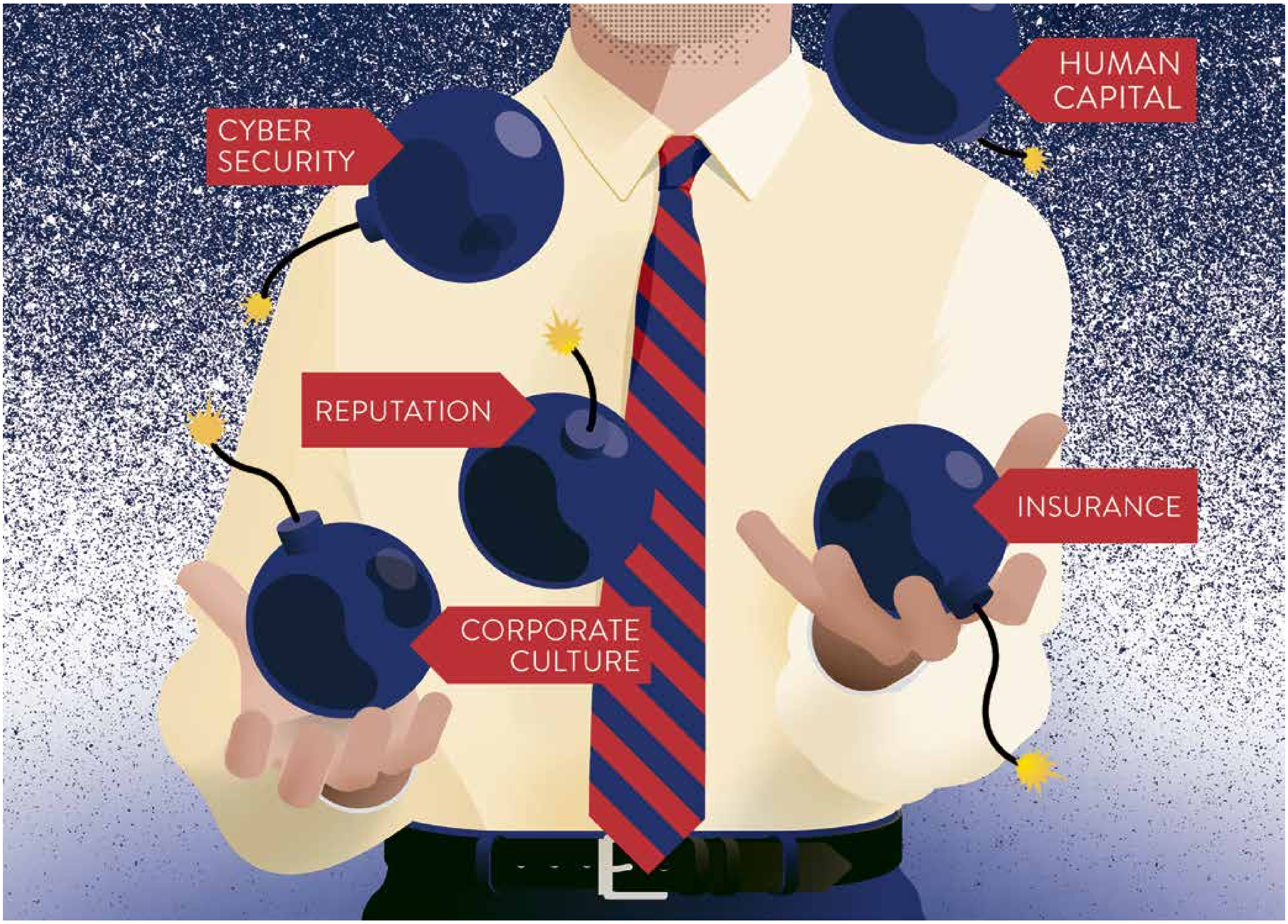
INDEPENDENT PUBLICATION BY

RACONTEUR

raconteur.net | #0380 | 31 / 05 / 2016

FUTURE OF BUSINESS RISK



FUTURE OF BUSINESS RISK

DISTRIBUTED IN
THE TIMES

DISTRIBUTION PARTNER
airmic

RACONTEUR

PUBLISHING MANAGER
Matthew Jones

HEAD OF PRODUCTION
Natalia Rosek

PRODUCTION EDITOR
Benjamin Chiou

DIGITAL CONTENT MANAGER
Sarah Allidina

MANAGING EDITOR
Peter Archer

DESIGN
Samuele Motta
Grant Chapman
Kellie Jerrard

CONTRIBUTORS

DAVID BENADY
Specialist writer on marketing, advertising and media, he contributes to national newspapers and business publications.

PETER CRUSH
Freelance business journalist, specialising in human resources and management issues, he was deputy editor of *HR* magazine.

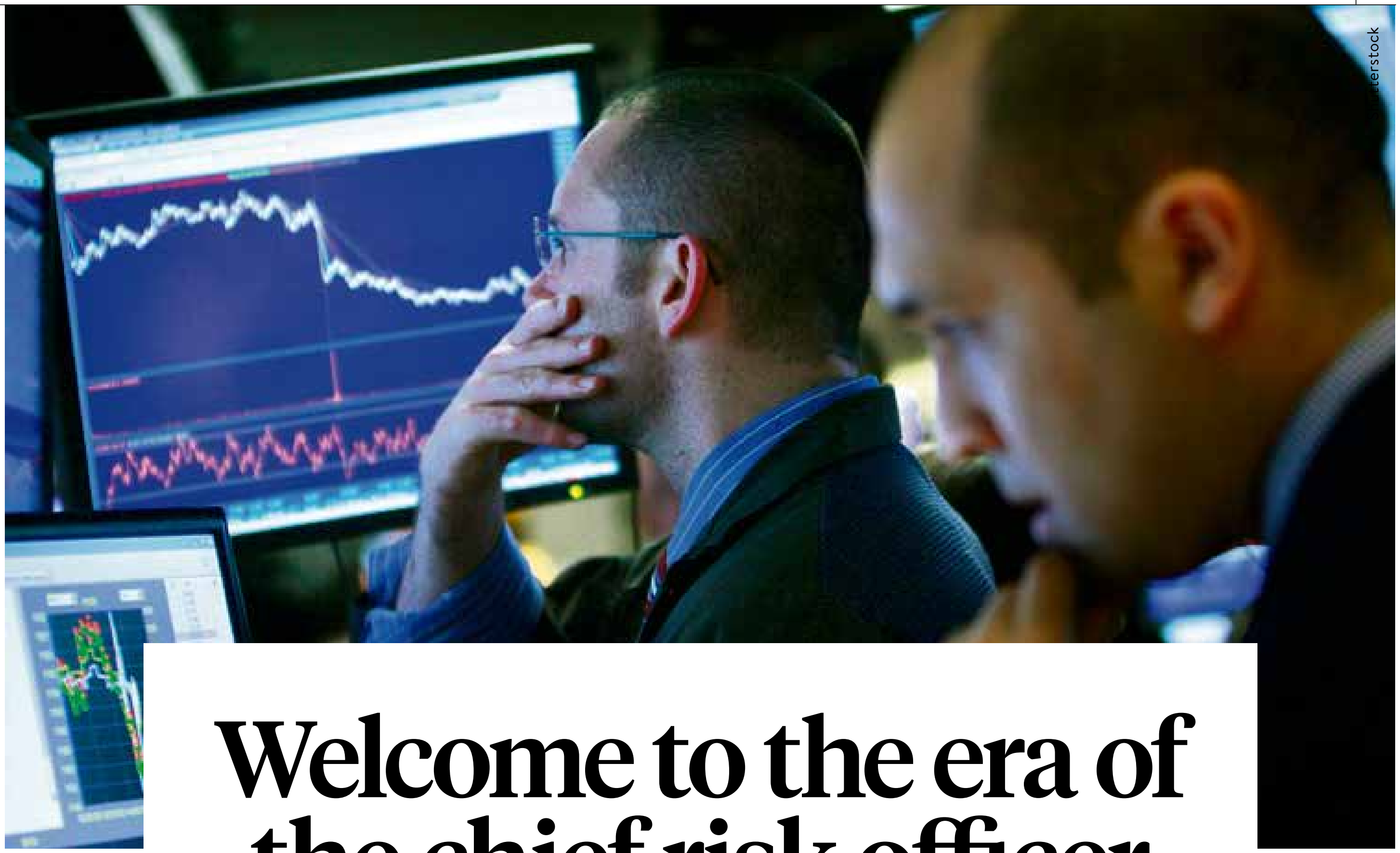
ANTHONY HILTON
Author, journalist and broadcaster, he is a former City editor of *The Times* and managing director of *The Evening Standard*.

DAN MATTHEWS
Journalist and author of *The New Rules of Business*, he writes for newspapers, magazines and websites on a range of issues.

CHARLES ORTON-JONES
Award-winning journalist, he was editor-at-large of *LondonlovesBusiness.com* and editor of *EuroBusiness*.

DAVEY WINDER
Award-winning journalist and author, he specialises in information security, contributing to *Infosecurity* magazine.

HELEN YATES
Freelance journalist, she was formerly editor of *Global Reinsurance* and managing editor of *Strategic Risk*.



terstock

Traders on the floor of the New York Stock Exchange in March 2009

Welcome to the era of the chief risk officer

The nature of risk has changed, beckoning the creation of a strategic role to manage business risks in the fast-moving 21st century

OVERVIEW
ANTHONY HILTON

Dr Johnson is said to have observed that nothing concentrates a man's mind so much as the prospect of being hanged in the morning. It is a brutal observation, but it encapsulates a basic truth. When things are going well, people do not feel inclined to change; only when disaster is upon them do they recognise how much of what is essential has been ignored and that survival involves rethink, reform and a new way of doing things.

It is no surprise then that the 2008 financial crisis, which was the biggest economic shock in almost 100 years, has brought in its wake a complete reappraisal across business about the nature of risk and how it might be better managed. It has been a catalyst for change well beyond the Square Mile. While banks were the most obvious sufferers from the crash, there was not a board in the land which was not shaken by it and disturbed by its consequences.

What is now much better understood is that the nature of risk has changed. It had long been thought, and taught in business schools, that the best way to control a business was to control the finances. This led to the development of risk control mechanisms which were numbers based. Performance against budget and performance against sales and production targets were closely monitored.

Variances from the norm – be that what was wanted in the budget or what had been achieved in previous years – was a signal that something was not working as it should.

But we now understand much better that numbers and performance-based systems do not go far enough.

First, such measures are silo based and take no account of how problems might impact horizontally across a business.

Second, they fail to appreciate how the nature of risk has changed with globalisation so that the challenge today is far less about managing hard assets and much more about intangibles such as reputation, supply chain issues, corporate culture, employee behaviour and now cyber attacks.

Third, the hierarchical numbers-based system assumed bad news would be passed upwards to a level where it would be dealt with, but the extent to which this genuinely happens is driven by the status of the risk professionals and the corporate culture, both of which are sometimes found wanting.

It is a fact, however regrettable, that in a world where everyone craves success, no one wants to be tainted by failure and there is still a tendency to shoot the bad news messenger.

Finally, no such system can alert a board to the risk inherent in the behaviour of the senior executive team and the board itself. If competence and commitment in the executive suite are the keys to success, character flaws at that same level and a refusal to confront uncomfortable behaviour are often the root cause of failure.

38%
of global companies rated business interruption and supply chain disruption as the biggest risks for firms in 2016

Source: Allianz 2016

The problems at BP, at Volkswagen, at Tesco tell us not only that no one is immune or exempt, but that in an age of social media, the damage done to a business through loss of reputation can far outweigh traditional losses from fire, flood and pestilence.

Structural problems require structural solutions. Hence the idea of the chief risk officer or CRO as someone who can cut across the silos and avoid being compromised by existing reporting chains and local loyalties. He must have the strategic nous to understand what needs to be brought to the attention of the board and crucially has the personality, panache and political support to do so.

Unfortunately, people with all those attributes and with the ability and experience to command the respect of the others round the boardroom table often think they should be chief executive themselves, and this does not make for an easy working relationship at the upper levels.

It sounds a good idea to give the CRO board status, but may be impractical because the more ambitious the appointment, the less likely it is that those who are sufficiently qualified would find it attractive. This is because support functions are rarely seen as a direct route to the top.

The alternative is to have a CRO who reports to a risk committee, which like other board spin-offs is staffed mainly by non-executives. But because the requirements for the CRO go well beyond the skillset of the traditional risk professional, it is perhaps a function which would form part of the management development of the brightest young talent.

In large organisations, the best aspiring managers are already rotated round the different divisions, geographies and functions of the business. Two or three years as CRO could be seen as a vital stepping stone in such career development.

