

# BUSINESS RISK STRATEGIES

03

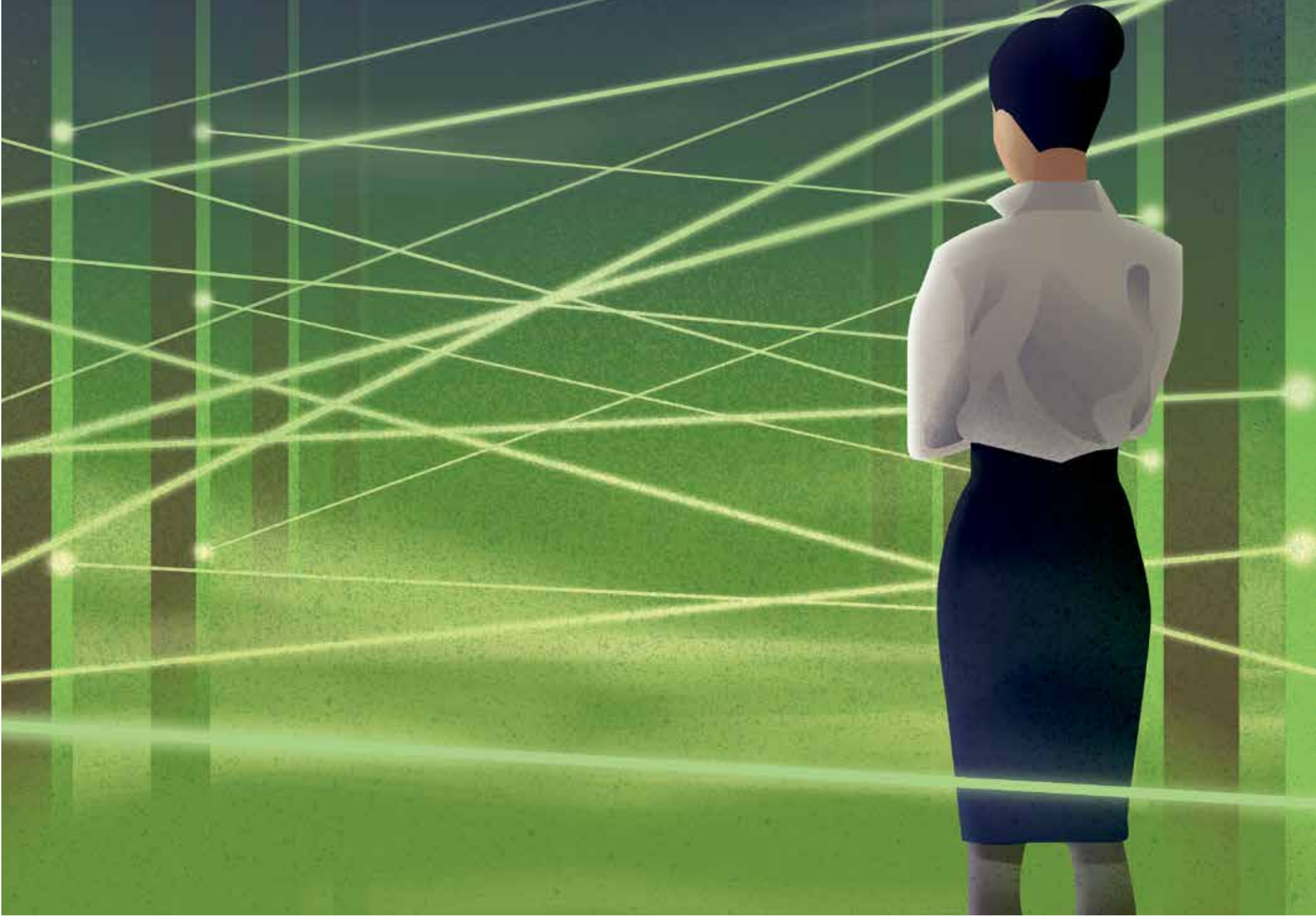
**BREXIT AND THE POLITICAL RISKS FACING UK BUSINESS**  
Amid geopolitical turbulence, businesses face Brexit turmoil

06

**WAYS TO MANAGE CONNECTED RISK**  
The potential domino effect of a major crisis is an ever-present risk

11

**TIME FOR BOSSES TO TACKLE HACKERS**  
EU legislation will force bosses to take cyber threats more seriously



Managing Risk in a Connected World



COMMERCIAL PROPERTY INSURANCE

**THE GOLDEN LION TAMARIN IS ONE OF  
THE RAREST ANIMALS IN THE WORLD.**



**BESPOKE SERVICE THAT SUITS YOUR UNIQUE  
BUSINESS NEEDS IS AN EVEN RARER FIND.  
UNLESS YOU'RE AN FM GLOBAL CLIENT.**

Unlike other companies, we don't provide off-the-shelf insurance. We prefer to take care of business with flexible, engineering-based solutions for companies of all shapes and sizes, across multiple sectors and territories. That's the reason why more than  $\frac{1}{3}$  of the Fortune 500 companies insure with us. And it's also why we're ranked #1 for service\*. Find out more about the commercial property insurer that really is one of a kind.

