Independent publication by RACONTEUR
raconteur.net / # 0320 / 11 / 06 / 2015

BUSINESS RISK STRATEGIES

FullProof
INTELLIGENCE
It's Second Nature

WE SELL AMMUNITION.

KNOWLEDGE ISN'T POWER, POWER IS HOW YOU USE THE KNOWLEDGE

Known for his outside of the box thinking, FullProof CEO, Mark Hill-Wood recently stated in a speech to Corporate Directors and Bankers:

> "As private intelligence specialists, we have access to funding from high-profile clients who respect the need to invest in encryption and other technologies necessary to stay ahead of the latest advancements in data hacking."

FULLPROOF CYBER DELIVERS VALUE TO YOUR ORGANISATION. THERE ARE 5 STEPS TO A MORE SECURE ENVIRONMENT:

IDENTITY

To identify the unknowns, in whatever form they may take. This may include: Data Leakage, Meta Data, Internet Inter-Orb Protocol related exposures or other reliance external services.

ACQUIRE

Upon identification of the object of the FullProof Cyber Footprint Service, the next phase is to acquire and gather all information in the most appropriate format to the investigative inquiry.

ANALYSE

One of the most critical phases is analysis, mapping and cross referencing what has been identified and acquired in order to ascertain the level of exposure it hosts, and its potential value to an attacker.

FORENSIC SECURITY (ForSec)

There are occasions in which the identified, acquired and analysed object may offer further information, internal to its body. In these instances, FullProof Cyber will apply its unique ForSec processes to look deeper into the object in order to further identify and retrieve other hidden sources of information and intelligence.

INTELLIGENCE REPORTING

The fifth element of the service is to supply an easy to understand report that maps the outcome of the activity and to provide observations, conclusions and recommendations

CONTACT US TODAY

+44 (0) 203 733 8105

fullproofcyber.com

fullproofintelligence.com

Getty images

Time to take the lead on managing risk

In a fast-moving and competitive environment, businesses must be prepared to take far-reaching steps to identify and deal with risk

◆ OVERVIEW

● ANTHONY HILTON

It is 31 years since the FTSE 100 stock market index was launched as part of the preparations in the City of London for the deregulation which became known as Big Bang. It comprised the biggest stock market companies of the day. Today only about ten of the original 100 survive. Bankruptcy, takeovers and growing irrelevance have taken care of the others.

There is a similar pattern in the United States. According to Yale Professor Richard Foster in the 1920s, the average age of the companies in its main index, the S & P 500, was 67 years. By 2012 the average age had shrunk to just 15 years. Now it is even less.

It seems clear that public companies don't survive and prosper like they used to. Modern business life does not allow them to.

Technology has changed how businesses compete. Even traditional firms are dependent on modern technology for design, innovation and marketing, and this makes them vulnerable to the scourge of cyber crime.

People risk is a similar though a less modern phenomenon. The real value of the business is often lodged in soft skills more than traditional production processes. But because these skills are knowledge based and people oriented they are much harder to patent, to keep secret or control. People move jobs and the business's competitive edge goes with them.

Then there is the pace at which things happen and the speed with which management is expected to react. Social media demonstrates every day how the world has moved on, but many businesses are still stuck in their silos.

Risk control systems in business almost entirely follow the pattern of traditional hierarchies in their approach to potential problems and their reporting lines. For good measure they are rooted in middle management. It follows, therefore, that the changes in business structure precipitated by the arrival of social media are going to require a fundamentally different approach.

Any command-and-control hierarchy struggles to respond fast enough. This is even more the case because so many of today's challenges are social-media driven and reputational; witness the recent problems of Thomas Cook and the Corfu holiday gas death case. Risk management is usually numbers driven, prone to box ticking, and often out of its depth when it seeks to identify and deal with softer intangible risks, supply chain weaknesses and reputation.

> Social media demonstrates every day how the world has moved on, but many businesses are still stuck in their silos

Share this article on raconteur.net

Business structures are also a problem. Businesses organised in silos can be poor at cross fertilisation. Threats and risks are reported upwards, but they are seldom reported across. Similarly risk control specialists are trained to look downwards and sideways, seldom to look over a wall and never to look up.

Up matters because there is a lot of people risk in the upper echelons of business. Directors under pressure may be as prone to rogue behaviour as employees further down the pecking order, but they are too far up the food chain to be tackled by those in charge of monitoring risk who suspect, often correctly, that they will simply be fired for their candour.

There is probably more money being spent on risk management than ever before, but things still keep going wrong. So you either believe that the modern organisation is so vast, fast moving, interdependent and complex no one can have any real idea what is going on in detail across the whole group – what you might call the HSBC defence. Or instead you think that a lot of money spent on risk management is wasted partly because it is not organised in the right way.

Airmic, the UK association for risk and insurance management professionals, and the think-tank Tomorrow's Company take the latter view and recently called for firms to appoint a senior executive to take on responsibility for risk leadership. It will be his or her job, with or without a team, to go anywhere in the organisation, to assess cultures and to understand how performance is achieved. They will know no boundaries.

If the business model, the culture and the results are out of alignment, this leader should say so; their internal and external sources should alert them to problems which have not yet shown up in the numbers. They must avoid being trapped in a silo of their own and see instead how events in one silo could destabilise another. And it would be for them to report to the board if they thought the chief executive was pushing too hard and forcing people to cut too many corners.

We cannot tell at this stage how many companies will be prepared to take such far-reaching steps or how many will find an executive willing to take such a job. But companies that refuse to think along these lines are themselves taking a big risk.

RACONTEUR

Distributed in THE TIMES

In partnership with airmic

Publishing Manager **Richard Sexton**

Commissioning Editor **Anthony Hilton**

Managing Editor **Peter Archer**

Head of Production **Natalia Rosek**

Digital and Social **Rebecca McCormick**

Design **Alessandro Caire** **Vjay Lad**

CONTRIBUTORS

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

ALEC MARSH Writer and award-winning editor, he contributes to *The Daily Telegraph, The Guardian, Daily Mail* and *The Spectator*.

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* magazine.

GIDEON SPANIER Journalist and commentator on business and the media, he is chairman of the Broadcasting Press Guild.

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

Straining the links in the supply chain

Even the simplest product may be made up of parts from the other side of the world, introducing significant business risk if the supply chain is interrupted

◆ SUPPLY CHAIN

● DAN MATTHEWS

With globalisation, supply chains have become elongated and at the same time diffuse. Opportunities for cheap manufacture in far-away places, along with new consumer markets in developing countries, have warped sourcing, production and distribution processes, pulling them in different directions around the world.

Even simple products sold by small businesses could have supply chains that disappear into the distance, fanning out in a complex web. These businesses, proud of their own commitment to consistent and ethical practices, can only know what their immediate suppliers are doing. But what about the secondary suppliers and their suppliers?

Before long the chain becomes opaque, like a mafia paper trail. It poses all kinds of potential issues for the businesses at the end of all those links, who risk operational disruption, reputational ignominy and financial ruin because of the chaos theory governing how items arrive at their door.

"Companies are facing an increasingly wide range of challenges to their supply chains, from human rights issues to natural disasters," says Mike Bailey at BSI, the UK's standards body. "Such complexity creates black holes of risk for organisations, both affecting the bottom line and a company's hard-earned reputation."

> Businesses risk operational disruption, reputational ignominy and financial ruin because of the chaos theory governing how items arrive at their door

BSI figures reveal that more than $300 billion (£197 billion) is lost to business each year because of disruption in the supply chain, with $30 billion lost due to natural disasters and $23 billion leaking out in the form of stolen cargo.

Counterfeit goods can make their way into the supply chain, as can unexpected ingredients such as horse meat in "beef" burgers. Meanwhile, criminals can also get in on the act by interfering with supply chain software and data, as well as more prosaically by secreting contraband in legitimate cargo.

According to Dominic Wong, head of supply risk mitigation at Deloitte UK, part of the problem stems from a rush of businesses hoping to save money by sourcing and manufacturing in developing parts of the world. This decision, he says, has back-fired in some cases.

"We have seen many suppliers set up operations in lower-cost economies, without a proper understanding of how to do business in that jurisdiction. As a result, project savings from labour rates have been eroded in inefficiency and poor control. In extreme circumstances, some have had to simply walk away from their purpose-built facilities," he says.

Risks in this area are many and various. Some are easier to control than others. Picking an accredited supplier, who is signed up to international covenants dictating best practice, for example, is a lot simpler than predicting an earthquake.

Andy Birtwistle, director of supply chain practice at Concentra, points to a long list of potential pitfalls that his business's supply chain software is designed to counteract. These are split into two groups – controllable risks that businesses can avoid, and uncontrollable risks they have to account for and deal with when they happen.

The first group includes falling quality levels, loss in transit, longer lead times, cyber security lapses, fake goods and problems associated with various countries' customs and border controls. The second list includes terrorism, natural disasters, economic and political change, and currency swings.

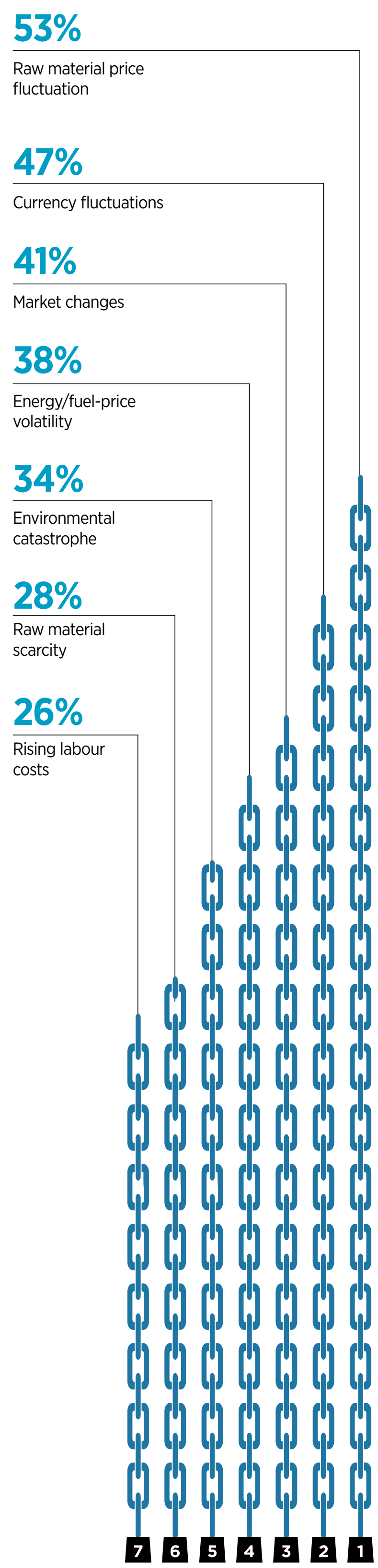
Dr Toby Waine, a lecturer in applied remote sensing at the Cranfield Institute of Soil and Agrifood, puts the second group in perspective. "The international vanilla supply – a very small-scale, specialist crop for farmers – was severely affected by weather in India and Mexico in 2012," he says. "The result was steep price rises and scarcity in 2013. It also meant a great deal of dependence on the Madagascan crop – a country beset by political instability.

"Another example is in the shortage of palm oil, which has been a recurring political issue in Thailand, as a staple in household cooking. The government resorted to importing palm oil from neighbours in 2011 to ease the crisis."

As Professor Clare Brindley at Nottingham Business School points out, there are many more examples besides, including a fire at a Nokia component supplier in South Africa, the Arab Spring's impact on bicycle part supplies to Halfords and finger-pointing at various fashion houses after factory blazes in Pakistan cost the lives of 260 workers.