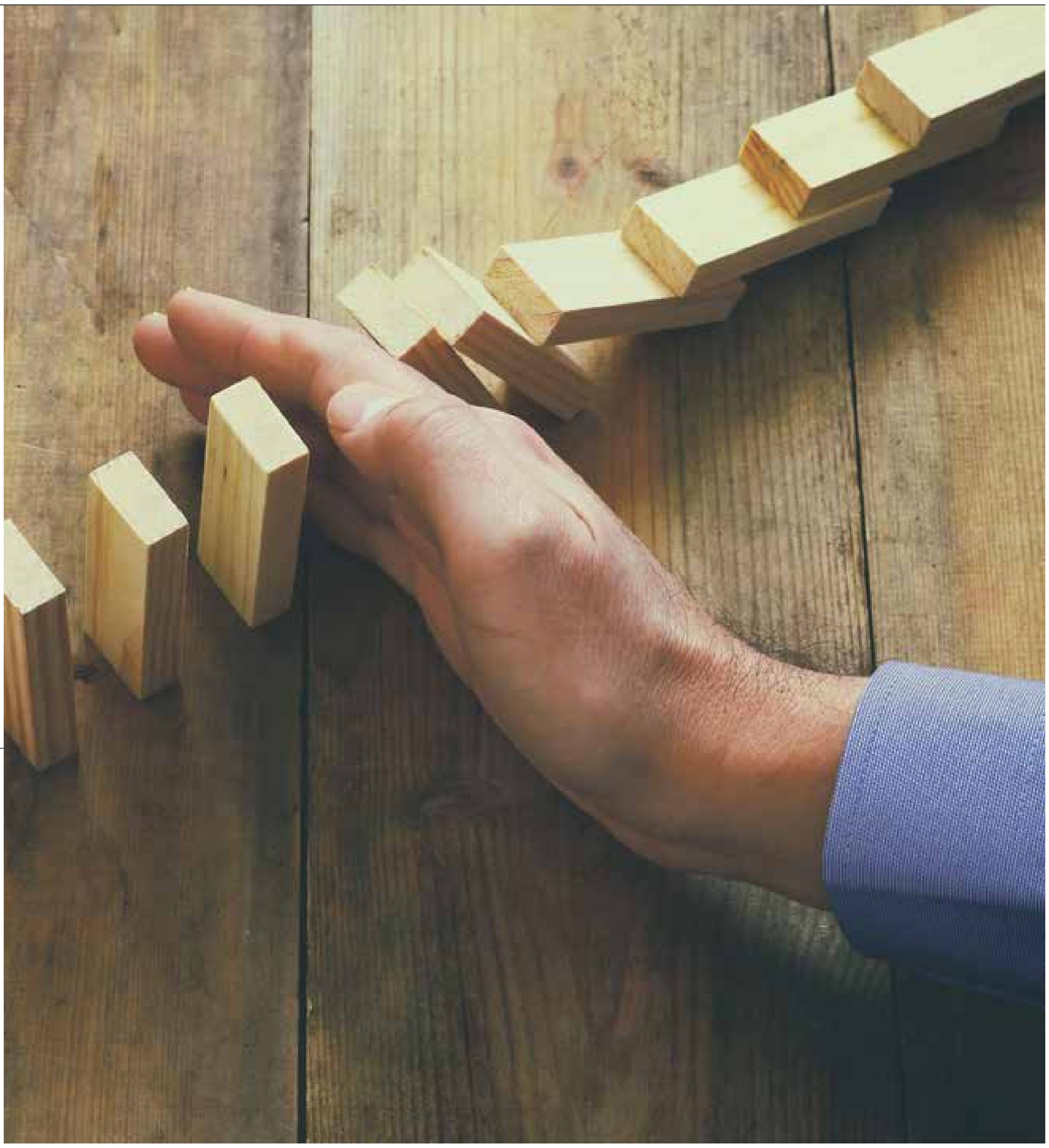
In truth, however, there is no right answer. Companies have to decide what works best for them. The point is that the essential first step in solving any problem is in recognising it exists. Companies may not yet know what works best for them, but there are very few who don't appreciate the need.

Share this article online via **Raconteur.net**

COMMERCIAL FEATURE

ACHIEVING RESILIENCE BY HARNESSING PEOPLE POWER

Companies that adapt to new risk cultures will be more resilient and successful, says ***Neil Cantle****, principal and consulting actuary at Milliman*



Milliman

Risk management is evolving. It is increasingly accepted that the old notions of control are incomplete. More and more, companies are being told they must actively manage their cultures, specifically their risk cultures. The prize is a more resilient, higher performance organisation.

What is culture? For many, it represents some sense of "the way we do things around here". A crucial factor often missed is that it is not just about how one or two people act; it is the emergent property arising from how everyone acts. We cannot directly act on culture or choose to have a good one, but have to influence our values and behaviours so that the resulting culture we observe is what we wanted.

> "We have to retain flexibility and learning as core skills, with the certain knowledge that things around us will not always go to plan

Does culture matter? Traditional management thinking encourages us to view our companies as machines, mechanical devices that can be monitored and brought back into line if they deviate from expected behaviour. In such a company, culture arguably plays a "nice to have" role because everything can be controlled anyway.

But companies are not like those simple machines. They are complex ecosystems where people go about their daily tasks, interacting with countless others inside and outside the company. In the real world, people are faced with situations every day that don't quite match the process manual, and they will use their initiative and try to find a way through to a successful outcome. Their judgments will reflect their values, so the question is whether those values are consistent with the culture your board wants to see?

For each activity that the company carries out, a number of participants will be involved. The nature of each person's contribution will be different and it is often necessary for different behaviours and attitudes to apply in order for a successful outcome to be delivered.

For example, we would expect our marketing and design people to be much more unbounded and free-thinking than the person with whom we are entrusting quality control or safety, where an eye for process and detail is clearly an advantage. We also expect some activities to require strict adherence to the rules, whereas others inherently require more creative and reactive attitudes. So companies don't have one culture; they are home to a number of interacting subcultures.

As our people interact they move the company forward a step at a time. The sequence of steps involves many players in different areas within the business and outside it. Each step puts the company on an emerging path, one that leads to particular sets of possible outcomes, while making it impossible to reach others.

In a world such as this, the notion of control, therefore, requires modification. We can no longer deliver the outcome we want with certainty, but can only choose our next action. Of course, we would like to select an action that will help take the company towards a successful outcome, but we simply don't know for sure which one that is. We have to retain flexibility and learning as core skills, with the certain knowledge that things around us will not always go to plan.

In fact, in situations of complexity, where the environment is dynamic and changing, a model of centralised control is far from optimal and often leads to unintended outcomes. The more appropriate approach to guiding progress here turns out to be empowering local experts to make localised decisions, with the proviso that they are aware of what is happening in the wider overall context.

Organising in this way, we need to empower our experts to make local decisions in the best interests of the whole, and are much more concerned about whether their attitudes and behaviours are consistent with what we would like. We are trusting them "to do the right thing" rather than directly controlling what they do. There will be some things we are so keen to avoid that we will implement very strict controls, making it hard to do the wrong thing, but we are largely going to be using our values to guide behaviours.

> "Culture is a much more important feature of our business than previously thought – an integral part of our control framework

There is a further dimension to consider. We need to recognise there is more than one valid perspective to be heard when deciding a course of action. Michael Thompson's work on the cultural theory of risk, for example, shows that four such views are always present.

In conducting our work we want to ensure each of these views is considered and debated, the surprising outcome being that this does not result in a compromise, suboptimal for all, but rather a solution which actually works better for all parties. Creating a culture where this type of debate is acceptable is, therefore, an important, and often overlooked, part of the governance framework.

So culture is actually a much more important feature of our business than previously thought, not just a "nice to have" after all, but an integral part of our control framework. When the board sets the risk appetite, it is establishing the tone for how business should be done. It must be clear what the objectives are and how they feel about the uncertainties associated with their delivery.

By describing the types of risks that are to be actively sought, in return for a reward, those that are to be accepted and those that are to be avoided, the board is providing a set of guiding principles staff can use when making daily decisions about which actions to take.

Neil Cantle
Principal and consulting actuary, Milliman

Given the complexity of modern business, companies must acknowledge they cannot be controlled using traditional command structures that focus on inputs. Decentralised control is the new paradigm because it allows experts to make local decisions based on a view of the big picture. Today's control frameworks are made up of sets of subcultures, and companies that adapt to this reality will be more resilient and successful.

For more information please visit uk.milliman.com

Be ready when disaster strikes

Robust risk assessment and a well-rehearsed crisis management strategy are essential in today's social-media world to protect valuable brand reputation if disaster strikes

BRAND REPUTATION

DAVID BENADY

From Volkswagen to TalkTalk, companies are learning that a brand's reputation is hard won, but easily lost.

The damage to a brand's public esteem from a scandal, disaster or accident can be devastating and long lasting. Some businesses never fully recover, as in the case of consultancy Arthur Andersen which saw its reputation hit by association with the fraudulent operations of Enron back in 2001.

In today's environment, with the explosion of social media platforms, chat boards and online review sites, reputation has become far more fragile and can be tarnished even more rapidly than in the past. A corporate disaster can be widely discussed on Twitter before the company's chief executive has even found out about it.

> The most catastrophic failures would have been survivable had there been better risk management

The insurance industry is waking up to the possibilities of covering companies for the loss of brand reputation in the event of such disasters. While historically, companies tended to derive most of their value from physical assets, such as buildings and machinery, today intangible assets, most notably brand reputation, make up the lion's share of value for many of the world's biggest businesses.

Insurer Tokio Marine Kiln offers policies that compensate companies for negative reputational events that can affect brand sales. That could include a product recall, a cyber breach or a case where a celebrity sponsored by the brand becomes discredited.

Innovation director Thomas Hoad gives the example of plain T-shirts which would normally sell for, say, €5. The moment you put the picture of a celebrity on them, they might sell for €25. But if the celebrity became involved in a scandal, the company might lose all or a substantial part of their expected sales of the T-shirts.

The Tokio Marine Kiln policy would cover the losses associated with that scandal, up to a maximum of $25 million per policy. Mr Hoad says reputational insurance has sold well since his company introduced it five years ago, though he believes many companies are reluctant to reveal they have this coverage.

"Alerting the public to the fact they have got it in a time of crisis is not a good idea," he says. "It is very sensitive." This could be especially true in the event of an accident in which people are seriously injured or killed.

While some brand-tarnishing events may be unpredictable and unavoidable, companies need to get better at risk management, says John Hurrell, chief executive of risk managers body Airmic.

The organisation has published in-depth research into reputational damage with its report *Roads to Ruin* outlining 18 of the most striking recent examples of companies brought low by reputational damage. "We found that in almost every case, the most catastrophic failures would have been survivable had there been better risk management," says Mr Hurrell.

Company boards may be made aware of the risks facing their businesses by risk-mapping, which are graphic illustrations of foreseeable events and their likely impact. But these risk maps are limited by the ability of risk managers to imagine scenarios, so may miss both the unexpected events and the most obvious failures which often bring companies down.

Getty Images

01
Toyota president Akio Toyoda faced intense media attention following a product recall in 2010 to fix faulty braking systems on four vehicle models

Getty Images

02
BP suffered severe reputational damage lasting for years following a disastrous 2010 oil spill in the Gulf of Mexico

REPUTATIONAL RISK IMPACTS

LOW	MODERATE	HIGH	VERY HIGH
• Local complaint recognition	• Local media coverage	• National media coverage	• International media coverage
• Minimal change in stakeholder confidence	• Moderate change in stakeholder confidence	• Significant change in stakeholder confidence	• Dramatic change in stakeholder confidence
• Impact lasting less than one month	• Impact lasting between one and three months	• Impact lasting more than three months	• Impact lasting more than 12 months/irrecoverable
		• Attracts regulators' attention/comment	• Public censure by regulators

Source: *Managing Risks to Reputation – From Theory to Practice*, Louisot/Rayner

Mr Hurrell says: "We are recommending that companies take a stakeholder-focused look at reputation risk, considering critical stakeholders, such as regulators, consumers and employees. They need to look at what underpins their reputation stakeholder by stakeholder. It might be different in the eyes of the customers and in the eyes of regulators. By taking a stakeholder-focused approach, it forces you to ask questions you don't ask in the conventional risk-mapping process."

Companies need a sophisticated crisis management strategy in place, for instance, knowing in advance which executive in the company will be able to comment to the media and ensuring the situation is quickly contained by suspending relevant activities. Some companies have practice run-throughs of their crisis management strategies to make sure they will be ready to act if the worst happens.

But Mr Hurrell believes many companies are failing to take the right steps to protect their brand reputations. "They are making very comforting noises about how important it is. Our members say their boards are putting it on the agenda, but you pick up a newspaper and organisations are failing," he says.

Reputational damage can be from self-inflicted wounds, such as Volkswagen's fuel emissions scandal, which has dented profits at the world's second-largest car maker and wiped $10 billion off its brand value, according to brand valuation company Brand Finance.

Or the damage may stem from the acts of a malign player. TalkTalk estimated it lost more than 100,000 customers after a serious data breach led to the credit card details of thousands of customers being stolen.

Alternatively, it may be a product recall, as happened to Toyota, or a terrible accident as in the case of BP's Gulf of Mexico oil spill. Many business people will be thinking, "There, but for the grace of God, go I", and wondering how they can diminish the likelihood of such disasters occurring and manage them if they do.

> You need to grow a capability in the company that understands and predicts the risks

For many businesses, the task of managing reputation falls to the public relations and marketing departments. However, a crisis that damages a brand will probably emanate from a different part of the business, usually operations, data-handling or from somewhere in the supply chain. So brand reputation needs to managed in a far more proactive fashion.