**GET THE FULL STORY AT [FMGLOBAL.CO.UK/BESPOKE](https://www.fmglobal.co.uk/bespoke)  
WHEN YOU'RE RESILIENT, YOU'RE IN BUSINESS.**

Source: [wwf.panda.org](https://www.panda.org). \* 2016 StrategicRISK Corporate Insurance Buyers' Survey.

©2017 FM Global. All rights reserved.



BUSINESS RISK

STRATEGIES

DISTRIBUTED IN

THE  TIMES

PUBLISHED IN ASSOCIATION WITH



RACONTEUR	
PUBLISHING MANAGER <b>John Okell</b>	DIGITAL CONTENT MANAGER <b>Jessica McGreal</b>
PRODUCTION EDITOR <b>Benjamin Chiou</b>	DESIGN <b>Samuele Motta</b> <b>Grant Chapman</b> <b>Kellie Jerrard</b>
MANAGING EDITOR <b>Peter Archer</b>	

CONTRIBUTORS	
<b>RICHARD BROWN</b> Business journalist, writer and presenter, he has worked for leading media organisations in London, New York, the Middle East and Asia.	<b>IAN FRASER</b> Author of <i>Shredded: Inside RBS, The Bank That Broke Britain</i> , he was business editor at <i>The Sunday Times</i> in Scotland.
<b>ANTHONY HILTON</b> Author, journalist and broadcaster, he is a former City editor of <i>The Times</i> and managing director of <i>The Evening Standard</i> .	<b>DAN MATTHEWS</b> Journalist and author of <i>The New Rules of Business</i> , he writes for newspapers, magazines and websites on a range of issues.
<b>CHARLES ORTON-JONES</b> Award-winning journalist, he was editor-at-large of <i>LondonLovesBusiness.com</i> and editor of <i>EuroBusiness</i> .	<b>DAVEY WINDER</b> Award-winning journalist and author, he specialises in information security, contributing to <i>Infosecurity</i> magazine.

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or e-mail [info@raconteur.net](mailto:info@raconteur.net)

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at [raconteur.net](http://raconteur.net)

The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher. © Raconteur Media

OVERVIEW

Brexit and political risks

facing UK business

Amid a swirling maelstrom of geopolitical turbulence, businesses in the UK face the added uncertainty Brexit brings to the boardroom

ANTHONY HILTON

To pass the time during a prolonged dull spell, a stock market analyst recently produced an analysis which showed that at least three quarters of the British companies in the FTSE 100 index were in some significant way dependent on politics and politicians for a major slice of their profits.

In defence and many other industries, government was a major customer; in transport it created and took away monopolies; in telcoms it controlled spectrum; in pharmaceuticals it approved products; in utilities it regulated prices. And all this was before it granted and took away investment incentives or invented new fundraising wheezes such as the air transport and banking levies or the insurance premium tax.

The observation is worth noting because it underlines that political risk has always been with us, even in Western democracies. But it also serves to underline why it is that the current times are so unusual. We have had several decades to grow used to the idea that governments and their regulatory agencies play by the rules so, even if we do not like them much, we know what to expect.

What is now different is that this has gone by the board. Consistency and continuity are so last century. The defining feature of politics today is its sheer unpredictability. The result is that of all the challenges facing business geopolitical risk is probably the fastest growing. It certainly has the ability to play havoc with the best laid plans.

For any UK-based firm or companies with investments here, Brexit must come top of this list. A year ago no major business took as real the possibility that the UK might vote to leave the European Union. But this is what happened and, having spent 40 years trying to harmonise standards, integrate markets and create cross-border supply chains, business now faces the possibility that some, if not all, will have to be undone.