The answer, says Mr Birtwistle, is multi-faceted. It includes selecting reputable

GREATEST BUSINESS RISKS IN THE SUPPLY CHAIN



Source: PwC/MIT Forum for Supply Chain Innovation

BLACK FRIDAY

Getty images

Born in America, Black Friday is just getting started in the UK. Yet the counter-intuitive "tradition" of slashing prices for a 24-hour period right at the beginning of retail's busiest season, at Christmas time, is already a phenomenon.

Assuming retailers won't be able to plug this particularly uncouth genie back into its bottle, they now have to factor the monstrous occasion and all its many ramifications into business plans.

It is awkward for retail bosses for a number of reasons, not least because they have to try and restoke demand for full-price products if they want to make any money at Christmas, but also because it has an explosive impact on supply chains.

Kurt Cavano, founder and chief strategy officer of GT Nexus, explains: "With retailers and manufacturers working way in advance to predict sales volumes, often forecasting on the success of a product that is going to be the 'in' thing that year, seasonal demand places a considerable strain on the effectiveness of the global supply chain network.

"However, this planning can only take companies so far. In this modern day, predilection to 'fast fashion', coupled with the quick turnaround of product lines, ensuring companies are able to adapt to demand and circumstance in an instant is key. In order to cope and to thrive in such an environment, a transparent, nimble and collaborative supply chain is essential.

"Black Friday is a momentous event and puts enormous stress on the supply chain network each year. Having started in the United States, it is an occasion that is only growing in popularity in the UK. And, while some retailers have won, reaping the many rewards of this shopping bonanza, others have lost out.

"Lacking the essential back-end capabilities to keep pace with demand and fulfil the orders flooding in, their performance has suffered and so too has their reputation.

"It's also worth noting that many forward-looking retailers are already predicting a large proportion of future sales will be primarily promotions-driven and this will have a marked, knock-on effect on the robustness of the supply chain."

'GREEN' UNILEVER

Global business titan Unilever owns some of the world's most cherished cosmetic and food brands, including Dove, Hellmann's and Lipton. The business has a stated commitment to "decouple growth from our environmental impact" – easier said than done for a business with such a reach.

Unilever introduced its responsible sourcing policy in 2014 – a reboot of a code launched four years earlier – with the aim to improve life for workers across the supply chain, as well as their communities and local environment.

The top level goal is to halve the business's environmental footprint by 2020 while at the same time doubling the size of its business. The plan was concocted with advice from a range of leading organisations, including charities and non-governmental organisations.

Since 2007 it has been sourcing most of its products and materials from their origin, rather than through middle men, to increase transparency. In doing so it removed millions of pounds in cost and increased yields for farmers.

Sustainable supply is also an important part of Unilever's business plan, particularly because a shortage of raw materials could put pressure on large corporates in future. By last year, it was purchasing 55 per cent of agricultural raw materials from sustainable sources.

An example is its sustainable tomato sourcing in India. Hindustan Unilever used to rely on imported tomatoes from China, but inconsistent quality and price volatility lead to a switch in 2010 to local sourcing through Varun Agro, a business working with 2,500 small-scale farmers.

The farmers are required to meet Hindustan Unilever's quality and sustainability requirements, including cutting the use of water, pesticides and fertilisers. In return they receive training on good agricultural practices from Varun.

Under the contract, the farmers can sell 25 per cent of their produce on the local market, giving them a secondary source of income and providing access to higher prices should the market move in that direction.

As a result, the farmers have seen yields more than double, the quality of the crops has improved dramatically and the businesses have benefitted from the security of a guaranteed buyer.

Getty images

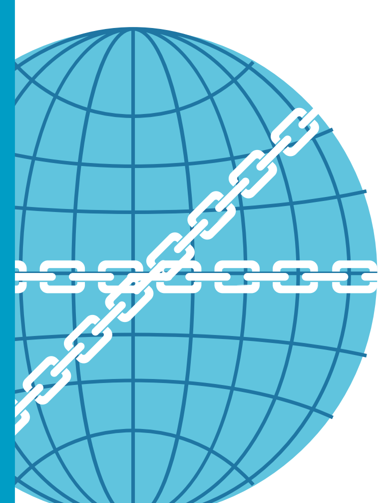
suppliers with a strong moral compass, choosing globally capable logistics partners, and appointing managers to oversee tasks and processes at every link along the chain.

For uncontrollable risks his advice is to implement a robust event alert and management system, reshoring production away from troubled zones, getting adequate insurance, and accurately modelling the impact and cost of possible events.

"Data analytics can model event likelihoods and impacts, removing human bias, to provide a realistic assessment of supply chain risks," he says. "Presenting the right information in the right format to the right people is the first step to making informed supply chain decisions.

"With access to this data, managers can understand the risks and take action. Data and analytics will bring back visibility and control of the supply chain that were lost due to globalisation. These systems can be used to support improvements in ongoing supply chain processes."

Tim Lux, a partner at advisory business Pathfinders, says when in doubt look for official standards. "A good starting point is the European Union's Authorised Economic Operator scheme. Other similar schemes are springing up around the world, offering mutual recognition benefits. The safety and security accreditation provides a good framework to build a safety-conscious culture within a company," he concludes.



Out of sight and out of mind?

Intangible business assets, such as key personnel and brand value, along with damage from cyber attacks, are difficult to quantify – and are strikingly underinsured by risk managers

◆ **INTANGIBLES**

● CHARLES ORTON-JONES

As the French romantic saying puts it, far from the eyes is far from the heart. Intangibles are all the things in a business which can't be seen and, when it comes to risk management, that means they are often overlooked.

Most businesses simply don't protect intangibles. According to new research by Clydesdale Bank and Yorkshire Bank, only one in four (27 per cent) of UK small and medium-sized firms has taken steps to value non-physical assets. It's not much better at larger firms. Government figures state only 2 per cent of big enterprises have cyber insurance, despite 80 per cent being breached in the last year. Accountancy body CIMA calls intangibles "a collective blind spot for decision makers".

So what intangibles should businesses be looking to protect? The list includes key personnel, brand value, intellectual property, cyber security, supply chain and third-party behaviour. Each category needs a risk mitigation policy in place. And, if there is a serious chance of disruption, insurance should be acquired to offset the damage when disaster strikes.

Official guidelines imply it is straightforward to calculate the value of intangibles. CIMA published a guide in late-2014 on reporting intangibles as part of global management accounting principles. But talk to insurance industry chiefs and it is clear there are grey areas.

> **"** Key people insurance is riven with disputes over how to calculate a value and what cover should protect

Take brand reputation. Valuing a brand is a common exercise. Agencies such as Millward Brown, Brand Finance and Interbrand perform brand valuations for purposes including mergers and acquisitions, insurance and credit guarantees. They use methods outlined in standards set in ISO 10668. There are seven methods cited in the ISO. For example, the "price and volume premium" method uses comparisons with generics. Nurofen painkillers are pure ibuprofen, but command triple the price over generic alternatives due to strong branding.

Yet there are two shortcomings no matter which methodology is used. First, rival agencies frequently produce divergent valuations. Millward Brown and Interbrand rate Apple's brand with a variance of up to $100 billion. Second, the impact of specific events on a brand is extremely hard to quantify using the ISO-approved system.

David Philip, partner at Kennedys law firm, points out: "It is possible to insure a brand against detriment, although placing a value on intangibles is extremely difficult as they are so subjective." Garry Sidaway, of risk management consultancy NTT Com Security, agrees, adding there are numerous complicating factors: "You can protect yourself to some degree from individual social comments and remarks, but insurance is based on actuarial data and loss, and brand value is a very difficult thing to measure effectively. The impact on market value is one measure, but again what am I insuring, how do I determine the necessary cover, and what controls must I put in place to protect my own interests?"

The solution? Insurance companies are increasingly offering more than cash payments to cover loss. Packages include consulting services in the event of a loss, such as help with public relations in the case of a product recall. Practical help, rather than a hand-out, may be of far greater value, when payment terms would be so hard to agree on.

64%

of the total value of UK firms is in intangibles

Source: Brand Finance/CIMA

50%

of companies cite brand risk as their top risk concern

Source: Aon Risk Solutions

Key people insurance suffers from similar difficulties. The category is riven with disputes over how to calculate a value and what cover should protect.

Ben Butler, director at insurance broker Macbeth, advises on key person valuations. He says the broad aim is to maintain a company's profits or turnover in case of the loss of a key person. "These can range from loss of goodwill or technical skills and knowledge, through to financial arrangements or potential expansion opportunities or business projects," Mr Butler says.

Methods of calculating risk vary. "Multiple of salary, cash flow and multiple of profits are all common methods," he explains. "None of these are perfect. For example, an individual's salary may not be a true reflection of their actual involvement. But, in establishing a plan, the very process of financial underwriting will assess the level of cover necessary."

These challenges mean key person insurance is gravely underused. Chris Hickey of broker Sutton Winson remarks that "very few people have heard of this type of cover". Which is troubling. A Legal & General survey shows 41 per cent of business owners expect their business to fold within 18 months following the death or critical illness of a key person. Six out of ten rated the loss of a key person as the worst disaster their firm could experience. Even a basic key person policy can avert catastrophe.

The biggest growth area in intangibles is cyber insurance. Lloyds of London reported a 50 per cent increase in submissions in the first three months of this year compared to 2014. First-time purchasers account for 70 per cent of Lloyds' customers. Globally, IBISWorld research reports premiums growing from $400 million in 2009 to $2 billion this year and estimates $10 billion in five years.

Yet the mood from the cyber defence sector is one of incredulity that more isn't being done. John Watters, chief executive of cyber security consultancy iSIGHT Partners, says paranoia ought to be standard: "If you're an investment firm, focused on global investing, you don't think sovereign funds want to know what your strategy and target list is? If you're an investment banking firm specialising in M&A, you don't think criminals want to gain insight into your M&A pipeline?"

Attacks are hardly rare. As Mr Watters says: "We can assume the data we have almost certainly understates the problem due to under-reporting."

The sector is trying to lure more businesses into taking out cover by diversifying policies. Some new contracts include reimbursement for reputation and PR damage caused by a cyber attack. This is a welcome development, when you consider the press frenzy following the high-profile breaches at US retailer Target and Sony Entertainment.

To promote coverage, the insurance industry needs to assure clients that threats can be quantified and explain clearly what a policy will cover.

Tim Ryan, executive chairman of the independent broker alliance UNA, stresses his colleagues have work to do. "Finding solutions to insuring intangible risks presents an opportunity for the insurance industry as traditional policies just won't cut it in these instances. This is where the insurance sector is set to evolve in order to plug the gaps," he says.

Until it completes the transformation, intangibles will remain the Achilles' heel in risk management. Both insurers and companies have a duty to change this.