As John Ludlow, senior adviser at Alvarez & Marsal, says: "You have lots of people in communications listening to what newspapers and Twitter are saying and responding to it. That's not the best way to react over time. You shouldn't just be relying on the comms department to bat away nasty stories, you need to grow a capability in the company that understands and predicts the risks."

He says reputation needs to be understood in a much broader sense, as something that affects the entire company, so every department needs to learn how to manage risk and minimise reputational damage.

As digital communications increases corporate transparency and allows the public an ever-greater ability to influence brand reputation, businesses need to take heed. Brand reputation is one of the most valuable assets many companies have, so they need to make sure it is well protected.

Be certain to insure against the right risks

Insurance can be a minefield through which businesses tiptoe unaided at their peril, but help is at hand

Shutterstock

INSURANCE
CHARLES ORTON-JONES

Most companies are clueless about insurance. They cover the wrong things. They pay too much or scrimp and end up with inadequate cover. And usually they are oblivious to these failings until things go wrong.

In fact, most business owners barely think about insurance more than one day a year. They renew. And forget.

Fortunately this is the perfect time to remedy this. The Insurance Act 2015 comes into force this August, bringing in a whole new culture of coverage. Every company will need to review its policies.

But how can companies get the best deals? Alex Balcombe, director of Harris Balcombe, is bursting with tips. His family have been loss adjusters for 145 years. He rattles off umpteen errors companies often make, starting with definitions.

"Check what the words mean in the policy," he urges. "What insurance companies call gross profit is different to what an accountant calls gross profit. Everyone assumes they are the same, but it's not so. As a consequence people are woefully underinsured."

A report by the Financial Conduct Authority last year confirmed exactly this. The FCA found a significant number of small and medium-sized enterprises lacked the correct coverage when making a claim, meaning they were out of pocket following a traumatic event.

To get the right policy, you need to negotiate. Here's another stumbling point for many companies, says Mr Balcombe. "One of the biggest problems in insurance is online insurance. Don't buy it online. People assume buying business insurance is like car insurance. It is not. You need to talk to a broker and get the proper advice. Otherwise you will never understand the wording and conditions, and how it affects claims and settlement," he says.

Even the insurer you go with is a crucial decision. They are not all alike. Mr Balcombe advises: "You get what you pay for. If you go with an insurer like Hiscox, you'll get a common-sense approach. Their name is their brand and so they would not repudiate a claim on a non-causative breach. But if you go to the Lloyds market and take out a policy with a fringe Lloyds syndicate offering a cheap-as-chips policy, they will look for every possible way out."

Naturally, businesses need to insure the rights things. But what are they? There's a long list of potential things, from key person and indemnity, to supply chain and brand reputation. How can companies know what to do?

John Hurrell is the man to ask. He's the chief executive of Airmic, an association of risk managers in the UK. Mr Hurrell has a guide for the clueless. "You need to look at your business and identify all the things which, if something happened, would severely threaten you," he says.

"This might include professional indemnity cover. If you are liable, and not covered, your business might not survive. Make a list of these and focus on them. Pay more, if necessary. This process will identify the less important things, too. Either stop buying insurance for these lesser issues or manage the risk better."

When that task is complete, then scrutinise the policies. Mr Hurrell continues: "Look at your critical policies and have them reviewed by coverage lawyers. Look at the wording of the incidents you are most worried about. Also, do scenario planning. What would happen if things went wrong? You should look at the financial strength of your provider and their track record of paying out without undue hassle."

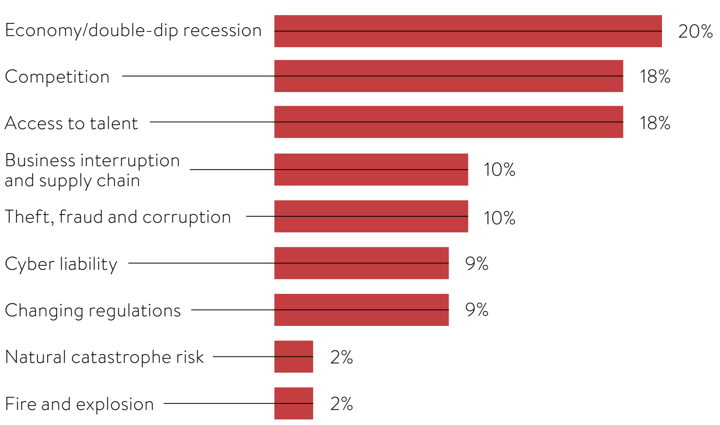
One vital step is to talk to the insurer about modifying policies. Five years ago insurers were rigid. They struggled to offer anything not on the menu. Today that has changed.

"Here's an example," says Mr Hurrell. "A hotel may take out coverage to insure against a terrorist attack. But what if there is a shooting incident in the area, however it doesn't affect the hotel directly? The policy probably wouldn't pay out. The hotel can talk to their insurer and change the policy so there is a payout under this circumstance."

Entirely new products can be created when requested. Vrumi is a startup allowing homeowners to rent rooms out to freelance workers. It's a novel idea – too novel for any standard insurance packet. So Vrumi worked with Safeshare Global

LEADING RISKS FOR UK COMMERCIAL INSURANCE CLIENTS

SURVEY OF INSURANCE BROKERS



Source: *Insurance Times* 2015

MAJOR CHANGES TO THE EXISTING INSURANCE LAW SYSTEM

FOLLOWING THE INTRODUCTION OF THE INSURANCE ACT 2015

- Responsibility of disclosure will shift from the insured by imposing a duty of inquiry on the insurer and limiting the insured's duty of disclosure
- Proportionate remedies introduced for non-disclosure
- Insured allowed to remedy a breach of warranty, merely suspending the policy while it is being breached
- In some cases the Act may allow the insured to disable an insurer's defence of breach of warranty or other term by showing that the breach of the warranty or term could not have increased the risk of the loss in question occurring

Source: Thomas Cooper LLP

LAWYER URGES CAUTION OVER NEW LAW

Shutterstock

Michael Wood, commercial solicitor and insurance expert at Keystone Law, points out some critical nuances in the new legislation

The Insurance Act 2015 is supposed to be good news for businesses because an innocent breach of warranty by the insured will not, under the new law, entitle the insurer to avoid the policy completely and so avoid liability for what would otherwise be a valid claim.

The difficulty which will remain, however, is the use in the new Act of those opaque words "fair" and "reasonable". Self-evidently, what is fair and or reasonable to one person may well not appear fair or reasonable to the other, particularly when the parties in question are parties to the same contract in relation to which they have fallen out.

It is said the new Act will redress the balance in favour of insureds, but this has yet to be tested. For example, section 8 provides that the insurer will have a remedy against the insured for a breach of the duty of fair presentation "only if" the insurer shows that, but for that breach, he would not have written the policy or would only have done so on different terms. But an insurer is always going to say one or the other of these two things, are they not?

There is nothing in the new law which suggests there will be any lessening in the number of cases coming before the courts, at all levels, where insurers and insureds dispute the insurers' liability to pay.

and Lloyds of London to develop a policy that would cover users of the service. It's an example of how flexible the industry has become.

The Insurance Act 2015 makes this opportunity to rethink contracts all the greater. The Act comes into force on August 12 and the government calls it "the biggest reform to insurance contract law in more than a century", referring to the Marine Insurance Act 1906, which is the foundation stone for the industry.

In terms of claim approval, the Act aims to introduce a more reasonable and nuanced approach to claims. Under the old regime, a claim could be rejected on tangential grounds. For example, a factory burning down in Sweden could be denied a pay-out because the owner possessed a factory in India, but had failed to pass on this information to the insurer. The Act means irrelevant errors must be ignored. Relevant issues will be assessed in proportion to their impact on the claim.

> "The Insurance Act 2015 comes into force this August, bringing in a whole new culture of coverage

The Act changes the way risks are reported. The old method demanded insured parties disclose every risk and circumstance the insurer might think relevant. A lot of guesswork was involved. Under the 2015 Act, there is a new "duty of fair presentation". Insured parties must provide "all material circumstances" or make the insurer aware there may be need for further questions on their part. Ideally, disclosure should be more thorough and collaborative.

Companies will need to take advice on their new duties under the Act. Ben Aram, a partner at international law firm Kennedys, says: "Although this new duty is likely to reduce old practices by companies, such as 'data dumping', it also raises a whole range of unanswered questions on precisely what kind of information insureds are expected to deliver and how.

"Both savvy corporate insureds and their insurers are, therefore, likely to seek to negotiate and include in their policies the specific parameters of 'reasonable' searches."

The Act will take a year or two to bed in. You'll need excellent advice to navigate the choppy waters in this period.

In fact, it's good practice to take advice on all areas of insurance. It is frankly amazing that so many companies fail to use brokers or independent loss adjusters in the event of a claim.

Mr Balcombe of Harris Balcombe offers some strong advice. "When a company has a major disaster they assume they need to phone an insurer. What they actually need to do is employ a loss adjuster. Don't rely on the loss adjuster appointed by the insurers," he says.

"Loss adjusters are not as independent as they make out. They are allowed to represent the insurer. You wouldn't go to court without a solicitor or barrister. Why on earth would you entrust the financial security of the thing you value most without the correct support."

Insurance is a tough game. Get it wrong and you could be badly out of pocket. With this in mind, it's a wonder so many companies are novices.

Share this article online via
Raconteur.net

COMMERCIAL FEATURE

CHANGING NATURE OF BUSINESS INTERRUPTION

Traditionally, businesses and insurers expected business interruption to arise from physical perils such as fires and floods. But in today's highly complex and technological world, not all sources of disruption emanate from physical damage, says ***David Hall****, managing director of retail at QBE Business Insurance*

Labour strikes, cyber intrusion, power outages, disruption to transportation networks, political unrest and terrorist threats. These are just some of the reasons businesses and their supply chains have been prevented from going about their normal day-to-day activities in recent months.

On May 15, a fake bomb caused a football match at Old Trafford to be postponed, just minutes before kick-off in a premiership game between Manchester United and Bournemouth.

Other recent causes of disruption have stemmed from the French ferry workers strike and migrant crisis, which resulted in gridlock for days on the M20 and into the Continent. In total, cross-Channel disruption cost the UK economy an estimated £250 million a day.

There is a growing realisation among risk managers, insurers and brokers that in a global, interconnected world, where technology plays an increasingly important role, business interruption can arise from a wide range of sources. Each of the top ten risks identified by the World Economic Forum *2016 Global Risks Report*, including large-scale involuntary migration, data fraud or theft and interstate conflict, can disrupt the normal flow of business.

Because so many of these sources of business interruption can be caused by events that do not result in physical damage to the insured or its main suppliers, it is now accepted that traditional business interruption (BI) insurance cover needs a rethink. This was the conclusion of an Airmic guide on *Overcoming Hurdles in Business Interruption*, produced in partnership with broker Marsh.

Organisations of all sizes and from a variety of different sectors are vulnerable to cyber attacks. According to QBE's Business Risk Sentiment research, conducted in the latter part of 2015, businesses perceive the overall level of risk has increased, the key drivers of which are cyber crime and data security risk.

However, the impact of business interruption arising from a cyber attack is a risk that can be underestimated. In 2011, the Sony PlayStation Network was down for nearly a month after a hack that exposed 77 million accounts.

The main impacts UK businesses say they have suffered, according to the UK government's *Cyber Security Breaches Survey 2016*, are staff time taken up both in dealing with a breach, being prevented from working as usual and repair costs. This was echoed by an Aon Risk Solutions report which found that while "media coverage of cyber incidents tends to focus on data privacy and regulatory fines, clients' number-one risk concern across the board is business interruption".

Insurers, working in partnership with brokers, should advise organisations on the extent of their BI coverage and on products that include both physical-damage and non-damage triggers, including specialist covers such as cyber that can help to plug any gaps. The onus is also on insurance buyers to make available quality data that will allow underwriters to build a clear picture of an organisation's risk profile, including its supply chain exposures, a duty that has been clearly enshrined in the Insurance Act 2015.

It is clear the wording surrounding business interruption risk and insurance needs to better reflect the realities of the modern business environment. Adapting traditional covers will ensure BI insurance is fit for purpose now and into the future, and will give comfort to insurance buyers. It will fulfil the promise of BI insurance, helping them get back on their feet as quickly as possible when the worst happens and indemnifying them for any loss of income, whatever the cause.

www.QBEeurope.com

2016 GLOBAL RISKS REPORT

◆ Technological ◆ Economic ◆ Environmental ◆ Geopolitical ◇ Societal

Top 10 risks in terms of likelihood **LIKELIHOOD**		Top 10 risks in terms of impact **IMPACT**	
1	Large-scale involuntary migration	1	Failure of climate-change mitigation and adaption
2	Extreme weather events	2	Weapons of mass destruction
3	Failure of climate-change mitigation and adaption	3	Water crises
4	Interstate conflict	4	Large-scale involuntary migration
5	Natural catastrophes	5	Energy price shock
6	Failure of national governance	6	Biodiversity loss and ecosystem collapse
7	Unemployment or underemployment	7	Fiscal crises
8	Data fraud or theft	8	Spread of infectious disease
9	Water crises	9	Asset bubble
10	Illicit trade	10	Profound social instability

Source: World Economic Forum *2016 Global Risks Report*

Staying alert against terrorist

Organisations should have contingency plans in case they are affected by a terrorist attack in an increasingly

GEOPOLITICAL RISK
HELEN YATES

In an increasingly global and interconnected world, political instability, unrest and terrorism can have a profound impact, disrupting supply chains, affecting staff safety, causing damage to property and interrupting business.