For the financial sector the problems of market access and contract certainty are the main issues, for mainstream business it is supply chains, and the fact that components and raw materials might attract tariffs every time they move across a border. Moving to a new order is, in the words of one consultant, like trying to unravel a



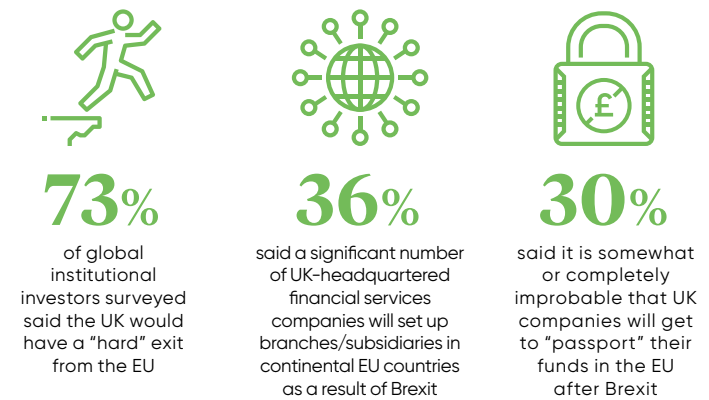
Theresa May at a question-and-answer session with workers at Screwfix in Stoke-on-Trent during the Conservatives' general election campaign

bowl of congealed spaghetti. The task is complex, costs are high and there is no guarantee at all that the dish will be palatable when the work is completed.

But in many ways Brexit is the beginning of the geopolitical story rather than its end. Leaving the world's richest market to trade even more successfully elsewhere implies that the UK will enter into a rash of trade deals. But each potential partner will demand access to some currently protected part of

our market in return for opening up its own. Each deal will come gift-wrapped with its own ticking time bomb of political risk.

Meanwhile, however, the world has other issues. More alarming in many ways is the change in administration and tone from the United States following the election as president of Donald Trump. On the campaign trail he accused China of killing America's manufacturing and Germany of exploiting America with its "grossly undervalued



currency". He promised to make America great again by bring manufacturing back on-shore, erecting barriers to imports and building a wall to keep out Mexican immigrant labour. No candidate in 80 years had campaigned on such a protectionist platform, let alone been elected on the strength of it.

Whether or not he lives up to the most extreme of his promises is not really the point. The rhetoric is already changing the reality on the ground. Cross-border activity has stalled and investment is flat; international acquisitions are much reduced; globalisation has not reversed, but people talk of its having reached its high water mark. They say history is not linear and even the spreading enlightenment of the Renaissance was halted when Florence's Medici rulers were toppled. It is a brave company today which bets against Balkanisation. There is much more emphasis on the local.

Then there is the fate of the EU. Historians have observed that previous periods of prolonged economic stress have led to a resurgence of right-wing extremism and economic nationalism. The Dutch and French elections brought some relief that the tide of populism had been stemmed, but no one, even in those countries, believes the problem has finally been defeated. With more elections to come things could still turn out badly. That in turn could cause a further bout of financial market turmoil and cast a shadow yet again over the sustainability of the euro.

Faced with all this executives have a choice. It might be understandable if they were to retreat into a bunker in the belief that it is just too complicated. That, however, is not the reality of how people behave. True there are moments of paralysis after a particularly egregious shock, but generally they do not last long. Instead business leaders tend to divide risks into two pots. In the first are the really big geopolitical risks about which they can do nothing other than to marshal all the facts at their disposal, prepare contingency plans, and resolve to stay nimble and alert so they can respond fast if something does happen.

In the other pot are all the other challenges with risks from cyber attacks to oil-price shocks, from reputational damage to currency volatility. Here they can do something. Here they can make a difference. And that is what the best businesses do. ●

# Risk management: why the best form of defence is offence

Effective risk management is often framed around keeping a company out of trouble. But faced with technological disruption, customer empowerment and low or even no barriers to entry, a company can no longer survive simply by defending itself



The three lines of defence model has been an essential part of a huge number of organisations' risk management strategies for many years. But this long-established approach, which involves identifying a first function or line that owns and manages risk, a second specialising in risk management and compliance monitoring, plus a third that provides independent risk assurance, is now being challenged.

For too many organisations managing risk has been viewed as a hindrance to entrepreneurial spirit, when in fact it should be the facilitator of agile business, according to EY, the global leader in assurance, tax, transaction and advisory services.

EY's view is that organisations must be capable of quickly assessing strategic risks and taking decisive action. The firm believes that maximising upside risk and managing downside risk in line with its appetite for risk can also make an organisation more entrepreneurial. It argues that the three lines should be used offensively rather than purely defensively, as has traditionally been the case.

"By rethinking how it deploys the three lines of defence model, an organisation can make its risk management process a force for more nimble decision-making and innovation," says John Abbott, risk partner UK at EY. "Instead of serving purely as a reactive approach, a growing number of risk management professionals are using the three lines proactively."