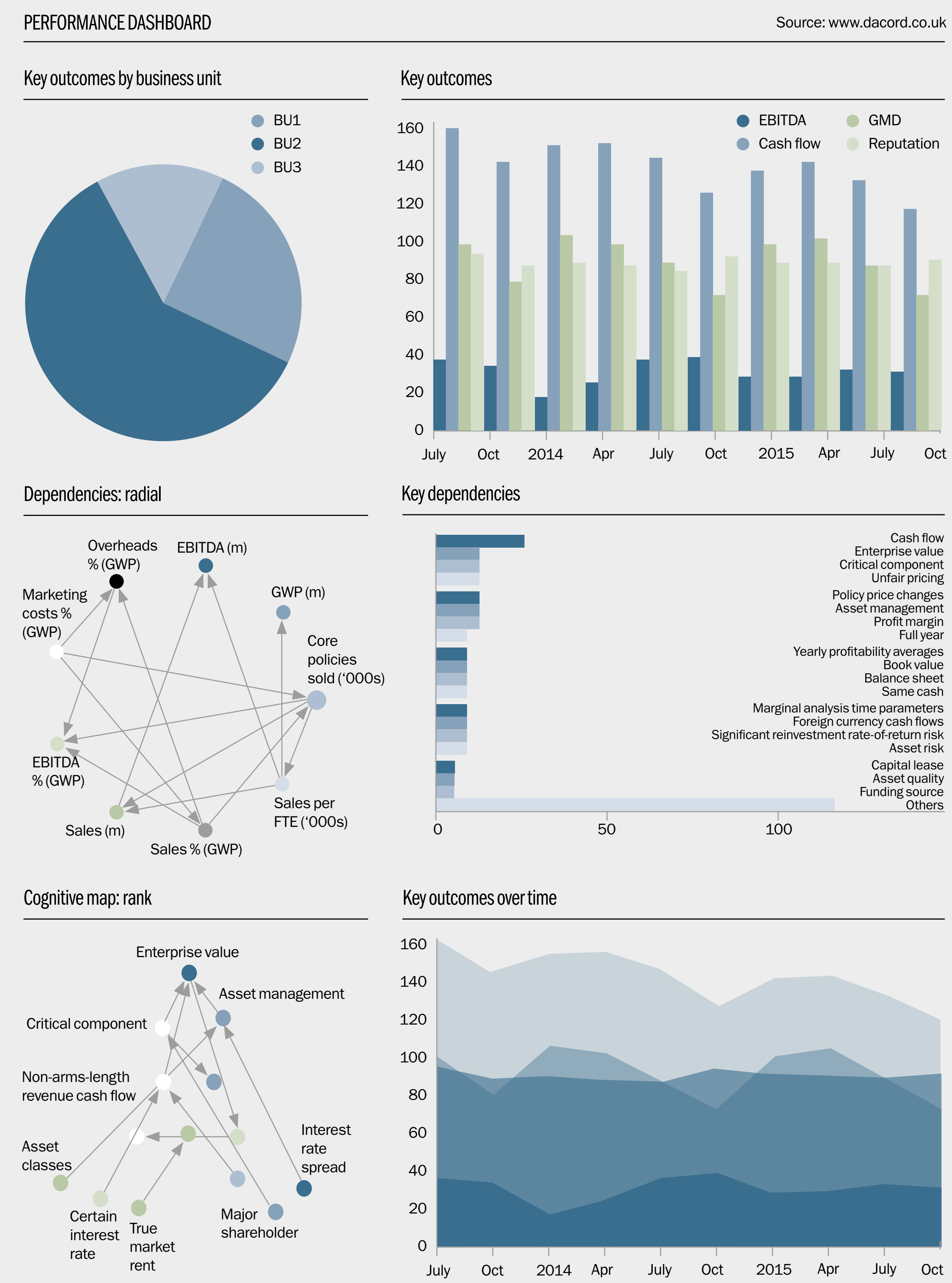
Share this article or infographic on social media **via raconteur.net**

COMMERCIAL FEATURE

WHY RISK MANAGEMENT MUST BE AGILE

What is risk management all about? Is it simply about avoiding things that threaten you? Or is it something deeper – how you think about business performance?

Neil Cantle
Principal



There is much more to modern risk management than simply saying "no" to things. Risk management activity has to be about everyone helping to achieve company goals.

Businesses now require a much broader understanding of how things and people interact, and how those interactions lead to different outcomes for business goals. The sheer complexity of modern life means it is no longer sufficient to consider "chains" of events, whereby sequences of factors might lead to adverse outcomes and try to intervene in that chain to preserve success. So-called "causes" are simply not that linear or visible any more.

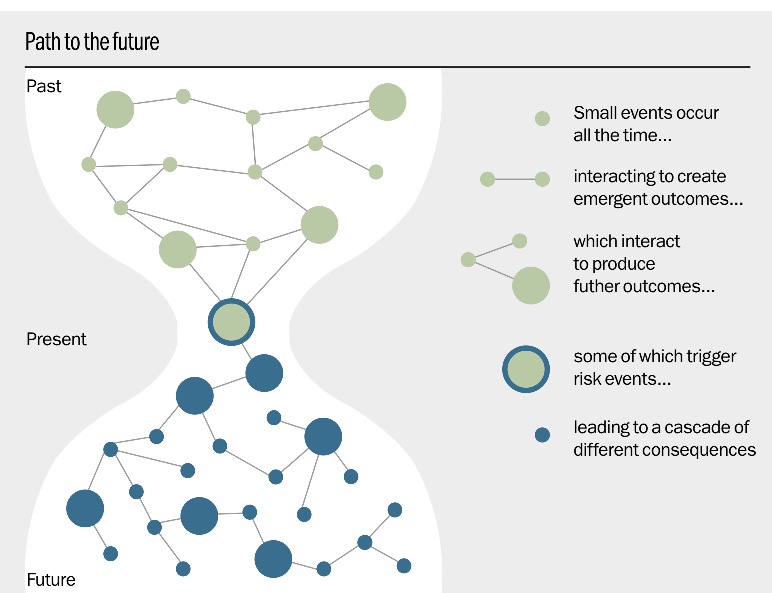
Indeed it is not even productive to think of risks arising simply by people "doing wrong". Many catastrophic failures arise despite people trying to "do the right thing" under difficult circumstances that were not covered by the governance manual. No. The uncertainties affecting modern business are much more about a complex network of factors that act in sometimes mysterious unseen ways to influence your business destiny, as illustrated in the graphic below. Risk management's job is therefore to lay out these unfolding patterns and to ensure that discussion takes place about how they should be taken into account.

Risk, by definition, lies in the future so we need to anticipate the ways in which current trends might unfold. Many risk assessment frameworks assume too much about the degree to which we "know" where we are and therefore build upon false foundations to make spuriously accurate statements about the future. However, by being honest about what we do and don't know, it turns out that with the right perspective, we can start to make some real sense of where we are, how we got here and what might happen next.

This is important. In a world of complexity, we have to get back to the business of making sense of things rather than pretending we can control everything. This requires an evolution of enterprise risk management into a new form – this is Agile Risk Management™.

Agile Risk Management embraces the complexity of modern business and offers a more useful path to organising business activity in such a way that goals are delivered within the board's appetite for risk. Recognising that "controlling" complexity means bringing visibility of enterprise context to managers who deal locally with risk and uncertainty is crucial. It is a proven fact that central command-and-control structures cannot efficiently guide complex dynamic outcomes as efficiently as a decentralised, but well-informed, approach can.

Aligning the organisation around clear outcomes means that local "best endeavours" accumulate to provide better overall outcomes. And accepting that some things cannot be known ensures people remain sceptical, alert and flexible, rather than stuck in a rut reporting the same old indicators each week. In this way companies become resilient to changing circumstances rather than paranoid about risk. In a world where the best of intentions can still lead to risk, such resilience is essential.



Developed alongside Telos Solutions, as experts in advising boards and chief executives, Agile Risk Management explicitly addresses the need for "risk" activity to be rooted in terms of business performance. The focus must be on things that matter to success and aligning the whole organisation around that goal. This also requires acceptance that risk management is about more than "oversight", and is actually about building common narrative around uncertainty and recognising solutions require an understanding of the cultures within the organisation.

Agile Risk Management embraces the fact that companies are made of people. Cultural assessment techniques developed in conjunction with Dr Hilary Lewis of Systemic Consult provide important insights into how people carry out key activity in the business. This knowledge helps to ensure all perspectives are heard and the intended outcomes actually happen, not just that the processes written in the policy documents are acted out.

> "The focus must be on things that matter to success and aligning the whole organisation around that goal

So how do you manage the performance of business in an agile way? The answer is by providing managers with insight. Insight into what is going on and what might happen next. This insight must lay out a clear picture of the interacting factors that are driving outcomes right now. To do this we need to determine where we are now, the path we followed to get here from the last time period and a falsifiable claim about where we think we will be next time. With this we can start to spot patterns, learn about evolving dynamics in our business and get smarter at making improvements.

Unlike the classic static management information reports, dashboards like the one above illustrate how your knowledge and your data can be combined to provide a real-time dynamic view of business performance. Rather than simply looking at the typical array of indicators which may or may not tell you something about your targets, this multivariate approach reveals which collections of indicators really are driving performance at each time. Armed with this knowledge we can start to look ahead and forecast possible outcomes.

So risk management should no longer just be about "worry lists". Taking an agile approach focuses on business outcomes – using decentralised, but universally informed, control and explicitly demanding cultural diversity to determine the best solutions. It is no longer possible to avoid risk, so the next evolution of risk must be agile and centred on delivering business performance through aligned local endeavours.

For more information please contact Neil Cantle, MA FIA MIoD CERA, principal, Milliman, neil.cantle@milliman.com

Geopolitical risks are still ris

Global business risk has never been greater as the world becomes evermore complex and interdependent amid regional turmoil

◆ **GLOBAL RISK**

● **ALEC MARSH**

We're at the crossroads for humanity. It could be our best century, but it could also be our worst because our capabilities of spreading risk are greater than ever before." That's the chilling conclusion of Professor Ian Goldin, director of Oxford University's Oxford Martin School, dedicated to the study of future sustainability.

Professor Goldin was closely involved in the creation of this year's World Economic Forum (WEF) *Global Risks* report, which for the first time listed interstate conflict in its top five list of risks in terms of likelihood. And not just that, it put it at number one.

"In the 25th year after the fall of the Berlin Wall, geopolitical risks are back on the agenda," the report warns. More worrying still, the panel of 900 worldwide business, governmental and academic leaders that the WEF surveyed in creating the report cited another unwelcome newcomer, water crises, followed by global pandemics and the consequences of failing to prepare for climate change as the leading risks by their likely level of impact.

"The nature of risk is changing,' says Professor Goldin, co-author of *The Butterfly Defect: How globalization creates systemic risks, and what to do about it*. "The walls have come down between societies. Something that happens on the other side of the world can quickly cascade and impact us. There's a growing complexity, a growing integration and it leads to a fundamentally different nature of risk. That's the butterfly defect, where small events elsewhere in the world will fundamentally affect our lives."

> There's a growing complexity, a growing integration and it leads to a fundamentally different nature of risk

Yes ladies and gentlemen, the four horseman of the apocalypse are now knocking at your firewall and can be at your doorstep inside 48 hours from anywhere in the world, carrying their antibiotic-immune infections, courtesy of global aviation connectivity.

If that wasn't bad enough, the economic risks we're all too familiar with haven't gone away either. Instead, they're being masked by the escalated threat from geopolitics and global diseases such as Ebola. "That creates a much more challenging cocktail for companies to deal with," says Richard Smith-Bingham, director of the Global Risk Centre at Marsh & McLennan Companies, an international risk management and insurance firm, which partnered with the WEF on the report.

What then can business leaders do in the face of such unremitting interconnected challenges? Well, as old soldiers know, time spent in reconnaissance is seldom wasted. First, if you have an international presence, supply chain or are investing overseas, you need to do your geopolitical due diligence.

So says Margareta Drzeniek-Hanouz, lead economist and head of the global competitiveness and risks team at the WEF. This will help tell you what might be coming your way, but it's only part of the answer. "Some of the risks you can only prepare for," she cautions. "Geopolitical risks are very difficult for the business community to mitigate."