Geopolitical and societal risks topped the list of concerns on the World Economic Forum *2016 Global Risks Report*, with 79.4 per cent citing state collapse or crisis, interstate conflict and failure of national governance as causing the greatest concern over the next 18 months. With its close relevance to geopolitical risk, 52 per cent were concerned about the widespread ramifications arising from large-scale involuntary migration.

The findings give some indication of how UK business can be disrupted by geopolitical events at home or abroad, clearly a primary concern for business leaders. Risk management respondents to this year's *Allianz Risk Barometer* cited business interruption as their top global risk for the fourth year in succession. Alongside traditional drivers, such as natural perils, they identified geopolitical instability as a new source of disruption.

> Businesses need to think about how they might respond if transportation systems or city centres shut down in the aftermath of an event

Whatever the nature of the threat, organisations need to prepare for a man-made catastrophe in the same way they have always prepared for a natural event, says Charles Hecker, global research director at Control Risks. "We need to be able to forecast thunderstorms and political storms at the same time," he says. "You have to have a very good bird's-eye view of your global footprint. Companies and organisations that do not have detailed and tested crisis management and crisis response plans will be caught out."

While the UK may be relatively well insulated from terrorist incidents, an increasing proportion of UK businesses have operations overseas or they may source components and services from global suppliers. This is where geo-mapping can be a useful tool in helping to understand an organisation's global footprint.

In its *Roads to Resilience* report, Cranfield School of Management and Airmic identify the importance of a rapid response to a crisis. It uses the example of the InterContinental Hotels Group, which found itself "in the centre of the storm" when the Arab Spring broke out. The organisation immediately went into crisis management mode and assisted other hotel groups that were adapting to the rapidly escalating situation.

"Some of the businesses that responded most effectively to recent unrest and terrorist events are those that have plans and practise them," says Julia Graham, technical director at Airmic. "I know several who, when events happened in North Africa, Paris or Belgium, because they had plans and had rehearsed them, knew what to do and their people also knew what to do."

A duty of care towards staff is essential, says Ms Graham, formerly the chief risk officer of international law firm DLA Piper and president of the Federation of European Risk Management Associations. She was at the airport in Brussels when the Paris attacks were unfolding on the night of November 13 last year. "Even though I'd left DLA Piper at that point, a former colleague who was in Paris called me and asked what I thought they should do," she says.

"One of the biggest issues is in travel and duty of care. If you've got people travelling around you've got to know where they are. It's no good having people caught up in an event and having no idea who is in a country, where they are and what they're doing. Know where your travellers are going and make sure they know how to contact you in the event that something goes wrong."

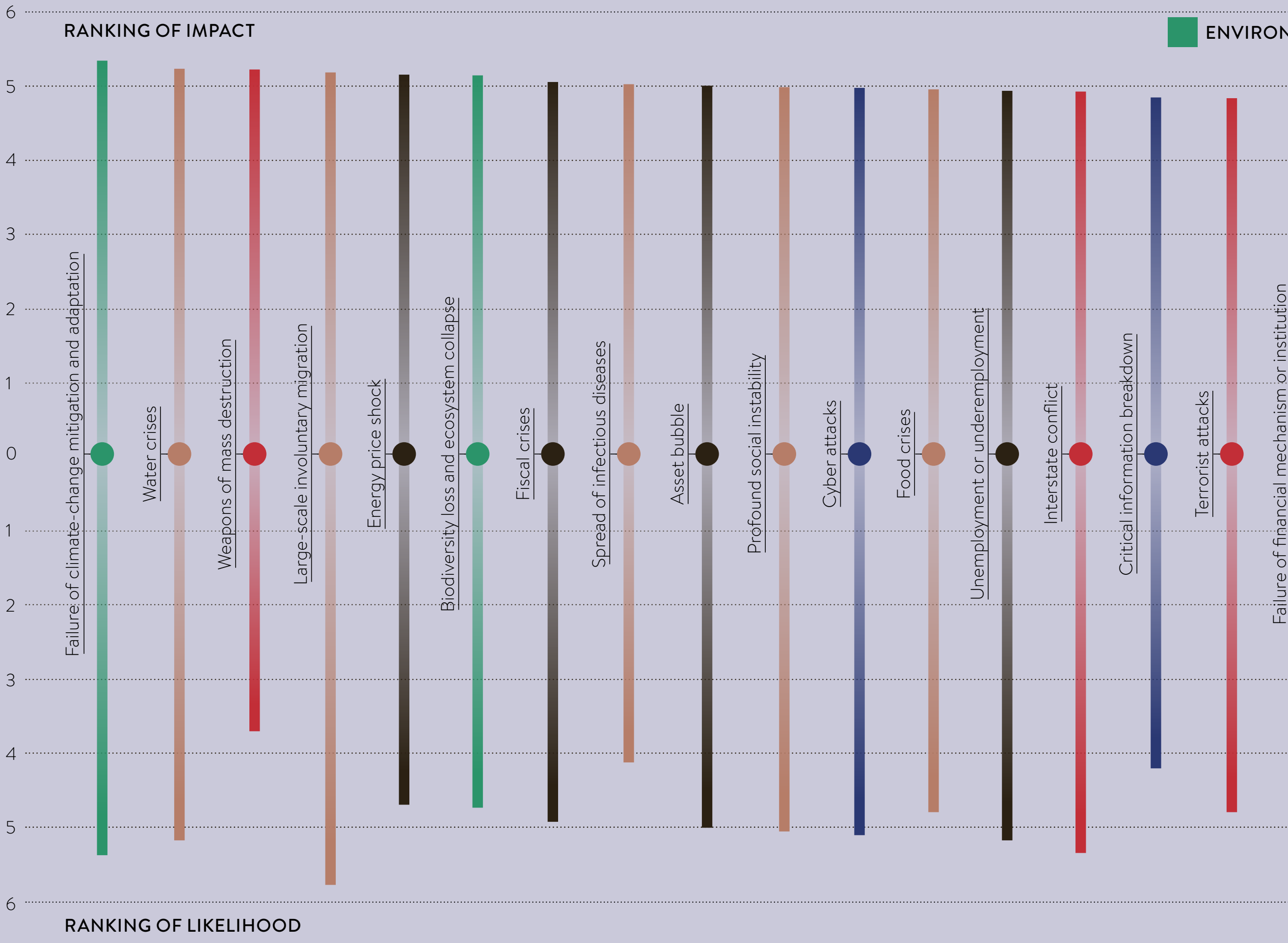
This is even more pertinent given the modus operandi of the so-called Daesh Islamic State or IS. Recent terrorist attacks have clearly demonstrated IS is targeting civilians and infrastructure with its primary aim to cause fear, disruption and panic.

"Traditionally, terrorism has been defined by attacks on property, resulting in significant business interruption," says Scott Bolton, director of crisis management at Aon Risk Solutions. "However, the rise of IS has brought about an increase in the use of shootings versus bombings as well as the targeting of private citizens and public gatherings, as seen most recently in Brussels. This new environment means businesses need to reconsider their risk profiles to more effectively limit the impact of attacks on their people, operations and assets.

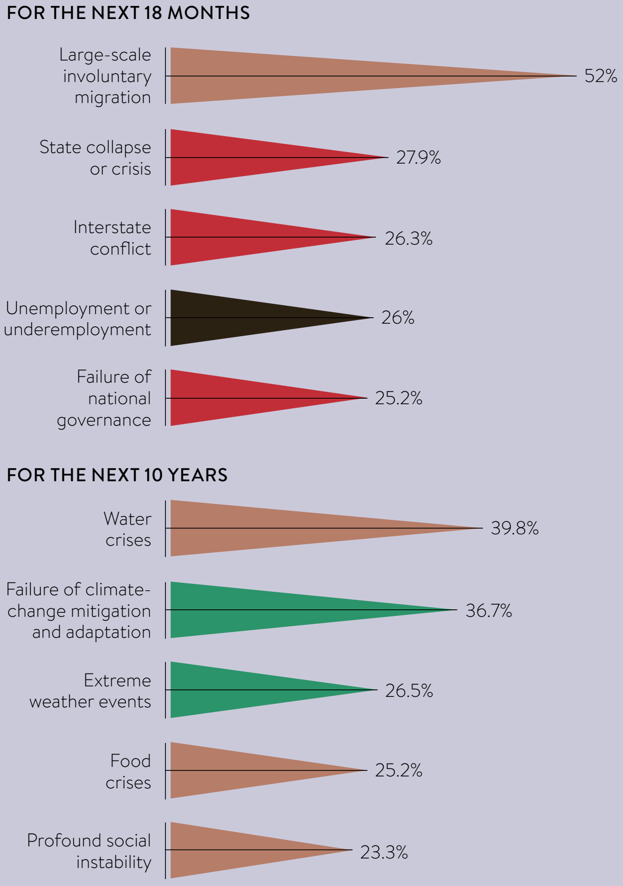
"We need to think more about how we limit the impact of an attack. For example, in an office tower, we can close off lift and stairwell access to the floors above, limiting the opportunity for terrorists to access additional targets."

GLOBAL RISK LANDSCAPE 2016

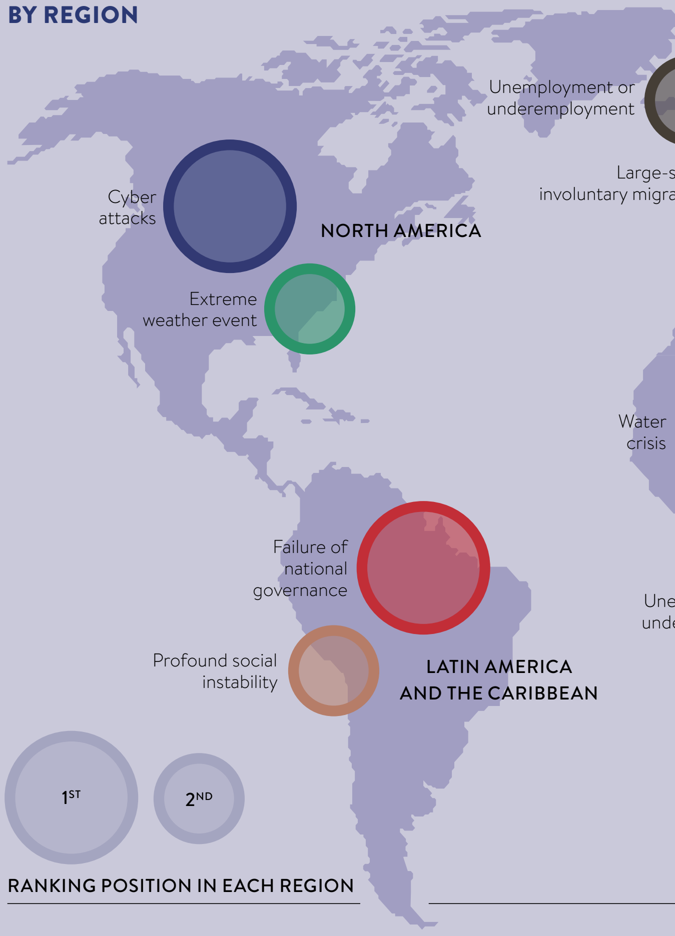
RANKING OF ONE TO SEVEN; SEVEN REPRESENTS A RISK THAT IS VERY LIKELY TO OCCUR AND HAVE MASSIVE AND DEVASTATING IMPACTS