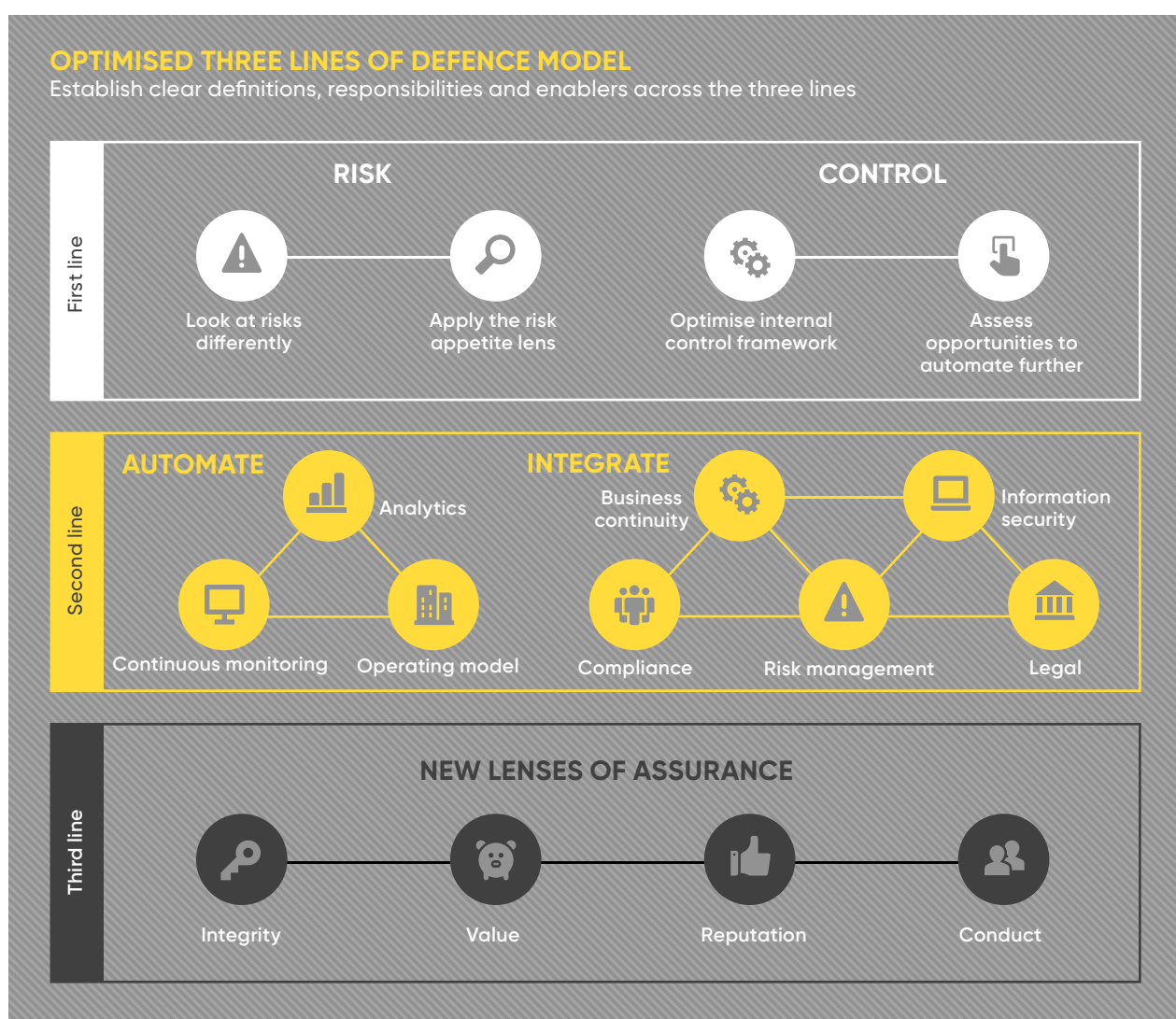
As the risks facing organisations in an evermore uncertain and fast-moving world increase, he explains, more shrewd risk management professionals are revisiting the application of the three lines of defence model in their organisa-

tion, and assessing what changes and improvements can be made at each of the three lines to manage risk in a more effective and proactive manner. And it's not just about fixes within each of the lines as responsibility and accountability across the lines need to be clarified.

Technological change, for example, in the form of the emergence of robotics and artificial intelligence is playing a key role by allowing companies to leverage automated controls to manage and mitigate their risk in the first line of defence. At the same time the introduction of scalable and cost-effective monitoring processes enabled by technology is helping companies to be more agile, while at the same time reduce the cost burden at the second line.