EVOLVING RISKS CALENDAR

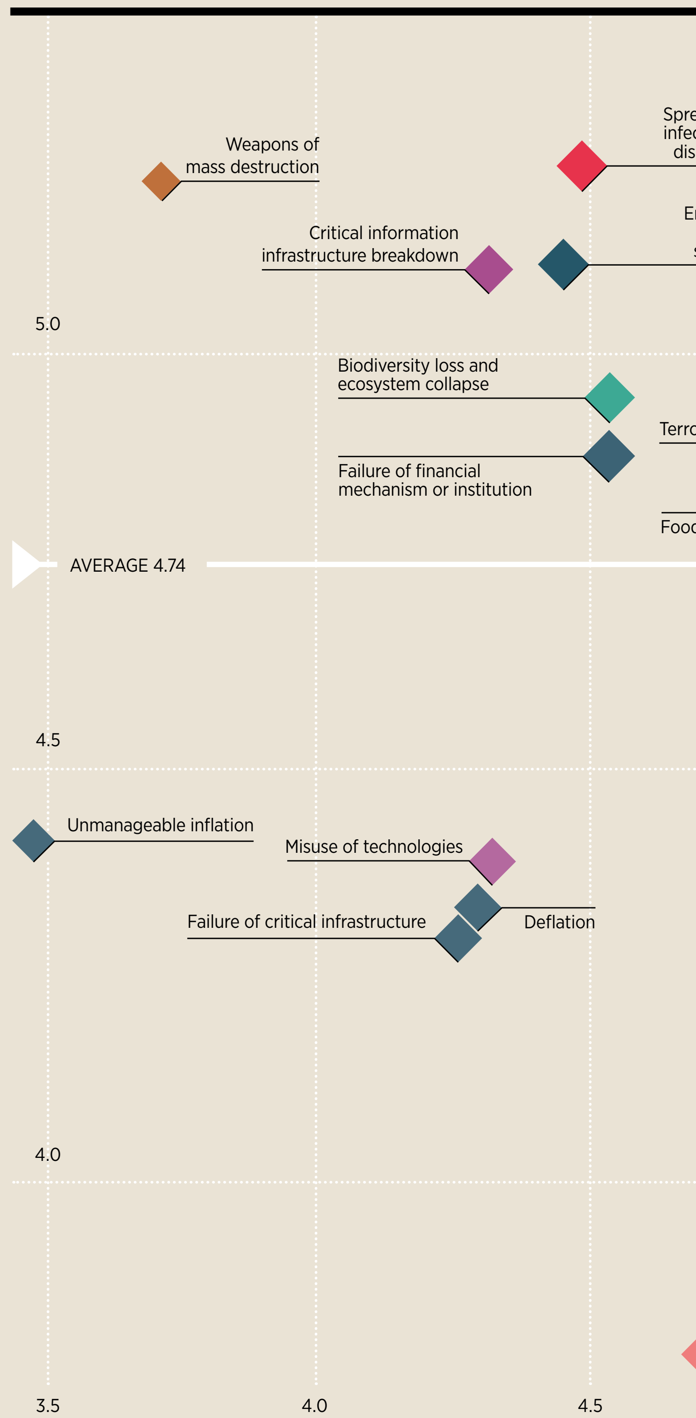
LIKELIHOOD

2012	2013	2014	2015
Severe income disparity	Severe income disparity	Income disparity	Interstate conict with regional consequences
Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events
Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment	Failure of national governance
Cyber attacks	Water supply crises	Climate change	State collapse or crisis
Water supply crises	Mismanagement of population ageing	Cyber attacks	High structural unemployment or underemployment

IMPACT

2012	2013	2014	2015
Major systemic financial failure	Major systemic financial failure	Fiscal crisis	Water crises
Water supply crises	Water supply crises	Climate change	Rapid and massive spread of infectious diseases
Food shortage crises	Chronic fiscal imbalances	Water crises	Weapons of mass destruction
Chronic fiscal imbalances	Diffusion of weapons of mass destruction	Unemployment and underemployment	Interstate conict with regional consequences
Extreme volatility in energy and agriculture prices	Failure of climate change adaptation	Critical information infrastructure breakdown	Failure of climate-change adaptation

GLOBAL RISKS L



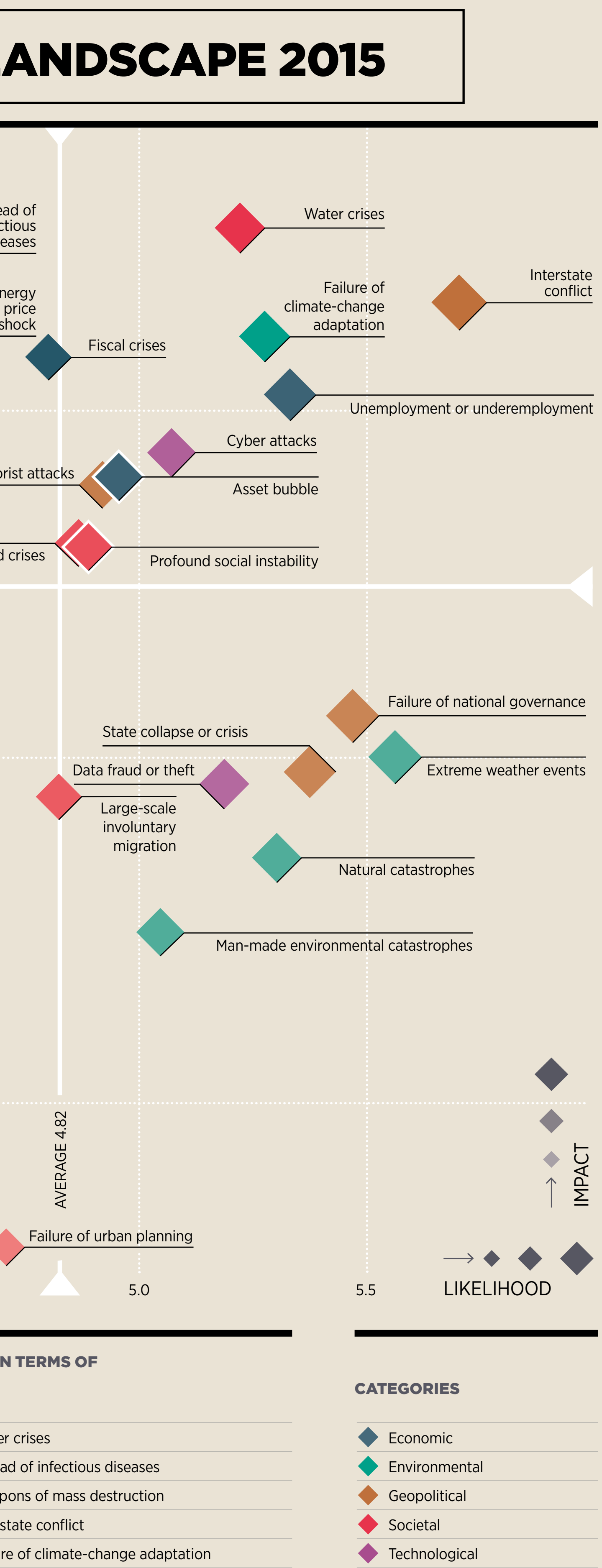
TOP 5 RISKS IN TERMS OF
LIKELIHOOD

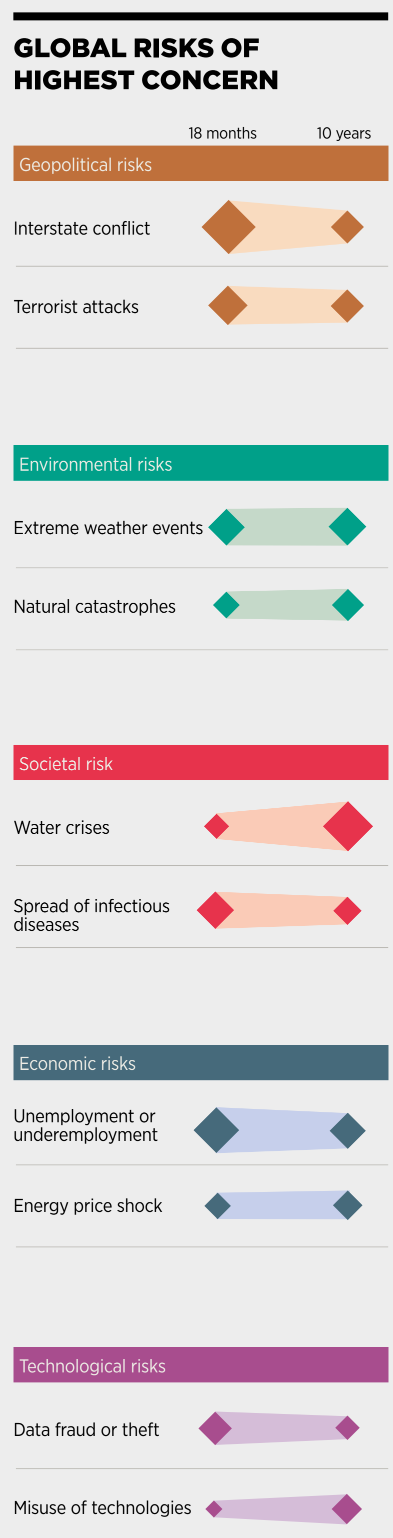
1. Interstate conflict
2. Extreme weather events
3. Failure of national governance
4. State collapse or crisis
5. Unemployment or underemployment

TOP 5 RISKS I
IMPACT

1. Wate
2. Spre
3. Wea
4. Inter
5. Failu

sing in an uncertain world





Source: *Global Risk 2015 report*, World Economic Forum

Since three of the top risks most likely to happen are geopolitical, something else needs to be done – without delay. Mr Smith-Bingham says: "Companies should really think about these endogenous risks in a more fulsome and diverse way." Don't just look at the headline macroeconomic indicators, he cautions, look at the underlying factors, such as social uncertainty, rising powers and economies, rapid technological advances and climate change. "They're the fundamental drivers of change in the world at the moment," he says.

Take these and build plausible scenarios assuming that one of them happens. Next, ask what would happen if a second event occurred at the same time. "It's about kicking the tyres against your own risk resilience to understand your own vulnerability," says Mr Smith-Bingham, pointing out that reputational risk is also ever present.

And if you don't like what you find, he adds: "You either need to protect your chosen strategy by building in more buffers or it's about changing your strategy, diversifying by geography or product, ensuring that you're not in areas that could actually blow up in your face."

> "Look at the underlying factors, such as social uncertainty, rising powers and economies, rapid technological advances and climate change – the fundamental drivers of change in the world

So how do you go about assessing global, regional, country or local risks? Government can help, both at home and through the overseas network of embassies, for instance. Then there are overseas governments themselves, which businesses should engage with.

Amy Gibbs, a senior consultant who analyses country risk at the UK insurer JLT, says her firm advises clients to take a holistic approach. "You can't really understand how the risk of terrorism is going to change in the future unless you are looking at political and economic circumstances as well," she says.

As a result she advises clients to engage national, local and even traditional power brokers in-country to build a picture of what's going on. Don't leave out opposition leaders either, since they could potentially tear up any agreements you have after the next election or coup. Ms Gibbs suggests pairing up with international bodies such as the World Bank's investment arm, the International Finance Corporation (IFC). They have expertise, plus: "If you are in dispute with your host government, having IFC involvement in a project can help with leverage," she says.

Finally, don't overlook non-governmental organisations (NGOs), which are not always the first port of call for business leaders. "NGOs have knowledge that very few other organisations will have," Ms Gibbs points out. "They understand the local nuances, where the risk environment is heading and are another source of information that corporates can use to build up a picture of risk."

If governments at all levels and NGOs can help grow your appreciation of the risk landscape at home and abroad, they can also help you begin to relandscape it, too. Up to a point, at least.

