk 4.0 lie within the complexity sciences. After all, no organisation can reasonably claim to be controlling the risks of increased complexity if they have none of the scientific understanding, skilled-up resources nor contextualised management tools required to do so.

The complexity sciences offer risk managers specific insights into how complex systems exist, interact and evolve, as well as how complex phenomena such as risks and disruption manifest, ebb and flow. This will be of particular relevance to Industry 4.0, as most participating organisations are going to be dependant on an advanced number of continually shifting and co-dependent relationships. Small changes in one relationship can easily ripple and compound throughout all the other co-dependant relationships to cause momentous outcomes further downstream.

Organisations will need to become intelligently responsive to those emerging industry forces.

**THE ABILITY TO IMPROVE RISK-RELATED DECISION-MAKING WITHIN HIGHLY COMPLEX AND DATA-SATURATED ENVIRONMENTS IS GOING TO BECOME A PARTICULAR REQUIREMENT OF RISK 4.0.**



### #3 BUILD IN RESILIENCE

Considering how Industry 4.0 is going to be an extended period of mass-scale changes, there is now more than ever a need for organisations to build in an internal resilience to disruption. Resilient organisations are those that can prepare, withstand and recover rapidly from such disruptive phenomena as market swings, consumer shifts, competitor advances, political shocks, accidents, disasters and even deliberate attacks.

Resilience during Industry 4.0 will have to become more than just securing business continuity and disaster recovery plans, it will also have to be about enabling an organisation-wide sensitivity, intelligence, awareness, agility and responsiveness to system-wide changes. More to the point, resilience will need to be about helping an organisation to become intelligently responsive to those emerging forces that have the potential to cause system-wide disruption. This is the truest definition of resilience and it will need to be one of the primary goals of Risk 4.0.

### #4 PROTECT INTANGIBLE ASSETS

In 2012, Instagram employed 13 full-time workers and owned only \$250,000 in physical assets, yet the company was bought by Facebook for \$1.3 billion. In 2009, bankrupt Telecoms manufacturer Nortel was surprised to see its operating patents auctioned off for \$4.5 billion – more than twice its liquidated debt.

These examples show that during Industry 4.0 there will have to be a significant paradigm shift in defining and protecting net business value, as the true value of many organisations is now in its intangible assets. Facebook, Google and Apple are all worth multiple billions of dollars, yet their balance sheets do not reflect physical

assets anywhere near such value. Their true market value lies in their operating data, innovation and the ability to create highly profitable, future revenue streams.

Risk 4.0 will need to include methods that protect not just the organisation's physical assets but also its intangible assets. Such intangibles may include: reputation, brand, operational data, client details, patents, licenses, prototypes, digital prints, audio files, graphics, videos, electronic signatures, service agreements and digital contracts.

The nature of many businesses will change during Industry 4.0 and so their value-drivers will shift from one asset class to another. Risk 4.0 will need to be hyper alert to this possibility and realign its focus accordingly. Organisations wishing to succeed during Industry 4.0 are going to have to place a particular emphasis on better understanding, evaluating and protecting their most current, value drivers and assets.

Although cyber, systems thinking, resilience and intangible assets are not particularly new nor unique to the risk management profession, it's their criticality and contextual relevance that will escalate during Industry 4.0. A greater focus, maturity and intensity will need to be afforded to each if risk management is to add value to future organisations.

We all know our working world is changing, and rapidly. Much of what we have traditionally accepted as business as usual will need to evolve in order to keep up with our changing world's most current needs. Risk management is no exception to this rule.

Undoubtedly, existing risk thinking, methods and tools are going to have to evolve to meet the needs of a working world that is significantly more dynamic, complex and disruptive than any other time before. For those organisations that wish to assess their risk readiness for Industry 4.0, they might start by assessing themselves against these four metric questions:

- Does our organisation's risk management capability fully embrace the advantages of the modern cyber culture? (Are our risk management efforts keeping up?)
- Does our organisation's risk management capability retain sufficient knowledge, capability and validity to control the risks associated with increased complexity? (Are our appointed risk officers trained in the science of complexity?)
- Does our existing risk management efforts enable an ingrained, organisation-wide culture of resilience (aka a systemic sense of resilience)?
- Are our organisation's risk management efforts protecting our most current value drivers? (Do we know where our most current value and risks lie?)

These questions are by no means an absolute indicator of whether or not an organisation's invested risk management capability is ready to meet the needs of Industry 4.0, but they are a start. And those organisations that cannot confidently answer 'yes' to all four of these questions are potentially ripe to being disrupted by the emerging forces of the Fourth Industrial Revolution.

**Risk expert Warren Black is a principal of [complexus.com.au](http://complexus.com.au). Find the full version of this article at [strategicrisk-asiapacific.com](http://strategicrisk-asiapacific.com).**

**MUCH OF WHAT WE HAVE TRADITIONALLY ACCEPTED AS BUSINESS AS USUAL WILL NEED TO EVOLVE TO KEEP UP WITH OUR CHANGING WORLD'S MOST CURRENT NEEDS. RISK MANAGEMENT IS NO EXCEPTION TO THIS RULE.**

# 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](https://zurich.com/my-zurich)**



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



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](http://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](http://www.aig.com).