GLOBAL RISKS OF HIGHEST CONCERN

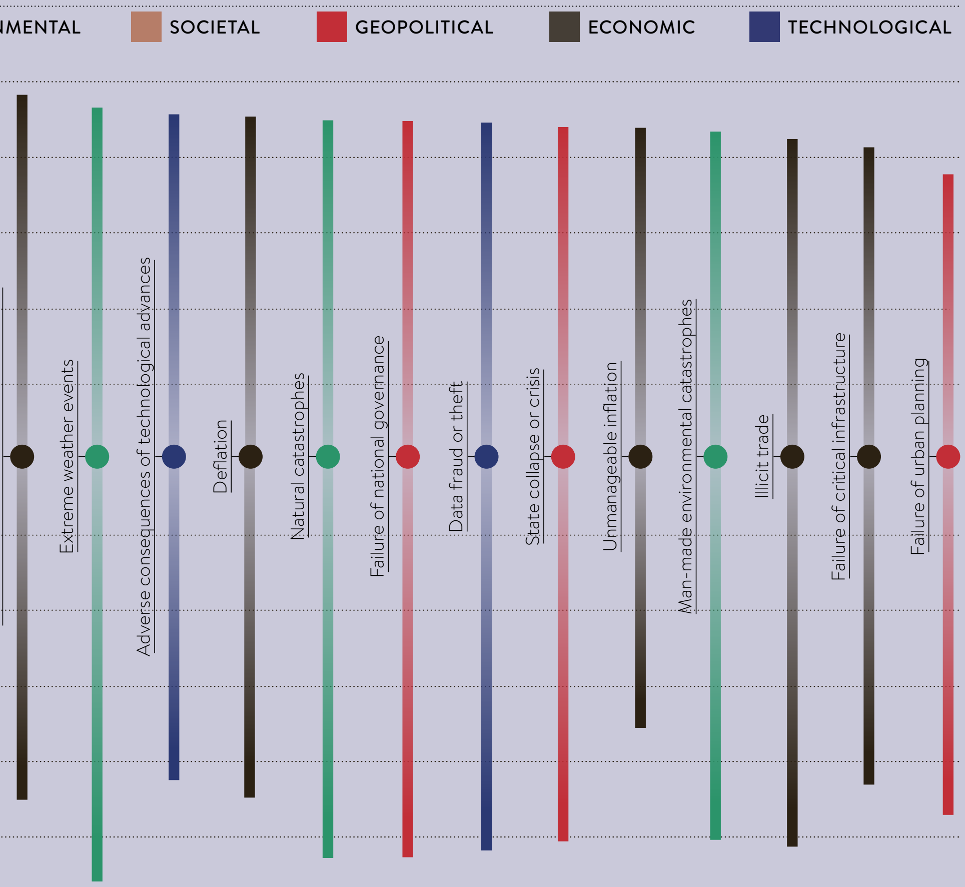


MOST LIKELY GLOBAL RISKS, BY REGION


Unemployment or underemployment
Large-s
involuntary migra
Cyber attacks
NORTH AMERICA
Extreme weather event
Water crisis
Failure of national governance
Une
unde
Profound social instability
LATIN AMERICA AND THE CARIBBEAN
1ST
2ND
RANKING POSITION IN EACH REGION

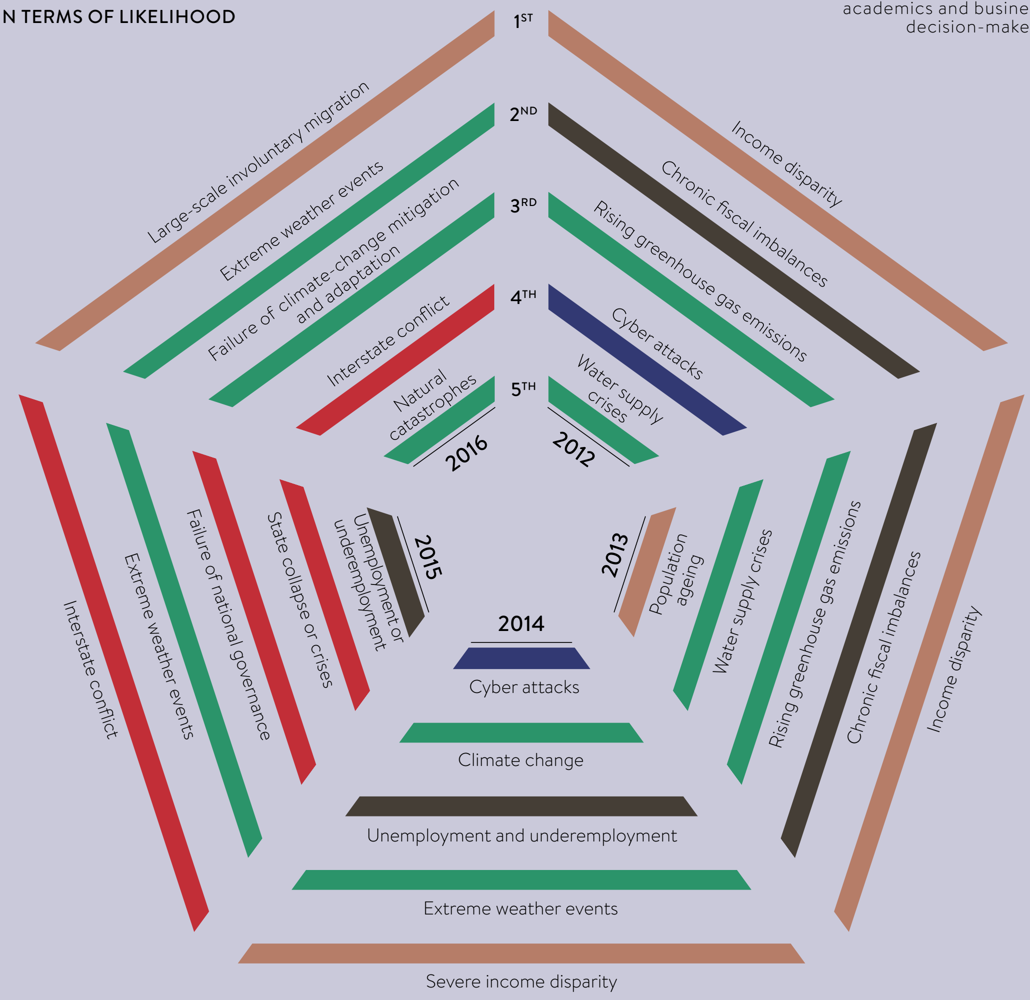
attacks at home and abroad

y uncertain and war-torn world where bombs and bullets kill and wreck lives

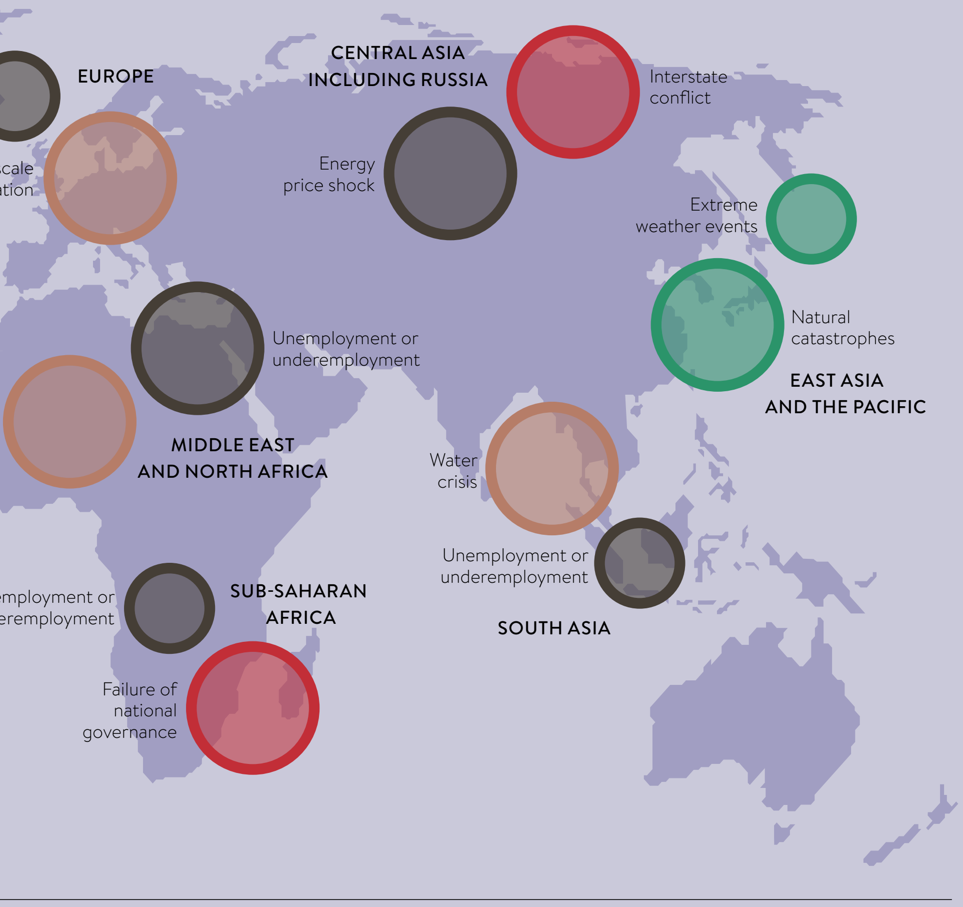


EVOLVING RISKS LANDSCAPE
IN TERMS OF LIKELIHOOD

Survey of 750 global academics and business decision-makers



Source : World Economic Forum 2016



EUROPE
cale
tion
CENTRAL ASIA INCLUDING RUSSIA
Energy price shock
Interstate conflict
Extreme weather events
Natural catastrophes
EAST ASIA AND THE PACIFIC
Unemployment or underemployment
MIDDLE EAST AND NORTH AFRICA
Water crisis
Unemployment or underemployment
SOUTH ASIA
mployment or
eremployment
SUB-SAHARAN AFRICA
Failure of national governance

While the chances of being directly caught up in a terrorist attack remain low, businesses need to think about how they might respond if transportation systems or city centres shut down in the aftermath of an event. It took five weeks to reopen the departures hall at Brussels Airport following March's deadly attacks.

"What we haven't seen so far in IS activity is a direct and specific targeting of business and commercial interests," says Mr Hecker. "We have seen attacks on public venues and government infrastructure, and these are important things to take into consideration when doing crisis management planning.

"I used to work in our Moscow office and expats would often say to me, 'In the event there are tanks on the streets in Moscow, I've got an open-ended air ticket out of here'. I would respond asking what they would do if the roads to the airport were blocked. So depending on how a terrorist incident unfolds, there are lots of different things that would become difficult to do."

Businesses can also find themselves caught in the crossfire of a terrorist incident. Certain types of organisation are going to be most vulnerable, such as shopping malls, transportation systems and stadiums where large numbers of people gather. "Trophy" buildings, stock exchanges and central business districts are also more prone to disruption. Spatial awareness is an important factor in risk assessment and response planning.

In the 15 years since 9/11, counterterrorism surveillance has improved considerably and the world has changed. Nevertheless, businesses should remain on alert, says Mr Hecker. "Attacks in Paris, Brussels, Jakarta, Beirut, Ankara and Istanbul show us that IS now has the capability to execute complex operations fairly far from its comfort zone. There has been a real internationalisation of what IS can do and that puts cities like London and countries like the UK on alert," he says.

Other examples of geopolitical risk can be less impactful, but cause much longer-term uncertainty. The rapidly approaching EU referendum on June 23 is one example.

"Businesses cherish predictability and stability," says Mr Hecker. "Whether the referendum is close or a landslide there has to be some sort of feeling that it is decisive and the issue has been resolved, as the prime minister says, for a generation. Otherwise this instability we're feeling now could remain and I don't think business will want or like that very much."

Ms Graham thinks that while it is likely to be a slow burner, the prospect of a Brexit should be among the principal risks identified by the boards of public companies. "I don't know how any listed company should not be preparing their businesses for this," she says. "It's not a subject for crisis management, because if something goes wrong it won't happen overnight, but nevertheless you need to be prepared and look at different scenarios."

Another, associated issue is Europe's migrant crisis, which is a big factor behind the rise of European far-right political parties. However, alongside the potential risks there are also opportunities for organisations that have planned and responded appropriately. Many migrants, for instance, are highly skilled individuals and could enhance workforces in their adoptive European countries.

Share this article online via **Raconteur.net**

OPINION COLUMN

Successful organisations have a risk-aware culture

Fostering the right kind of corporate culture lies at the heart of successful risk management

JOHN HURRELL

Airmic
Chief executive

Many outside suppliers at Virgin Atlantic are given the company uniform to wear so that they feel part of the "family" and are more likely to promote its values. Management at Drax power station were inundated with valuable risk information after offering employees supermarket vouchers in return for tip-offs about safety near-misses. Junior staff at the insurer AIG are actively encouraged to ask their bosses difficult questions about the way the company is run.

These are three of many illustrations of how organisations have developed risk-aware cultures, all of them featured in our 2013 report, researched jointly with Cranfield Business School, *Roads to Resilience*.

Conversely, a 2011 piece of research, by CASS Business School and published by Airmic risk management association, *Roads to Ruin* investigated 23 companies with aggregate pre-crisis assets of more than $6 trillion, all of which had suffered potentially life-threatening corporate traumas. In every single case corporate culture was at fault. In all but one, for example, there was a failure of risk information known within the organisation to reach the top, creating "risk blindness" at board level.

These two pieces of in-depth research demonstrate how risk management goes much wider than mere compliance or having the right processes in place, essential as these factors may be. All corporate disasters reflect the behaviour of people working for the organisations concerned – as do the success stories. And behaviour invariably reflects culture, which more than anything else determines the robustness of an enterprise's risk management.

The UK Corporate Governance Code, published in 2014, underlines this view. It is quite explicit about where responsibility for risk management and internal controls lies – with the board. The guidance includes specific reference to risk culture and assurance, and the need to ensure that an appropriate culture is embedded throughout the organisation.

How to make this happen is, of course, a complex and demanding question. However, the two pieces of research mentioned provide some helpful insights into where the solution lies. *Roads to Ruin* found that corporate failures had a remarkable amount in common, regardless of the sector of the company involved.

Lack of the necessary board skills and insufficient control by non-executive directors, board risk blindness, leadership failures, poor communications, organisational complexity, inappropriate incentives and a "glass ceiling" that prevents risk information reaching the board – these factors recurred time and time again.