Take climate change, where corporates have been working with governments and the United Nations to come up with a strategy for the world, or the B20 gathering of global business leaders' organisations, which holds summits to advise the major G20 powers on policy initiatives.

Elsewhere, as Mr Smith-Bingham notes, his organisation has worked with the UK's Cabinet Office on ways to reduce the challenge of cyber crime. And in its 2015 *Global Risks* report, the WEF cites an example of a multi-stakeholder approach to modelling water flows in Australia's Murray-Darling Basin, which supplies drinking water for two million people. The model is crucial for providing credible data that can be used to manage this vital resource more sustainably. The WEF, says Dr Drzeniek-Hanouz, expects to see this sort of collaboration to increase exponentially.

"It's those corporates with the attitude that they can shape the risk environment they operate within that will typically do better," adds JLT's Ms Gibbs.

But if engagement is the key, there are challenges. A high barrier to effective strategic collaboration between corporates, government, and local and international bodies is trust. Mr Smith-Bingham says it's about having the right infrastructure, established relationships and safeguards in place so companies are comfortable about sharing their information, for instance on cyber crime events, for the greater good. "Governments and business can interact to ensure there is a more resilient business eco system," he says.

And Professor Goldin of Oxford Martin School agrees, though he sees it as being even more fundamental than that. "What we're seeing in the politics of the UK and many countries is people feeling very uncertain about the future and globalisation," he says. "For any corporate leader, this is very dangerous because there's a chance we might reverse the advantages of globalisation. Businesses must be more engaged not only in managing the risks, but in managing the understanding of society." And that goes for governments too.

No hiding place for companies in the age of social media

Safeguarding corporate reputation and brand value is now firmly on the boardroom agenda as executives must learn to be nimble in response to criticism and crises


Getty images

◆ **BRAND AND REPUTATION**

● GIDEON SPANIER

Companies often say staff are their most important asset, but brand and reputation are arguably more valuable.

A reputational crisis can wipe tens of millions of pounds from a company's value, and this risk has increased because the rise of online and social media means crises are now less predictable and can happen faster.

Lorna Tilbian, executive director at the investment bank Numis Securities, says: "Of course, risk is impossible to eliminate, but fail to identify and monitor it and you and your brand are dead."

Deloitte's annual survey of reputation risk found "reputation damage is the number-one risk concern for business executives around the world". Some 87 per cent of 300 senior figures surveyed said reputation risk was "more important or much more important than other strategic risks their companies are facing".

Reputational crises can be divided into four main risk areas, according to Deloitte. Issues of ethics and integrity, such as fraud and corruption, are arguably the most serious. It says a lot about the problems facing the banking industry that, seven years after the collapse of Lehman Brothers and the bailout of Royal Bank of Scotland and Lloyds Banking Group, trust remains so low because of interest rate and foreign exchange fixing, mis-selling and tax avoidance.

Security risks, both physical and cyber breaches, are a second area of concern. Sony has suffered at both a consumer level, when PlayStation customers' personal details were leaked, and at a corporate level, when its Hollywood executives' e-mails were hacked and embarrassing details published on the internet.

> "
> Reputation damage is the number-one risk concern for business executives around the world

Product and service risks around safety, health and the environment are a third issue. Recent examples include BP's 2010 oil spill in the Gulf of Mexico, and the 2013 scandal over Tesco and other supermarkets selling horse meat in beef and other meat products.

Third-party relationships also pose a risk because, in the words of Deloitte, companies are "increasingly being held accountable for the actions of their suppliers and vendors". The travel company Thomas Cook recently found itself embroiled in legal action over the death of two children who died of carbon monoxide poisoning in a Corfu hotel run by a third party. Even though the hotel admitted liability, Thomas Cook was criticised for failing to apologise or pay adequate compensation to the bereaved parents.

In many cases, the crisis became personal as the chief executive and other bosses were thrust into the spotlight, with online and social media feeding TV and newspaper coverage. Facebook users set up no fewer than nine campaigns on the site criticising Thomas Cook and calling for a boycott.

Little wonder that there is growing recognition in the boardroom that companies must improve their risk controls. Ms Tilbian says: "The majority of boards in financial services spend more time on risk, regulation, governance and compliance than they do on strategy."

Seven years after the banking meltdown, demand for candidates with experience in risk and compliance remains strong. "There may be up to ten jobs listed for one role from a single client," says Sholto Douglas-Home, group marketing director of Hays, the global recruitment firm.

Andrew Linger, a director of executive search at headhunters Robert Walters, says boards are not only more proactive, but also improving their internal controls. "Old style internal audit departments concerned with processes and controls would spot risks, but not necessarily quantify them," he says. "With this new approach, risk is examined in a detailed and quantifiable manner by far more sophisticated methods, and it has become a major focus for businesses and brands, and no longer just a back-room exercise."

Devising practical strategies to cope with a reputational crisis is still a challenge. As Deloitte puts it: "Companies are least confident when it comes to risks that are beyond their direct control."

Co-operating with regulators and government is within the corporate comfort zone. However, any apology needs to be sincere. Bob Diamond, the then chief executive of Barclays, memorably told MPs in 2011 that the time for "remorse" for banks should be over – a remark that came back to haunt him a year later when the libor-fixing scandal exploded.

Appearances matter. Tony Hayward, chief executive of BP during the Gulf of Mexico spill, found his British accent did nothing to endear him to angry Americans during the crisis. A senior, local BP official proved to be a better face for the company on US TV screens.

For companies facing a reputational crisis, handling Facebook, Twitter, YouTube and user-generated blogs is proving tougher.

Companies can appear paralysed by the speed of online media. When Barclays was plunged into crisis in 2012 over libor-fixing, the bank made little use of social media or its own website to apologise or explain its behaviour.

Being too open online has pitfalls. When BP set up a live video feed of the gushing leak in 2010, it illustrated how slow the company was being in stopping the flow of oil into the sea.

Now that boards have seen the growing power of social media, they are taking action. Deloitte found that more than half of companies "plan to address reputation risk by investing in technology such as analytical and brand monitoring tools". They are also doing more scenario-planning and devising crisis management plans.

Smart boards are beefing up their in-house public relations and social media-monitoring, and ensuring PR is part of the senior management team.

A clear chain of command, starting with the chief executive, is important because, when a crisis strikes, there is so much online "noise". Deloitte says: "Response times should be in minutes, not hours and days."

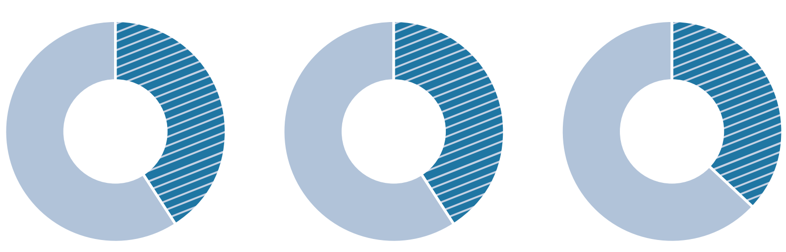
The danger about an increase in risk control is that it leads to a risk-averse mentality. America's anti-fraud Sarbanes-Oxley Act has forced companies to spend more on monitoring internal processes. But Mr Linger warns: "Some businesses, who have been strongly and commercially risk aware all along, may argue that Sarbanes-Oxley, and other similar approaches, actually send them back in time due to their 'box-ticking' approach which may actually divert from the important focus of commercial impact."

Jim Prior, chief executive of WPP's branding agencies The Partners and Lambie-Nairn, goes further. "Risk should not be confused with bad decision-making," Mr Prior argues. "For a business to do something that is clearly morally or legally wrong, such as selling horse meat or libor rate-fixing, has nothing to do with risk. That is just stupidity and, of course, when it gets found out, it will damage the brand and reputation, quite deservedly.

"Risk is important because for businesses to grow and evolve in line with the ever-changing demands of the market, they need to pursue new ideas and innovative approaches, without which they will stagnate and ultimately fail."

He cites Virgin, Apple, Google and Red Bull as brands that "demonstrate how taking risks leads to enhancement, not damage, to the brand".

RESPONDENTS WHO EXPERIENCED REPUTATIONAL DAMAGE SAY THE BIGGEST IMPACT WAS...



Source: Deloitte

87%

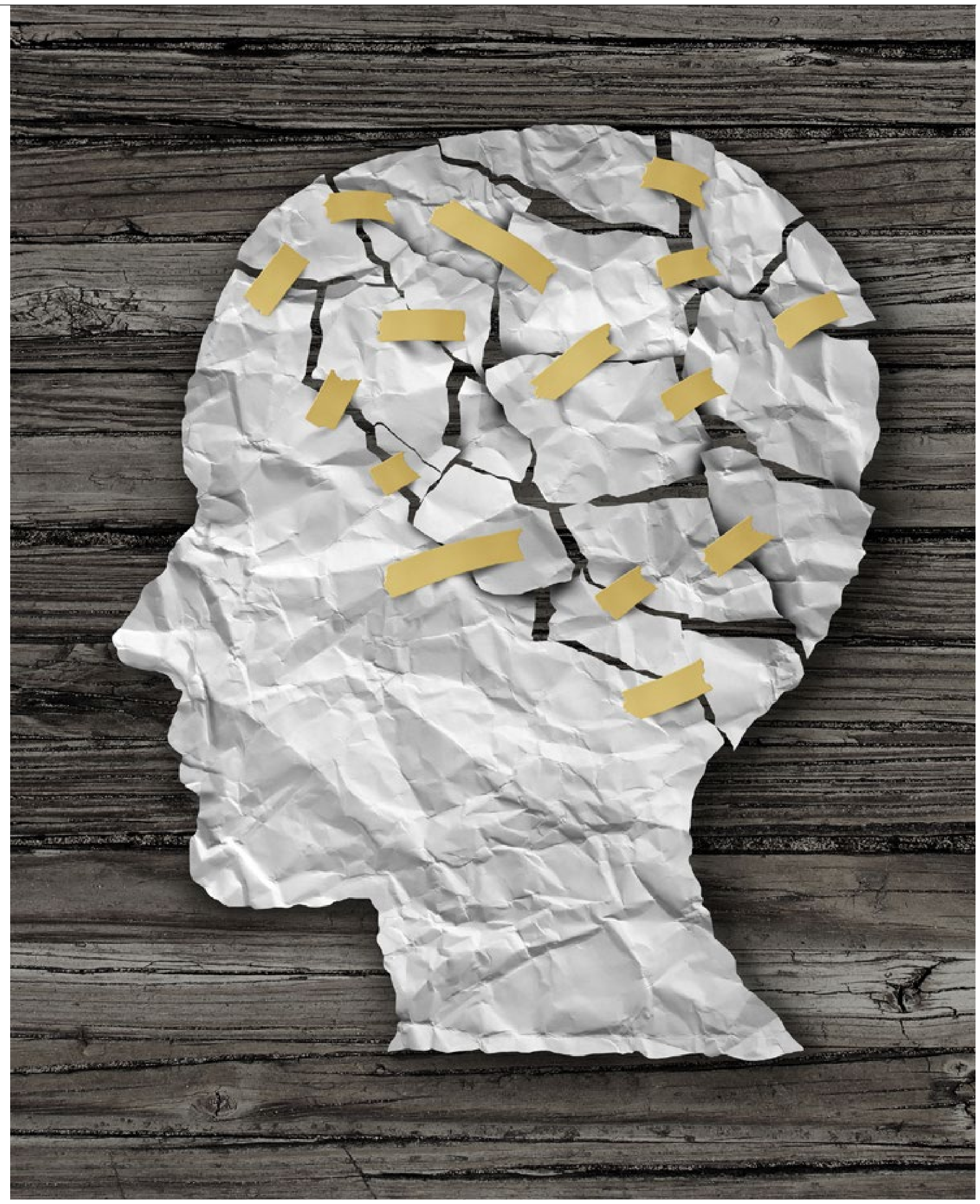
of executives rate reputation risk as more important or much more important than other strategic risks their companies are facing

50%+

of companies say they plan to address reputation risk by investing in technology such as analytical and brand-monitoring tools

Source: Deloitte

COMMERCIAL FEATURE



FACING UP TO MENTAL HEALTH

Mental health remains a taboo subject among many employers who fail to provide help for staff which could not only benefit the individual but also the company

Chris Rofe
Senior vice president of employee benefits

LOCKTON®

Enhancing employee benefits and involving multiple stakeholders in corporate purchasing and programme design could be key to reducing business risk arising from staff health issues, according to new research.

Members of the employee benefits team at global insurance broker Lockton began work on the project following a survey of business risks arising from mental health issues in the workplace.

This latest piece of research found that the traditional approach to buying employee benefits through human resources (HR) departments alone could be done better through a cross-departmental consensus involving HR, corporate risk, occupational health, finance and legal teams.

Chris Rofe, senior vice president of employee benefits at Lockton, explains: "Risk managers view life differently, so you could mitigate exposure for employer's liability claims and potentially reduce the number of employee disputes and tribunals. There might also be a knock-on effect to the cost of health and safety liabilities.

"Because all of these services have traditionally been bought in silos, you don't get any congruence. Bringing a risk manager into the room to look at your greatest asset – the workforce – can give a business a huge advantage."

The risks arising from employee wellbeing can range from slight to extreme, says Mr Rofe. His comments follow a Lockton report of FTSE 100 companies that looked at which companies offered mental health support to employees, and the implications for the workforce and the business.

It found that only 42 per cent of FTSE 100 companies recognise mental health as an issue in its own right, while just 30 per cent have programmes that are targeted at the mental health of their workforce.

Mr Rofe says this is an example of where business risk could be significantly reduced, at the same time simultaneously improving the working lives of employees and their families.

"Our industry is awful about comparing 'return on investment' or ROI. New initiatives are often justified by all too simple ROI calculations with a focus on short-term savings," he says. "Understanding the complex interaction of employee health and wellbeing to key business processes and linking target outcomes to quantified business objectives is a far better measure."

Mr Rofe says that if businesses are truly to reduce the risk in the business, they need to improve their policies and procedures beyond pure corporate social responsibility projects.

"Chief financial officers have to take a leap of faith. You have to mine large and disparate data sets, and get your insights from many, many sources – exit interviews, days lost through absence, customer service scores, and so on," he says.

"Set that against the possibility to trim insurance costs, improved productivity, improved engagement and ultimately improved profits."

The Organisation for Economic Co-operation and Development Policy Framework published in March 2015 estimated that 20 per cent of the working population are experiencing some kind of mental health issue at any one time.

The statistics are even more frightening when you consider that half of all workers will suffer a period of poor mental health during their lifetime.

A UK government survey of mental illness in the workplace, conducted in 2013, suggested that industry could be losing up to £100 billion a year because of unresolved mental illness issues in the workforce.

Insurer Legal & General recently announced that it had started work with the charity Business in the Community to consider what the company can do to assess the mental wellbeing of its workforce.

Chief executive Dr Nigel Wilson has been well publicised in encouraging other business leaders to seize the initiative. "What gets measured gets managed," he says.

So why has mental illness not received more attention from senior executives? Mr Rofe believes it could be due to the fact that the healthcare industry has historically focused on other ailments.

> "There is so much that employers can do around emotional support, signposting of services and guidance on what is appropriate

"The key drivers of claim costs and inflation on private medical insurance premiums are normally muscular-skeletal, cancer, cardiac and mental illness. Over the years, cancer has received the greatest focus due to significant advancements in treatment and resultant cost implications," he says.

"Muscular-skeletal has had a lot of work going on for better signposting and better prevention, and cardiac has also benefitted from a lot of focus in the press linked with obesity and lifestyle issues.

"Mental illness is a tough one to tackle. Line managers are fearful of getting involved in mental illness cases. They may lack adequate training on how best to support their employees; they may not know what questions to ask or how to deal with the answers. There is a fear of causing offence or doing the wrong thing."

Incredibly, this remains the case, despite the Chartered Institute for Personnel Development reporting in 2015 that around 40 per cent of organisations have witnessed an increase in reported mental health problems over the past year.

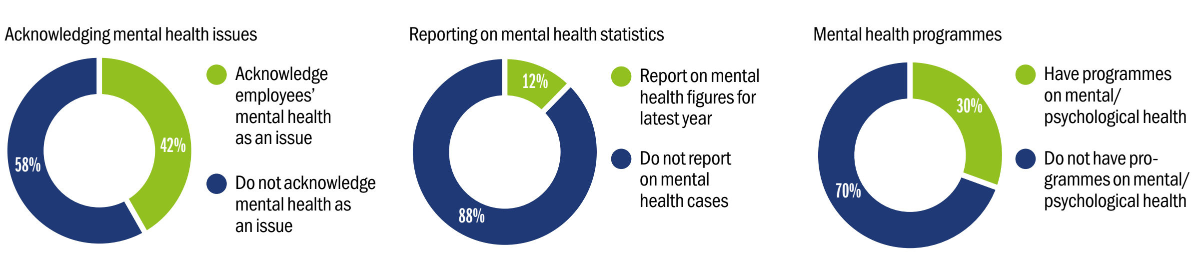
The findings are "shocking", says Mr Rofe. "There is so much that employers can do around emotional support, signposting of services and guidance on what is appropriate," he says.

"With little risk and cost, employers can do so much more to support the emotional resilience of their people, whether it's to reduce the chance of their employees making the wrong business decisions, preventing long-term sickness or more serious incidents."

There are some positives, however. The Lockton survey did find that four FTSE 100 companies have made leaps forward in assisting employees with mental health concerns. GlaxoSmithKline, Royal Mail, WPP and Reed Elsevier reported mental health statistics in 2014. The hope now is that many more follow in their footsteps for the benefit of both the business and the workforce.

www.lockton.com

MENTAL HEALTH PROGRAMMES AND REPORTING, 2014



Source: Lockton's analysis of FTSE 100 reports and accounts

OPINION COLUMN

Reputation and resilience in the business model

Looking through the risk lens to build reputation and resilience into the business model could help avoid or mitigate a corporate crisis

JOHN HURRELL
Chief executive, Airmic

If it feels like a high-profile corporate crisis is never very far from the headlines, then there is good reason. According to an estimate by risk advisers at Willis, the average enterprise will experience a crisis once every eight years. Many will suffer long-term damage and some will not survive at all.

The business climate is more cut throat, faster moving and less forgiving than ever. Partly as a result of the speed at which reports travel, spurred on by 24/7 news and social media, firms and their top executives are exposed to intense scrutiny. Reputations built over years can be trashed within days.

Business models, meanwhile, have become so complex that many top executives do not truly understand them. It is an alarming fact that, according to McKinsey survey data, almost a third of UK companies say their boards have "limited or no understanding" of the risks their companies face.

Airmic's *Roads to Ruin* research published in 2011 demonstrated how a lack of understanding or focus on risk at the very top of the company is a root cause of corporate failure. By contrast, last year's follow-up research, *Roads to Resilience*, demonstrated that companies where senior management were fully engaged with risks were not only more resilient, they were also more profitable.

> If a corporate crisis is perceived to be mismanaged, a loss of reputation can very quickly render all other assets virtually worthless, whatever your business model

We know from our research that boards are waking up to the importance of good risk management. Yet directors sometimes admit they do not know where to begin and they have plenty of other demands on their time. Many are frustrated that they lack the right tools and information to enable them to have an effective risk conversation. For example, the conventional event-driven risk maps, while useful in the right context, overlook many deep-seated risks with catastrophic potential.

If this brief analysis resonates with your organisation, we would urge you to consider a new approach, whereby boards explicitly view their critical risk exposures through the following two risk lenses:

- A detailed review of the corporate business model with analysis of critical threats and the effectiveness of response plans;
- A review of reputational risk vulnerabilities through the eyes of key stakeholder groups.

The benefit of using the business model as the basis for risk identification is that it provides the big picture and makes it easier to scrutinise the sustainability of how the business makes money.

Very briefly, our proposed approach, as described in the report *Looking Through the Risk Lens*, written together with the Chartered Institute of Management Accountants (CIMA), uses the four components of a business model – inputs, business activities, outputs and outcomes – as a basis for identifying the risks found in each layer of the value-creation process.

What does this achieve? It enables boards to view the risks to the business from a strategic, tactical and operational viewpoint, and to identify the risks that really underpin success. It also pulls together risks arising from different siloes, while bringing to the surface those that have been overlooked. Perhaps most importantly, it forces boards to ask themselves different, and often difficult, questions.

No analysis of the business model is complete, however, without taking account of the company's reputational risk vulnerabilities. Reputation is a critical underpinning of the business model – it is your licence to operate. If a corporate crisis is perceived to be mismanaged, a loss of reputation can very quickly render all other assets virtually worthless, whatever your business model.

It can require a different way of thinking to manage this hard-to-define risk. For example, a business might act within the law and even best practice, but yet still fall foul of public expectations. How often have we seen a company suffer for not issuing an apology early enough or sincerely enough?

We have worked closely with Reputation Institute on this subject and the importance of looking at risk events through a reputational lens has become increasingly clear. The most resilient companies constantly monitor how all stakeholders perceive their company which in turn encourages transparency. Looking at risk events through the reputational lens is therefore a critical dimension to identifying and mitigating risks before they turn into full-blown crises.

How does your business make its money? It sounds like a simple question, but much of our research has illustrated that many directors cannot adequately answer it. Or if they can, they have little understanding of what processes and events could leave it vulnerable.

Would this new approach have prevented the many corporate disasters we have witnessed in recent years? We are not claiming to have found a magic cure. But our approach surely would have flushed out some challenging questions for the C-suites to answer.

MANAGING RISK THROUGH THE BUSINESS MODEL

INPUTS

- Financial
- Manufactured
- Intellectual
- Human
- Social and relationships
- Natural

Conisder:
Supply and demand
Cost
Availability
Quality

BUSINESS ACTIVITIES

- Strategy
- Processes
- Projects
- Incentives
- Distribution

Conisder:
Changes to activities
Process
People
Technology

OUTPUTS

- Products
- Services
- Finances
- Infrastructure
- Intellectual property
- Brands

Conisder:
Supply and demand
Quality
Consistency
Distribution
Distinctiveness

OUTCOMES

- Market share
- Reputation
- Profitability
- Share price
- Customer satisfaction
- Sustainability

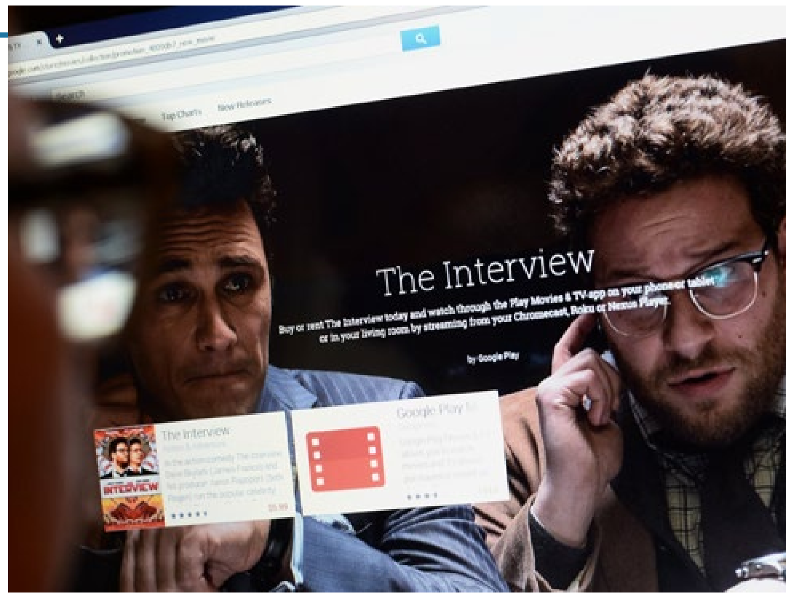
Conisder:
Stakeholders
Risk and reward
Long-term viability

Dealing with the risk of cyber hackers

Hackers can bring chaos and even ruin to businesses and organisations often with impunity, but what can be done to counter the computer attacks?