Similarly, *Roads to Resilience* found that well risk-managed organisations have much in common with each other. They all promote the idea that everyone is responsible for risk and constant vigilance is required (hence the earlier example of Drax), complacency has been engineered out, and constant questioning and challenge are encouraged (for example, at AIG). All the organisations appreciate the critical importance of good communication.

Sadly, we fear these shining examples represent a minority of enterprises. It is only a matter of time before the next big corporate disaster and, when it comes, we will see how it could have been avoided. But you do not need hindsight to do so. Any organisation can develop the culture to handle all eventualities swiftly and effectively – even the so-called "black swan" events. This represents perhaps the board's biggest single challenge and duty.

Getty Images

Leicester City football team on their Premiership winners' parade earlier this month

Building a team can be a risky business

If people are a business's most valuable asset, how do you assess the risk of losing them?

HUMAN CAPITAL

PETER CRUSH

Football clubs might not be the first businesses to spring to mind when it comes to conversations about human capital and risk, but they probably understand it a lot better than most.

Build a team around a few key players and, if they leave or can't play, disaster inevitably awaits. That's why Leicester City's recent Premier League triumph was such a shock. It involved just 23 players – the fewest in the league.

Physiotherapists say it was having the fewest injuries of any top-flight club that really saw them through. Indeed, according to a report this month by human capital analyst Organisational Maturity Services, Leicester would actually be in the bottom half of the table if ranked on their human capital index. This is an AAA to D scale that rates organisations in terms of key management systems, such as talent pools and succession planning, and predicts long-term, sustainable success.

> Build a team around a few key players and, if they leave or can't play, disaster inevitably awaits

Paul Kearns, chairman of the Maturity Institute, which developed the scale, points out that this type of ranking acknowledges the well-known human resources cliché, which says "people are a company's greatest asset", and so by definition people pose risks too.

But while grading goes some way to comparing how organisations manage their human capital, he says putting a number on the balance sheet about the people component of risk is still the Holy Grail of HR and accountancy.

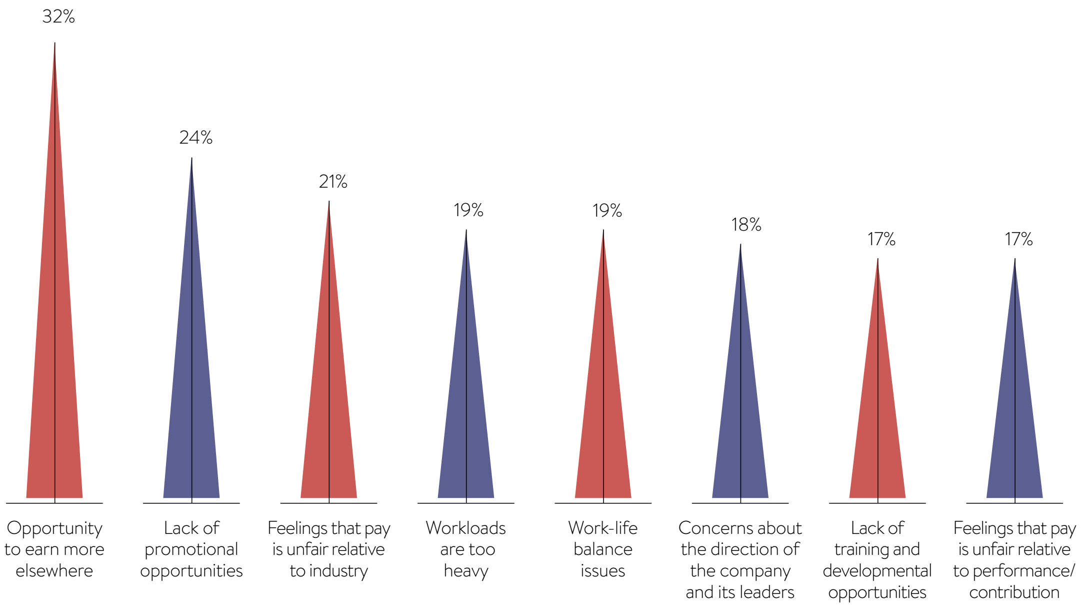
"Added value stuff is fairly easy to demonstrate," says Mr Kearns. "Training adds value, while reward structures that aid retention also add value. But risk is always 'lost' value and that's always hard to calculate."

According to the *Harvard Business Review*, 80 per cent of a company's value is its people, but while the departure of a chief executive of finance director can trigger stock market revaluations, these are nearly always short lived and don't account for the contribution (or lack of it) from the rest of the staff.

"Markets still seem trapped using the 'leader as hero' way to either value or devalue a business, even though they know it's not the case," says Catherine Shepherd, development consultant at Roffey Park Institute. "There is hardly ever talk about the whole human capital in a business and the impact of people making mistakes, turning against their employer or leaving – all things that do actually happen."

TOP REASONS WHY KEY EMPLOYEES QUIT

PERCENTAGE OF HR PROFESSIONALS THAT AGREE WITH THE FOLLOWING STATEMENTS



Source: WorldatWork

Infosys is one of the few businesses quoted as making some attempt at putting a value in areas like this. It uses the famous 1971 Lev and Schwartz accounting model to calculate employees' collective worth. But even this is a formula based on the present value of future earnings, adjusted for such things as the probability of employees' death, separation, retirement or training.

Today this model would fail to account for, say, the social network value of people and the positive or negative impact those with lots or a few social media followers might add to a business. It also doesn't consider the implications of what some argue is an even greater contributor to risk – organisational culture.

"There's a phrase 'culture eats strategy for breakfast'," says Rob Noble, chief executive of The Leadership Trust. "Leaders have a role creating a common set of behaviours and expectations, and this must be a part of assessing risk, but it's also hard to pin down.

"At this level of granularity, other things like whether you have diverse teams or good female representation also feed into this because diversity is known to avoid group-think and challenge decision-making that might fly in the face of the culture of the business."

Mr Noble believes that in most companies it's not lone wolves who pose the greatest risk, but rather it's the environment in which employees are expected to work that has most impact and this is partly set by the executive.

An organisation that is trying to make sense of all of this is enterprise applications provider Unit 4. Kara Walsh, chief human capital officer, says: "My job title reflects the CEO's view people are assets and so I do calculate risk as I see it, including the risk of people leaving us, especially those in R&D.

"We also look at the risks to the business of having people not performing as high as those being more productive. This is a big change in dialogue around people compared with what was happening 20 years ago.

"People are intangible assets, but other things we measure, like time to productivity, makes them tangible. We would say productivity is actually our greatest area of risk. To lessen it, we've reduced the time it takes new hires to get up to speed time from nine to six months.

"A project I'm looking at now is productivity gaps and extrapolating a value for this in terms of the risk of not improving it going forward. Taking this approach means we put a value-add on things like training, which moves our performance needle along. The simple fact is, if you class your people as an asset, you have to treat them like any other asset. That means investing in them to grow value."

Experts argue taking a company-wide, systemic approach to risk, rather than trying to find it in one or two people that might cause damage, is a much better overall defence.

"Investment management company Black Rock will now rank the organisations it thinks are better to invest in according to diversity metrics, while analysts are also looking at things like the risk around not paying staff a living wage," says Mark Quinn, UK head of talent at Mercer.

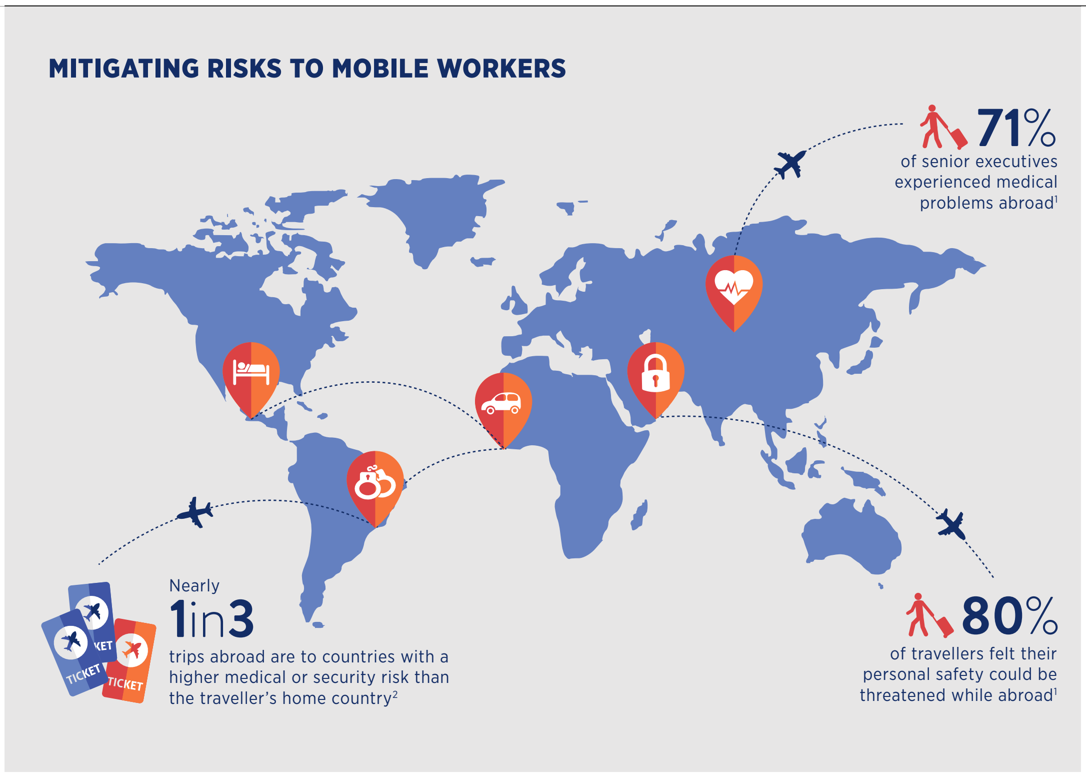
"HR has long had things like strategic workforce planning, succession planning and talent pipeline programmes, which will all mitigate the risk of key people leaving, so combining the two will be more common. Predictive analytics will start to look at what the path for staff is if you hold on to them and all this feeds into the people side of risk."

But while experts might still be divided on how to quantify risk, one thing they are agreed on is the irrelevance of options such as key-person insurance, which firms can take out to protect themselves against risk.

"This only encourages bad management," says Mr Kearns. "Insurance won't keep people, so paying it is simply a cost to a business. It's far better to look at your own management systems." Mr Quinn agrees: "It's disaster recovery only and not a solution to risk."

Share this article online via **Raconteur.net**

COMMERCIAL FEATURE


MITIGATING RISKS TO MOBILE WORKERS
71%
of senior executives experienced medical problems abroad[1]
Nearly
1in3
trips abroad are to countries with a higher medical or security risk than the traveller's home country[2]
80%
of travellers felt their personal safety could be threatened while abroad[1]
TICKET
TICKET
KET

[1] *International Travel: Risks and Reality*, an Ipsos Global @dviser research study, 2015 [2] International SOS travel tracker data

MITIGATING RISKS TO MOBILE WORKERS

Organisations entering uncharted markets expose staff to new risks

INTERNATIONAL SOS
WORLDWIDE REACH. HUMAN TOUCH.

After watching the news or reading the newspapers, many people could think we are living in increasingly risky times. Cities we previously thought were generally safe, such as Paris and Brussels, are now portrayed in the media to pose a threat to travellers, and global events like the European migration crisis are unprecedented.

While it's true that some things are indeed different from 12 months ago, one of the fundamental principles of risk management is to understand and assess the actual, rather than the perceived, risk.

The world hasn't suddenly become a riskier place, but what is the case is that businesses, drawn by the need to send their staff into new countries, to develop new markets and maintain a competitive edge, are exposing their people to new risks.

It's gauging this exposure to risk from a safety, productivity and business continuity perspective that is vital for organisations to get right. Terrorist attacks and pandemics are likely to grab headlines, but it's the more mundane, everyday occurrences like road accidents, petty crime and illness that are actually the largest causes of disruption to both the travelling employee and their organisation.

These disruptions matter. At the very least, there are the costs to business of lost productivity, revised travel itineraries and incomplete projects due to staff spending their time in consulates, in police stations or navigating local healthcare systems.

> Mitigating risk is all about knowing the facts and being prepared

More concerning though is the potential for exposing both the traveller and the organisation to further risks as minor incidents can have major safety and financial repercussions if not properly managed.

So what does all this add up to? As already noted, we need to put risk into perspective. Threats aren't necessarily hiding around every corner and the vast majority of employees live, work and travel abroad without incident. However, it's also important to remember that a "been there, done that" view can breed complacency.

We find many organisations underestimate risk by assuming that because their people have previously travelled to certain territories and come back without incident, there is nothing to worry about. But people make their own, often unpredictable, decisions. That's why travellers themselves and their travel behaviour are key components to overall risk mitigation.

Organisations should ensure business travellers are trained and equipped to make the right decisions if exposed to a security or medical incident. Equally, it is vital organisations know where their people are and can communicate with them in an emergency and support them with trusted, qualified local resources.

Travellers may also face risks based on their personal characteristics, such as age, race, gender and sexual orientation. Organisations need to be aware of these variances and provide appropriate guidance for all their travelers.

Mitigating risk is all about knowing the facts and being prepared. The health, safety and security of mobile workers falls under the responsibility of the employer. There is a need to have clear organisational policies in place and competent individuals to mitigate these risks to staff.