◆ **CYBER THREATS**

● **ANTHONY HILTON**



Guardians of Peace hackers invoked the 9/11 attacks in their most chilling threat yet against Sony Pictures, warning the Hollywood studio not to release a film which has angered North Korea

Among the thousands of reports and surveys to come out of the annual world economic summit in the Swiss ski resort of Davos, one of the most useful is the study of business risks in which executives rank what they consider to be the most pressing of their current concerns. Particularly significant this year was that cyber security grabbed number three position.

Today cyber attack is the existential threat to commerce. There is the threat to the integrity of a company and to its processes, which may need to be repaired and made good. There is the damage attacks can do to reputation; witness the problems of HSBC over tax avoidance. There is the risk of a loss of confidence from customers or suppliers who become reluctant to do business with or engage electronically with the firm. There is damage which is so severe it stops a firm from trading altogether.

All these are damaging, but there is something bigger still. There is also the open-ended threat of an attack on the financial infrastructure which is so severe it brings the system down. This is something which is a very real concern to the Bank of England. And then there is a vast amount of stuff in between where the system survives, but the costs run out of control. That is why insurance is so difficult to arrange; the scope and impact of cyber attacks are potentially so open ended. Marsh, one of the world's biggest brokers, is on record as saying that the cost from a single attack could reach £20 billion.

Not for nothing did Stephen Catlin, one of London's best-known insurance figures, say earlier this year that in his view the threat of cyber crime presented the biggest challenge the insurance industry had faced in his lifetime. He knows his firm and others like it are struggling to find answers. But while most can now offer some protection against narrowly defined risks, many clients feel what is on offer is nowhere near to meeting their needs.

Cyber attacks come from a variety of sources; it is not all about the money. There are conventional criminals of course, and extremely well organised ones at that, but there are also governments and their agents making mischief, evidenced by the North Korean attack on Sony Pictures over the release of a film making fun of its leader. There are organisations interested in commercial espionage, either a target company or its competitors, there are whistleblowers who believe some sensitive data should be put in the public domain and there are people without motive who hack into systems just to show they can.

> One of the world's biggest brokers is on record as saying that the cost from a single attack could reach £20 billion

The pressing question for board chairmen is how to assess the vulnerability of their own business and how then to manage the risk. What sort of governance do they need to put in place?

It is difficult because, while most boards are at ease in dealing with finance, they feel less comfortable with technology. It is important that the board is not overawed, however, because there is no qualitative difference in approach to risk control, be it in IT or any other area. Ultimately, at board level, it needs to be grounded in common sense and responds to the same line of questions. What are the crown jewels which the firm has to protect? Is the firm structured in a way which minimises its vulnerability? What are the threats and what systems are in place to deal with them? When were these systems last tested? What were the results? How often are the threats reviewed?

There are some experts who say this is not enough and that the only effective strategy is to assume at some point an attack will succeed. Working on this basis, the firm should ensure that once a hacker does get through, the damage they can do is limited, perhaps by having several different systems, rather than one big box, with tight security between the different silos. But that, of course, removes a lot of the advantage of centralisation and having all data in one place.

Unfortunately this is not cheap. A decade or so ago banks spending on cyber security ran into the low millions of pounds. Now it is hundreds of millions. The rest of the business world is about to set out on a similar journey.

COMMERCIAL FEATURE

PREPARE AND PREVENT: KEY TO EFFECTIVE RISK MITIGATION

As more organisations are sending staff abroad in an increasingly uncertain and unpredictable world, the power of prevention is getting its time in the spotlight, says ***International SOS***

Whether it's to explore new markets, access new suppliers or develop new business relationships, organisations are increasingly taking a global perspective, as more and more workers from all sectors are finding themselves on overseas assignments.

With global mobility levels predicted to grow 50 per cent by 2020[1], there will be more workers facing unfamiliar environments – and uncertainty raises risks.

"In order to make the most of the increasing opportunities around the globe while reducing their risk exposure, organisations are focusing on risk prevention strategies," says Franck Baron, Group general manager, risk management at International SOS, the world's leading medical and travel security risk services company. "It makes more sense, they're realising, to head off a problem than try to mitigate the damage once it has occurred."

> Pre-travel health check programmes reduce the number of failed assignments: $1 invested in prevention programmes returns a benefit ranging from $1.6 to $2.53[3]

Prevention strategies clearly produce a significant return on investment. According to a study published this year by Prevent, a research and consultancy firm, the average investment in an international assignment is $311,000 a year, while the cost of a failed assignment ranges between $570,000 and $950,000.

The study demonstrates how an organisation's successful implementation of a pre-travel health check programme aimed at identifying pre-existing medical issues before assigning employees to a foreign country reduced the number of failed assignments due to poor health, producing up to 2.5 times' cost-savings.

"Effective prevention requires intelligence, thought and planning, as well as education," says Laurent Fourier, director of the International SOS Foundation, a think-tank dedicated to improving the safety, security, health and welfare of people working abroad. "Organisations should understand the risks to their workforce and implement education programmes to mitigate risk and prevent incidents."

A case in point is that road accidents are one of the top five causes of medical evacuations led by International SOS. To mitigate this risk to business travellers, International SOS and Control Risks* developed *Travel Risk: Road Safety*, an e-learning programme with best practices from their combined expertise and that of the Global Road Safety Partnership.

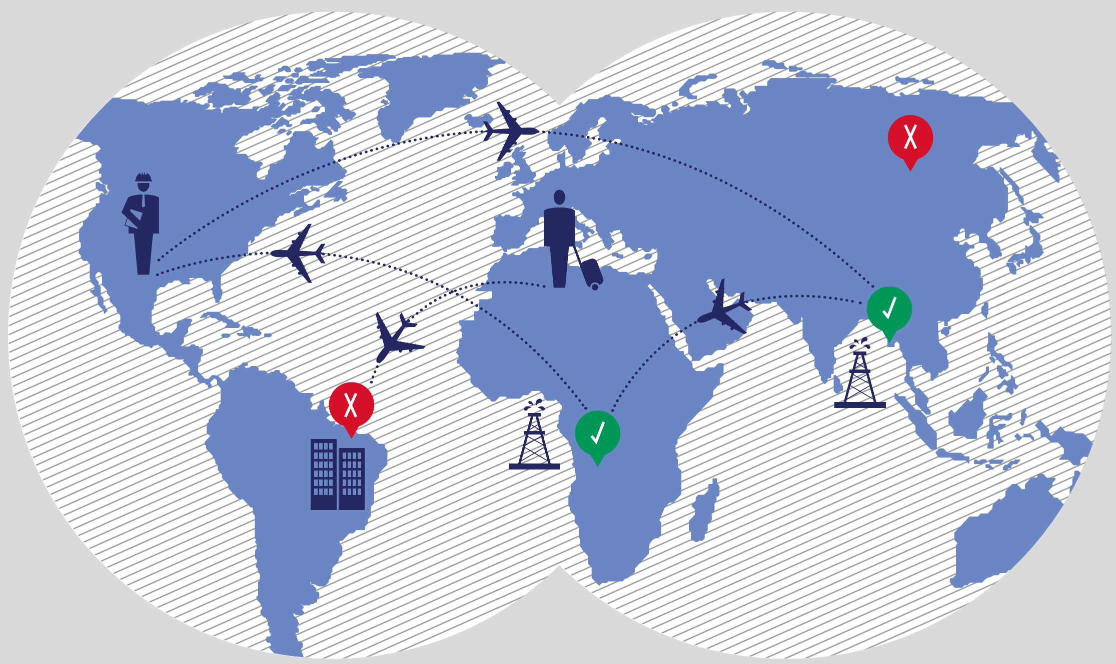
This emphasis on prevention means International SOS is regarded by its clients as a business enabler. "Corporate clients, governments and non-governmental organisations can further their business interests, while mitigating the risks to their workers through our information and assistance services. Productivity increases when organisations proactively mitigate risks and cultivate a 'duty of care' culture. Workers can focus on their core business mission with the confidence their organisation is developing and deploying appropriate travel risk management approaches to protect people from possible harm," says Mr Baron.

Knowledge is key to implementing meaningful prevention strategies. "Our deep knowledge of local environments, cultures, health systems, endemic risks, security threats and local infrastructure allows us to develop an accurate picture of the risks at any given destination," says Rob Walker, head of travel security intelligence, International SOS and Control Risks. "Rather than rely on information from a single source, we use a network of security and medical experts, both in-house and with external credentials, to provide real-time information that keeps travellers informed and supported."

In order to ensure that this information is accurate and reliable it's important to have a process of checks and balances to test the credibility of the sources. "Our personnel and our network of providers around the world give us the unique ability to source additional information or assess unconfirmed reports as necessary to further our prevention agenda," says Mr Walker.

PRE-TRAVEL HEALTH CHECKS & MALARIA PREVENTION PROGRAMMES BENEFIT BUSINESSES & EMPLOYEES

INTERNATIONAL SOS
WORLDWIDE REACH. HUMAN TOUCH.



The number of mobile employees is expected to grow
50% BY 2020[1]

Annual investment in an international assignment averages
$311,000[3]

Investing in pre-travel health programmes delivers savings of up to
2.5X[3]

NO PRE-TRAVEL HEALTH CHECK
Assignment is not complete. Cost $$$
Cost of failed assignment ranges between $570,000 to $950,000

PRE-TRAVEL HEALTH CHECK
Successful assignment. Cost $
Pre-travel health check programmes reduce the occurrence of failed assignments

Source:
1. www.pwc.com/talentmobility2020
2. http://www.ey.com/Publication/vwLUAssets/EY-Global_Mobility_Effectiveness_Survey_2013/$FILE/EY-Global-Mobility-Survey.pdf
3. internationalsos.com/return-on-prevention

Staff who feel vulnerable during their travels are less productive. This is an important message to risk managers, as only 30 per cent of companies have a system in place for tracking business travellers[2].

Organisations must have a proven system to contact workers abroad in case something happens that could affect their safety.

> It's not always possible to prevent every problem and organisations must have a solid plan for responding when incidents occur

As leaders in technological innovation, International SOS and Control Risks have created programmes, such as TravelReady, which automates compliance with an organisation's travel security and medical policies; and TravelTracker, the industry's leading traveller tracking service. In addition to helping organisations locate their workers, TravelTracker e-mails travellers with information on their destinations before and during their trips to keep travellers informed of potential safety risks and how to mitigate those risks.

Organisations with workers going to high-risk or especially remote locations may require additional levels of risk mitigation. Active monitoring solutions allow organisations to define high-risk areas and safe zones, and then notify them when, and if, workers enter those areas. Travellers are also notified if they are entering a high-risk location so they are aware of the dangers.