For more information please visit www.internationalsos.com

How to pre

Companies are largely unprepared for an
probability they will become victims

CYBER RISK
DAVEY WINDER

NTT Com Security's *Risk:Value 2016* report reveals only 45 per cent of UK business has any kind of insurance to cover the financial impact of data loss or a security breach. However, 37 per cent admitted that poor security could invalidate that cover. Which begs the question why are so many organisations unprepared for a serious cyber attack, given a quarter are expecting one to hit them in the next 90 days?

That the threat-scape has evolved from hackers looking for notoriety into a well-organised, and highly profitable, criminal enterprise is beyond debate. Yet many organisations still perceive cyber security as a technology issue rather than a business matter. "This asymmetrical nature is why cyber security must have input at a strategic business level," says Greg Sim, chief executive at Glasswall Solutions.

"Risk mitigation should be integrated into core business processes, as opposed to being an afterthought in which only the bare minimum of managing, and not solving, the impact of a breach is done."

There's even an argument to be made that attackers should be seen not solely as criminal adversaries, but as competitors in the market. "Business leaders must understand cyber criminals' business models, strengths, weaknesses, opportunities and threats just as they would their competitors in the marketplace," says Tim Grieveson, chief cyber and security strategist, for Europe, the Middle East and Africa, with Hewlett Packard Enterprise.

> Many organisations still perceive cyber security as a technology issue rather than a business matter

With some organisations still not having cracked who "owns" security, be it the chief technology officer, the chief information officer or even the chief executive, it's hardly surprising business is often so unprepared for attack.

"When ownership, responsibility and accountability are confused," says Adrian Crawley, regional director for Northern Europe, the Middle East and Africa at Radware. "It dilutes the effectiveness of the strategy and in most cases undermines the budget needed to put in place the right processes, policies, people, partners and technology."

Which is why we end up with situations such as a case recounted by Kroll's global investigations and disputes practice managing director Ben Hamilton, where a large energy company was in the middle of an attack. "The company was not able to protect its key processes or quarantine the hackers who were still in the system," says Mr Hamilton, "because it did not know what data or processes were being managed on what servers."

As Richard Horne, cyber security partner at PwC and a former cyber security director with Barclays, says: "A unique feature of cyber-related crises, as opposed to physical ones, is the often total lack of facts in the first 72 hours, such as answers to seemingly obvious questions like what data has been taken or what systems are affected?"

But it's not just at the business end of things that such confusion exists; the complexities of cyber have led to a confused insurance marketplace as well. While some insurance brokers are undoubtedly making sure they are well educated with cyber risks, that's not always the case.

"I think the insurance sector is shying away from cyber because it's very complicated and we don't fully understand what the exposures are or how the insurance policies can respond," says Tim Ryan, executive chairman at UNA Alliance, which is owned equally by 11 of the UK's largest regional insurance brokers. Mr Ryan says his organisation has seen evidence of people being sold cyber policies that have no bearing on what their risk is. "This, in turn, is a risk in itself," he adds.

pare for serious cyber attack

assault by hackers and fail to mitigate the risk of cyber attack as a business priority despite the growing

Details of 157,000 TalkTalk customers were compromised in a cyber attack last October, resulting in a financial cost of £60 million

When designing cyber cover, insurers must take into account not only a business's liability to its customers, but also potential impacts on the business itself, while the client's customers may find their finances, intellectual property or reputation under threat due to a leak of personal details or commercially sensitive information.

Ben Rose, insurance director at Digital Risks, says: "The business itself also has to consider issues such as website downtime, loss of sales and long-term reputational damage." The cumulative cost of all these issues can make cyber insurance particularly complex and expensive.

The insurance industry needs collectively to set premiums that truly reflect the risk, but how do you put a price on a breach? The challenge is to achieve an objective measurement of the true costs incurred. "This is where, by working with the information security industry, they can gain a better understanding, so that insurers can more accurately calculate a risk profile and what the potential impact cost would be for different events," says Kirill Slavin, managing director at Kaspersky Lab.

Paul Simpson, principal consultant with Verizon RISK, reveals that his organisation's research points to a high percentage of all security incidents being traced back to just nine basic attack patterns. These are miscellaneous errors (such as sending an e-mail to the wrong person), crimeware (malware aimed at gaining control of systems), insider misuse, physical theft or loss, web-app attacks, denial of service, cyber espionage, point-of-sale intrusions and payment card skimmers.

"These vary from industry to industry, with each industry having three specific attack patterns connected to it," Mr Simpson says. What this means is that businesses can effectively shape their security strategies to combat these specific threat patterns. He gives the example of 88 per cent of attacks in the financial services sector following a denial-of-service, web-app attack or crimeware pattern.

Good things also often come in threes, such as a three-step crisis management strategy as Ryan Kalember, senior vice president of cyber security strategy at Proofpoint, explains. "A critical first step is an organised programme to compare actual risk to critical information assets against senior management's level of tolerance for the risk of losses due to cyber," he says.

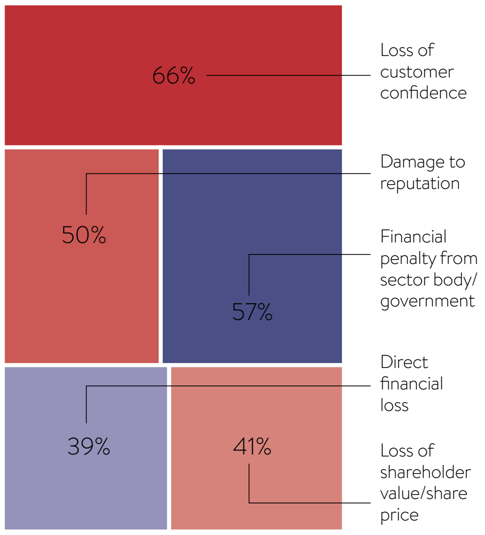
"Next, the security team needs to create an incident response and remediation plan to ensure they have the proper procedures in place to prepare for a cyber incident, such as a data breach, ransomware infection or a denial-of-service attack."

And finally, a coalition of key internal stakeholders needs to create a crisis communications plan. Usually headed up by corporate communications, this team includes cyber security, IT, customer support, web, legal and an executive sponsor.

"This team should develop a list of worst-case scenarios and outline which response processes an organisation will follow, and how the organisation will handle crisis communications with media, customers, employees and partners," Mr Kalember concludes.

Share this article online via **Raconteur.net**

MOST LIKELY EXTERNAL EFFECTS OF A SECURITY BREACH



Source: NTT Com Security 2016

RISK MITIGATION

Scott McVicar, general manager at BAE Systems for Europe, the Middle East and Africa, outlines five top measures for mitigating cyber risk

01 UNDERSTAND THE RISK

Understand where your business is and make sure your cyber security strategy is taking all movements into account. Review and update it constantly as your business changes and don't be caught out by the evolution of attackers.

02 HAVE THE RIGHT SECURITY CONTROLS

The perimeter is gone and the security controls of yesterday won't work. You need the security controls of today, protecting all the end-points with integrated, configured and patched security controls. Once the defensive controls are in place, continually monitor for a breach in the defences.

03 BALANCE BUSINESS AND RISK

Businesses need to have the courage to make the right decision that balances security risk against commercial return, and does the right thing by the business and customers in the long term. Take those difficult decisions on what systems and services are protected, and at what level.

04 BUILD A DEFENSIVE CULTURE

Security needs to be ingrained into the company culture. It isn't a checklist, but something which should be ever-present. Security by design involves everybody making sure they are working securely, whatever role in the company they have.

05 PREPARE A RESPONSE

What makes the difference between a full-blown crisis and a problem to be tackled is the plan you have in place to respond and repair. There needs to be a thorough, rehearsed response plan known to clients and employees. With the right planning, there's absolutely no need to make a bad situation worse.

COMMERCIAL FEATURE

HOW TO REFORM YOUR CLAIMS HANDLING

Risk managers need a single pan-European platform to handle claims – Van Ameyde's platform could be just the answer

Claims Management: 360° insight in risk

Van Ameyde

There's a common complaint from risk managers. Their beat covers multiple territories and in every location there is a different system. Reports are filed differently, processed differently and the data generated is different. Then the risk manager is asked to pool the data and it's impossible.

This is a serious issue. Fragmented data means there's limited overview. Trends can't be identified. And it's time consuming to deal with many local systems.

The optimum solution is to move to a unified pan-European claims and incident management system so there is one system in use across the entire continent.

Willem van der Hooft, business development director of Van Ameyde, says: "We see the same issues across the board. Risk managers who are responsible for a multinational scope are facing different processes and different systems with almost no integration between them.

"Risk managers then have to spend valuable time consolidating and matching data from different sources, and in the end they have to base their risk management strategy on incomplete information."

46
offices in 28 European countires

80%
of the work is automated, lowering costs and accelerating resolution times

30-50%
typical saving by Van Ameyde

The solution? Move to Van Ameyde for claims management and standardise everything across the continent.

There are three reasons to consider doing so.

The first reason is Van Ameyde's presence across Europe, with 46 offices in 28 European countries. A single solution can be rolled out in every territory. The nightmare of data fragmentation, multiple rival systems and unique local practices is ended.

A second big advantage is Van Ameyde's scale of solution. Every part of the claims journey is covered, from first notification of loss and triage to recovery of uninsured losses. From this moment every step is handled by the outsourcer.

The third benefit of the deal is the advanced use of technology. Van Ameyde offers an online management system. Around 80 per cent of the work is automated, lowering costs and accelerating resolution times. Van Ameyde offers a wide variety of data analytics tools.

Mr van der Hooft stresses the advantages: "It becomes easy to identify common themes. All systems are ISAE 3402 compliant – an assurance standard compulsory for many stock market-listed firms.

"The new arrangement means managers can view pan-European data on claims in real time. Costs are down. Typically Van Ameyde enables savings of 30 to 50 per cent. And claims handling is smoother. Senior management can focus on strategy, rather than matching and consolidating data."

The platform is ideal for large corporates in any sector. The same specifications are common across industries. There is a need for a single management system across regions, for economies of scale offered by a specialist and for an uplift in productivity derived by unifying all data so it can be analysed as a whole.

> The optimum solution is to move to a unified pan-European claims and incident management system so there is one system in use across the entire continent

A global car rental giant offers a textbook example of how to improve incident and claims management. It worked with Van Ameyde to create a bespoke solution for its European operations. Like many corporates, the client faced difficulties with its IT systems. It had a different set-up in different locations to manage its fleets. This made it a challenge to merge data into a whole and get a unified overview.

The company moved to Van Ameyde's Incident Management System. This online portal standardised incidents and claims across Europe. Using this new infrastructure, the client worked with Van Ameyde to identify areas for improvement, such as uninsured loss recovery.

As part of the continuous optimisation review, Van Ameyde and its client established processes to ensure quality of service delivery and cost-efficiency gains in casualty and liability claims management, and this risk has been fully entrusted to Van Ameyde.

Today, the company's data is clear, accurate and reliable. Productivity is up, and risk assessment and detection have vastly improved. Financial planners have the data they need to make accurate reports and forecasts. And customer and stakeholder satisfaction are higher.

"Claims management is a really important part of insurance, as well as risk management," says Mr van der Hooft. "Yet many companies have sub-optimal systems, resulting in lower productivity. We cover the whole of Europe with one solution which works everywhere."

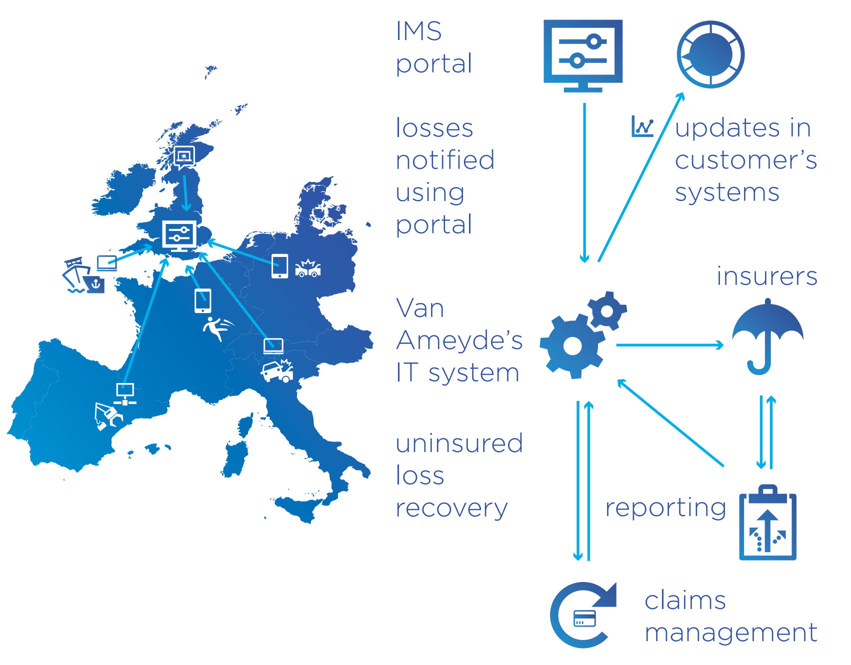
It's not the only area where a partner can help. Van Ameyde also offers risk assessment and auditing services, which help identify risks and result in practical recommendations. The analysis will take into account the company's unique requirements, such as its multi-office locations, supply chain, security, IT systems and compliance.

Valuation of fixed assets can be provided for the purpose of GAAP (generally accepted accounting principles) and IFRS (international financial reporting standards) or indeed insurance. Irrespective of the company's size, risk managers can all make use of this specialist service.

Risk managers play a vital role in companies. They need the best solutions and technology available. It is essential they be given a unified pan-European reporting and claims management system. Trade doesn't stop at borders – nor should claims management.

To find out more visit vanameyde.com or call in at Booth 85 at the Airmic 2016 conference

Van Ameyde's Incident Management System



Countering the impact of catastrophes

Businesses with comprehensive contingency plans, proper oversight, modern technology and agile management can mitigate the damage caused to supply chains and production by a natural disaster

NATURAL DISASTERS
DAN MATTHEWS

Sadly there are scores of natural disasters around the world each year. Floods, storms, wildfires, volcanoes, earthquakes and tsunamis are relatively common events that routinely bring with them death and destruction, most often to the developing world.

The tragedy of these events is in the loss of lives and wrecking of communities, but they increasingly also have a disruptive impact on global trade. A delicate web of supply chains crisscrosses the globe with manufacturing units, transport hubs, warehouses and service providers coming together to create the things we buy.

It’s a symphony of moving parts that relies on benign and predictable conditions for it to work. An unexpected event disrupting one part of the machine can bring the whole thing grinding to a tuneless halt.

As recently as April, two earthquakes in Japan caused car manufacturer Toyota to suspend production at several plants due to parts shortages. Other companies in the region including Sony suffered damage to factories and subsequent disruption.

Transport was severely disrupted as landslides cut off major roads and the clean-up bill ran into tens of millions of pounds. This in a prosperous country with some of the toughest construction regulations in the world, due to its regular bouts of seismic activity.

“Other examples include the Icelandic volcano eruption in 2010, whereby volcanic ash in the atmosphere shut down much of Europe’s airspace for a number of days. This brought significant disruption to air freight shipments,” says Mark Morley, director at OpenText Business Network.

“The 2011 Japanese earthquake resulted in severe devastation to utility infrastructures and the consequential tsunami brought longer-term disruption to global supply chains due to many factories being flooded. Ultimately, production had to be halted.

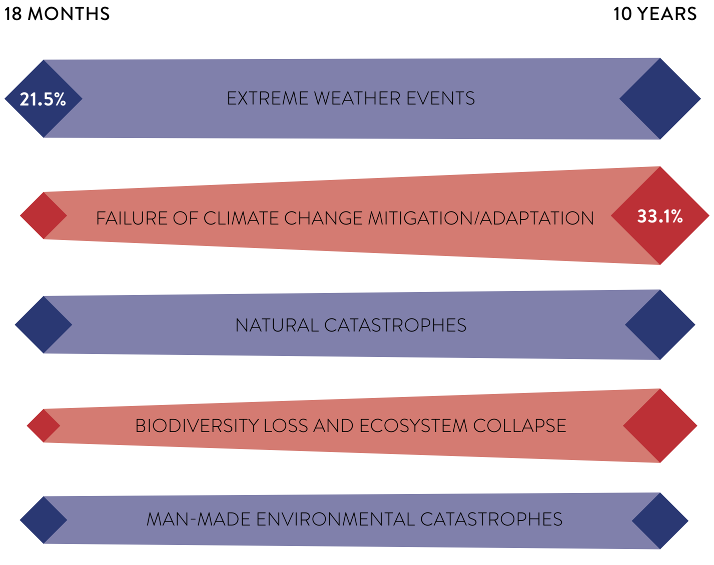
“Hurricanes, too, cause supply chain standstills. In the wake of Hurricane Isaac and Hurricane Katrina, severe flooding, power outages and a lack of fuel to transport goods caused supply chains to be brought to a halt.”

Globalisation and lean processes are two factors that are magnifying the disruption caused by “acts of God”. As the world becomes more intimately connected and pressure on profit margins intensifies, chains are becoming even more brittle and vulnerable.

Getty Images

Companies such as Toyota and Sony experienced severe operational disruption from two earthquakes in Kumamoto, Japan, in April

GLOBAL ENVIRONMENTAL RISKS OF HIGHEST CONCERN



World Economic Forum 2015

Combine these factors, plus tight delivery deadlines, consolidation strategies and shrinking contingency stocks, with the likely impact of climate change on global weather patterns, and the risks spiral even further.

Rick Cudworth, UK resilience and crisis management lead at Deloitte, says the increasingly global sourcing of components has the effect of obscuring supply chains. Collaboration by partners within chains, especially with potentially weak links, makes them stronger, he says.

“We’re seeing an expansion in global sourcing and more complex supply chains as companies strive to reduce cost. As production sites are increasingly located in regions more prone to natural disasters, the risk of supply disruption is rising,” says Mr Cudworth.

“Supply chain risk is climbing to the forefront of the agenda, but many organisations have concentrated on reducing cost in the supply chain without considering resilience. Recent examples of supply chain incidents have led to organisations receiving fines from the regulator for third-party failures.”

Executives and boards are under pressure to deliver day-to-day efficiencies in production and supply, and the temptation to ignore far-off threats must be significant. Yet a single obscure event can bring disruption, potentially reversing cost-cuts overnight.

All is not lost. Organisations with strong contingency plans, proper oversight, decent technology and an agile approach can curb the damage inflicted by natural disasters.

CASE STUDY: CATERPILLAR

Caterpillar

In March 2011, a huge earthquake triggered a devastating tsunami off the northern coast of Japan. Tom France, the director in charge of work vehicle manufacturer Caterpillar’s supply chain, was in Singapore. Caterpillar has two plants in Japan. Mr France and his fellow executives acted quickly.

“We identified where our containers were and their status, as well as whether they were shipped. Our products had either been shipped or were undamaged and ready to go. We needed to get them diverted to a different port and move them quickly,” he says.

The company’s chief concern was whether its factories in Japan had enough fuel following the earthquake. It prepared to fly in fuel shipments if necessary.

The year before, when the Icelandic ash cloud caused major disruption to transport networks, Caterpillar’s responded. The company determined which parts in the flight backlog needed to fly first and which could be delayed until after the ash had settled. Then it booked the earliest available air cargo capacity out of Europe.

“We were the first ones to lock down 747 charters,” says Mr France. “While others were sitting at their whiteboards, we knew before the ash cloud lifted what we needed to do. We protected our supply chain.”

Industrial unrest in various parts of the world has also tested Caterpillar’s supply chain resilience. When a strike in Italy caused ports to seize up, the business was able to assess shipments of parts ready to leave its Italian factory and whether others were stuck on route or in the port.

According to Tobias Larsson, head of the resilience team at DHL, it all starts with a complete picture of who you are dealing with.

“First, make sure you have the full visibility you need of your supply chain; you cannot protect what you cannot see. Second, understand where the critical hotspots are and how they might affect your supply chain,” he says.

“Use this understanding to assess the risk. Ask yourself where your supply chain is most vulnerable to a natural disaster. Consider your and your peers’ previous experiences; are your factories based near flood zones or are storage facilities along fault lines?

> An unexpected event disrupting one part of the machine can bring the whole thing grinding to a tuneless halt

“By assessing potential impact from disruptions and subsequently creating a detailed contingency plan, you will mitigate risks, receive early warnings and create awareness around the risks affecting the supply chain. This can ultimately help you to devise ways to protect the bottom line.”

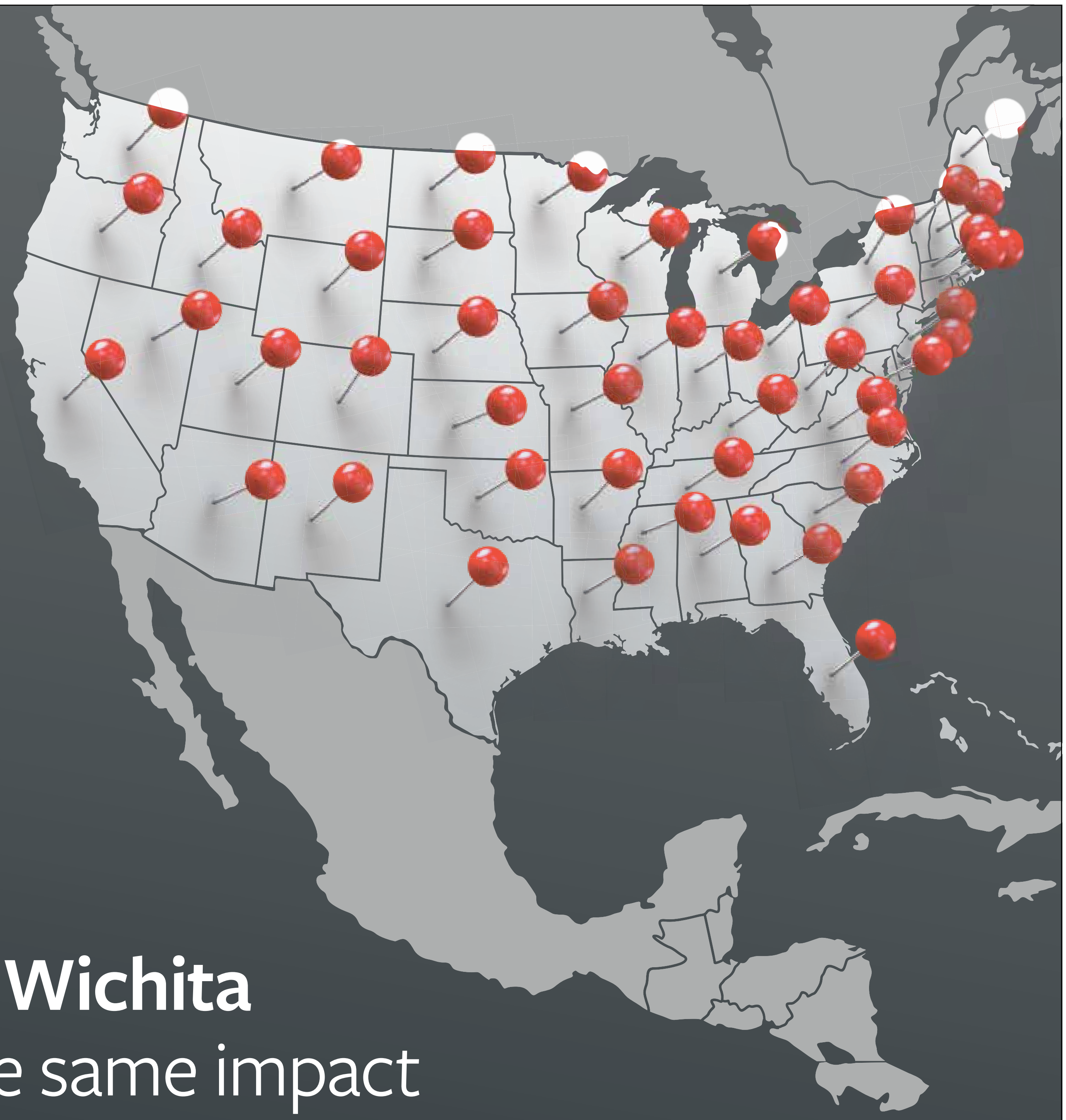
Systems that alert you to goings-on around the world are an essential ingredient of good contingency planning, Mr Cudworth agrees. “Establish early-warning intelligence through global monitoring tools so you can react quickly to unfolding events in real time and implement your contingency plans,” he says.

“Build a coherent crisis response plan that covers all the third parties that make your supply chain happen and conduct crisis simulations to identify potential gaps.”

Meanwhile Razat Gaurav, at supply chain experts JDA, believes a comprehensive package of technology coupled with open communications channels and good relations across the supply chain is the best way to mitigate potential disruption.

He says: “Investments in modern equipment, software and processes are mature steps to prepare a supply chain for an incident. So is going the extra mile and identifying alternate arrangements with suppliers, secondary facilities and occasional workload shifts as part of a disaster recovery exercise.”

Share this article online via **Raconteur.net**



A tornado in Wichita won’t have the same impact as a hurricane in Tampa

Growing your US Business? We’ve got you covered

For UK businesses looking to grow their operations across the Atlantic, US corporate insurance presents a complex challenge.

With unexpected risks and requirements changing dramatically from state to state, it’s good to know we’ve got you covered. Find out how our specialist coast-to-coast expertise and proven experience can help.

Visit travelers.co.uk/corporate to download our FREE RISK WHITE PAPER

Call us on 020 3207 6275

Or come and see us at AIRMIC Stand 109

Pinpointing US risks and helping you overcome them

- Highly complex market
- State-by-state variations
- Highly litigious environment
- Unfamiliar regulations
- Extreme natural disasters

TRAVELERS

travelers.co.uk

Travelers Insurance Company Limited. 5th Floor, Exchequer Court, 33 St. Mary Axe, London, EC3A 8AG. Travelers Insurance Company Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registered office: Exchequer Court, 33 St. Mary Axe, London EC3A 8AG. Registered in England 1034343.