It's not always possible to prevent every problem, however, and organisations must have a solid plan for responding when incidents occur.

"Sometimes travel to high-risk areas is required and timing is crucial when responding to an event. Active monitoring solutions provide organisations confirmation of the safe arrival of an employee and timely information to enact a response if that individual is not at the location expected," says Mr Walker. "In addition to speed of response, travel safety advice must be easy to act on, and should come from experts with detailed regional and local knowledge.

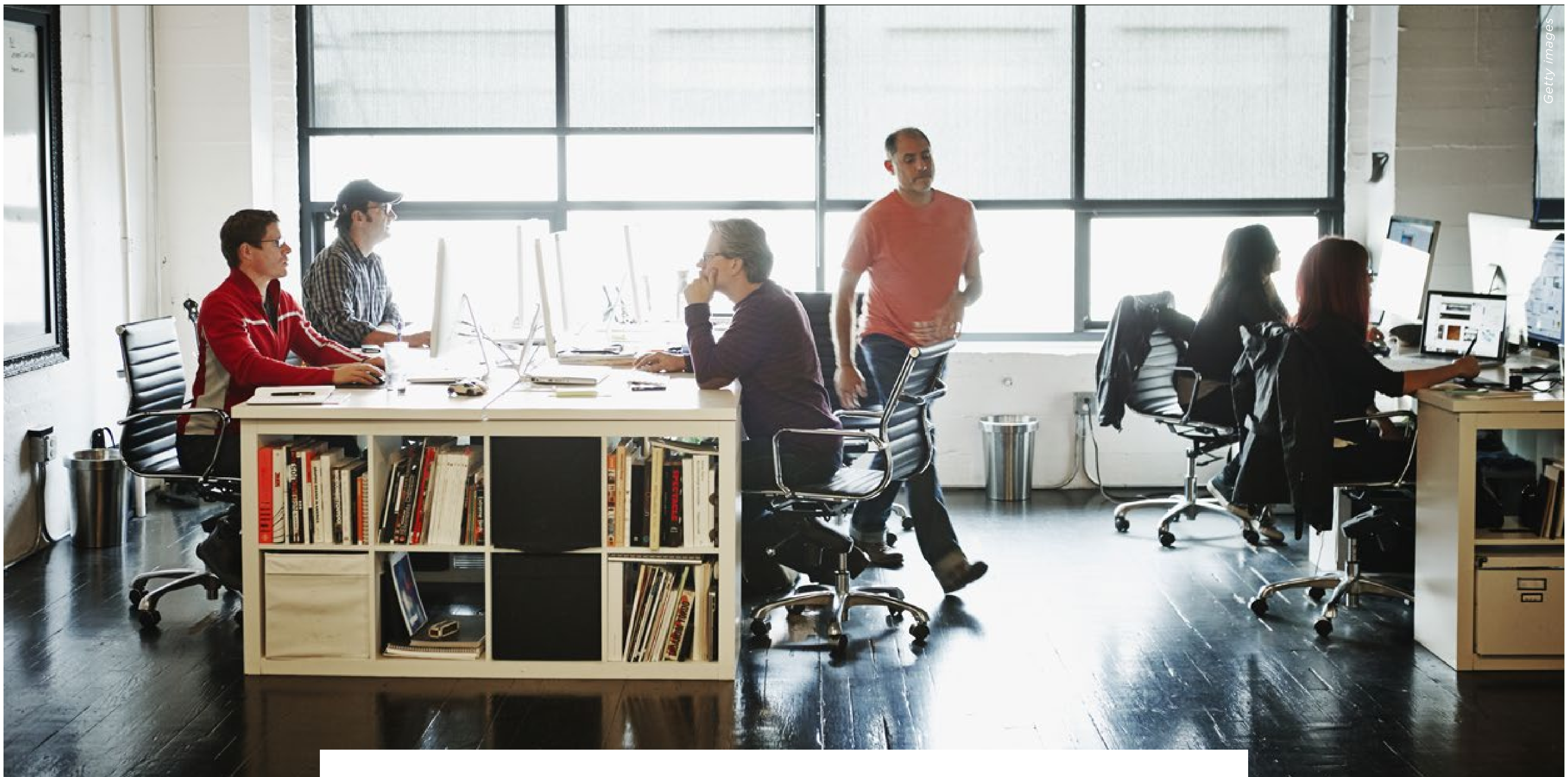
"Our goal is always to reduce risks to an organisation and their workers. However, when an event does occur and assistance is needed, a global assistance network to support clients is essential."

Today, this network, alongside a policy of preparation and prevention, is increasingly vital for organisations sending their staff abroad.

International SOS is the world's leading medical and travel security risk services company, caring for clients across the globe from more than 850 locations in 92 countries.

*International SOS and Control Risks combine the expertise and resources of both companies to provide a comprehensive suite of travel security risk services for mobile workers.

www.internationalsos.com



◆ INSURANCE

● HELEN YATES

Beware the pitfalls of underinsurance

With many smaller businesses struggling to recover from the recession, keeping insurance cover to a minimum has been a way of cutting costs which could, however, prove disastrous

When catastrophes strike, small businesses are frequently caught in the crossfire. For example, two thirds of small and medium-sized enterprises (SMEs) have been badly affected by severe weather in the UK over the past three years, according to the Federation for Small Businesses, with damage from the 2013-14 winter floods costing an average of £1,531. Others were temporarily unable to open their retail outlets as a result of riots in 2011.

SMEs are the backbone of the UK economy. Yet research by Towergate shows 43 per cent lack adequate storm cover. Underinsurance is a chronic condition, with up to 80 per cent of properties underinsured and 40 per cent of businesses lacking adequate business interruption cover, according to the Building Cost Information Service and Chartered Institute of Loss Adjusters. Small firms are particularly vulnerable as they do not have the risk management and insurance buying resources of their larger contemporaries.

"Underinsurance is unfortunately a very real feature of the current UK insurance market; a significant issue for material damage and business interruption exposures in particular," says Jason Eatock, head of SME at Zurich Insurance. "The fundamental issue is one of unexpected negative outcomes for customers when they have a claim, especially where an insurance policy becomes void because underinsurance is found to be deliberate and severe."

In tough economic times, when many firms are fighting for survival, there is pressure to keep insurance premiums at a minimum. Just under a third of insurance intermediaries saw a reduction in non-essential insurance cover in 2009. By 2010 this had grown to 57 per cent, the British Insurance Brokers' Association (BIBA) says. During hard times, the cost of insurance rather than extent of coverage is the main criterion for many firms.

KNOW THE JARGON

CONDITION OF AVERAGE
This clause is applied when a claim occurs and the sum insured under the policy is below the actual value of the item. Insurers then apply an "average" to the settlement of the claim, effectively reducing the payment made by the percentage of underinsurance. For instance, if a property is underinsured by 50 per cent and it experiences a £20,000 loss, the insurer will typically offer £10,000, half the amount needed to rebuild.

GROSS PROFIT
A flexible term, this is often interpreted differently by accountants and insurers. Overheads, especially wages and utility costs, are routinely deducted from turnover to calculated gross profit in accounts, but should be included for the purposes of calculating business insurance.

SUM INSURED
This is the maximum amount the insurance company will pay out, if everything you own is totally destroyed.

VALUATIONS
Best practice is to carry out a professional valuation each year or at least at intervals of no more than three years. This allows the surveyor to factor in issues affecting rebuilding costs, including inflation, alterations to the building and legislative changes.

REINSTATEMENT
This cover will replace old machinery for new, but indemnity cover will only provide for the market value of the equipment that has been damaged or lost.

It is often only in the event of a claim that underinsurance gaps are discovered. "If there is a disagreement over the settlement offered, it could be due to the customer not disclosing the right sums insured in the first instance," says BIBA executive director Graeme Trudgill. "Many customers will look to keep their insurance spend to a minimum, so they may not want to increase their sum insured every year."

The financial crisis was a big test for small businesses. In an environment of restricted lending and unreliable cash flow, many diversified their business models in order to survive. Plumbers turned their hand to solar panel installation, local grocery stores installed lottery machines and bookshops created in-store cafés.

While their entrepreneurial spirit helped such businesses weather the downturn, this introduced them to new risks. "Shops selling online may well start to export to North America not knowing that standard policies would usually exclude that territory," says Mr Eatock.

Keeping brokers and insurers abreast of changes to their business is not always at the forefront of a small business owner's mind. "Our experience tells us that clients do not think to contact us generally," says Chris Wilde, head of commercial at insurance broker Higos. "It's only when the insurance broker ties them down to review the cover that they remember they've purchased some extra machinery."

When Leicester-based Eurokey Recycling's plastics recycling site was destroyed by a fire in May 2010, the plant's combined commercial insurers threatened to avoid the policy as a result of gross underinsurance.

> "In tough economic times, when many firms are fighting for survival, there is pressure to keep insurance premiums at a minimum

The rapidly growing recycling firm had seen its turnover grow from £3.2 million in 2005 to an anticipated £25 million in 2010. But the business interruption sum insured of £2.5 million with a Lloyds syndicate had been based on a projected turnover of £11million. The value of stock and machinery was also significantly understated and, as a result, the insurer made a once-only offer of £1.5 million to settle the claim.

Few small businesses knowingly underinsure. Reasons often stem from ignorance surrounding industry terms. "There is a general misconception in that your building sum insured represents what you paid for it, the market value," says Mr Wilde. "From an insurance perspective it isn't, it's the rebuild value that's important.

"Quite often the problem with underinsurance, particularly of a building, is a partial loss rather than a total loss. If you lose 25 per cent of your building, say the roof, you've got to find the money to put that back on because, if you're underinsured, your insurers aren't going to give you the full rebuild costs."

Underinsured SMEs frequently go out of business. According to the Arson Prevention Bureau, 70 per cent of businesses involved in a major fire either do not reopen or fail within three years. "Underinsurance puts you under an extreme financial burden," says Mr Wilde. "If you have the resource to ride that pressure you will get through. If you haven't got the resource, it's likely to end up in the business closing."

Infrequent valuations and insufficient indemnity periods, in the case of business interruption, are other causes. The typical indemnification period for business interruption is one year, but this could prove too short a time-frame. Onerous building regulations and environmental factors, asbestos for example, could leave a small business out of action for a much longer period. "In a market town it could be a 200-year-old building with six-foot walls," says Mr Wilde. "That will cost a fortune to rebuild and, if it's listed, that brings in additional complications."

Disintermediation, as growing numbers of SMEs, particularly micro businesses, bypass the broker to buy insurance online is another concern. SMEs need access to expert advice, says Mr Wilde. "Whatever size your business is, commercial insurance is a complex animal and my view, after 36 years in the trade, is you need to be talking to people who understand your business so they can build the proper protection."

There when you need us

At Travelers we understand that in today's dynamic world things don't always go to plan and can sometimes go wrong. We recognise the importance of being prepared and the need for businesses to have insurance in place that addresses their evolving risks. That's why our flexible approach to insurance and risk management includes a broad range of property and liability insurance and risk solutions that are carefully designed to meet the needs of today's businesses.

From simple to complex risks; all underwritten individually with attention to detail, our products are tailored to meet clients' needs and priorities. Our specialist risk managers take the time to advise clients on current and emerging risks whilst our reliable and expert claims team are standing by to provide support if something goes wrong.

We are passionate about insurance and proud of it. Then again, as part of The Travelers Companies, Inc., one of the world's leading commercial property casualty insurers with more than 150 years of experience, you'd expect nothing less.

For more information about Travelers' range of insurance solutions and risk management services, visit travelers.co.uk or contact your local Travelers representative for a quotation.

TRAVELERS

travelers.co.uk

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