"We're working with a wide range of clients to make the most of the various opportunities they face to help them to accelerate the improvement in their lines of defence," says Colette Devey, risk director UK at EY. "Newer, fast-growth clients are better placed to adopt by building highly automated systems from scratch very easily. Larger, more mature organisations, typically FTSE 50 companies, are often restricted by legacy systems and are having to consider how they can strengthen their lines of defence in a different way. It's almost as if they're changing the tyres as the car is moving."

"The typical impetus to change here are situations in which companies have experienced control and accounting issues and surprises. For example, this could be where they have suffered cyber attacks similar to the one that gripped the NHS and other organisations worldwide earlier this month. In these instances such attacks have



exposed cracks between the lines of defence and this has driven companies to make improvements."

EY helps smaller, newer companies to use technology to build an effective and efficient model for proactive risk management from the outset. On the other hand, the firm also advises risk management professionals at the larger, longer-established organisations on how to build an effective business case for more investment, as well as other ways in which risk management can be made more agile and proactive, for example applying a different lens on risk.

"Brexit provides a good example of how to use the three lines of defence in this new offensive or proactive way," says Ms Devey. "It also shows how risk management professionals can become more involved in C-suite discussions and strategic decision-making. Firstly, they should work

to understand the economic, political and business risks that Brexit represents to their organisation."

"Then they should paint potential scenarios over next the few years and beyond, and look at how they would deal with them, using risk techniques such as the three lines, but in a more forward-looking way."

Mr Abbott adds: "For example, risk management professionals at a pharmaceutical company looking at moving its management team abroad because of Brexit could take a more proactive role to advise the board on whether simply to identify new office space or whether it should go a step further and actually sign leases."

This proactive approach to the three lines also makes it easier to turn threats into opportunities, he argues, offering an example from another, very different sector: "Brexit could mean a reduction

in immigration and, therefore, if you're in the fruit-picking business you could be looking at automation as a way of not only managing this risk, but of cutting costs and gaining competitive advantage."

Risk management has traditionally been seen as reactive or negative, with a focus on telling teams of people that they can't undertake a particular initiative or activity.

"Using the three lines of defence in a different, more proactive way, by carrying out predictive analysis and testing risks relative to each other, allows risk managers to have a greater influence on the C-suite and to add value for shareholders," says Mr Abbott. "This new approach is now essential for managing risk in these uncertain times."

For more information please visit [www.ey.com/uk/risk](http://www.ey.com/uk/risk)



**COLETTE DEVEY**  
DIRECTOR  
EY RISK



**JOHN ABBOTT**  
PARTNER  
EY RISK



BREXIT

IAN FRASER

Lloyd Blankfein, chief executive of Goldman Sachs, warns that the City of London “will stall” and see its position as a global financial centre eroded as a result of UK’s decision to leave the European Union.

His bank, which has had a London presence since 1970 and currently employs 6,000 in the capital, has already started to shift hundreds of workers out of London to Frankfurt, Paris and Warsaw as Brexit looms. There have been rumblings that Goldman’s London-based staff will eventually dwindle to 3,000 as a result of last June’s referendum result.

Brexit was always going to be tough for the UK’s highly internationalised financial services sector, whose total annual revenues are £200 billion, according to consultants Oliver Wyman.

Given the Theresa May government’s recent policy pronouncements on Brexit, which have been largely underpinned by her focus on limiting immigration, there’s a widespread acceptance that Brexit will be much “harder” than some had envisaged, and will include full departures from the single market and customs union.

UK financial services, a sector which is also clustered around regional centres including Edinburgh and Leeds, derives 25 per cent of its annual revenues – around £45 billion to £50 billion according to Oliver Wyman – from sales to other EU states.

So some or all of these businesses are vulnerable to drifting away to places such as Frankfurt, Paris, Dublin and Luxembourg, and each of these centres has since last June been seeking to woo decision-makers in the sector.

In prime minister May’s Lancaster House speech on January 19, she made clear she favoured a hard Brexit, effectively killing off any residual hope among City firms they would be able to retain the “passporting” rights, which enable them to sell products and services freely across the EU.

The tone from Downing Street in recent months, including Mrs May’s triggering of Article 50 on March 29 and manifesto launch on May 18, ce-



Chris Ratcliffe/Bloomberg via Getty Images



Estimates of how many jobs could ultimately be lost in the UK financial and professional services sector range wildly from 9,000 to more than 230,000

J.P. Morgan is likely to be moving them to its existing bases in Frankfurt, Dublin and Luxembourg, while Deutsche Bank, which has had a London presence since buying Morgan Grenfell in 1989, has indicated it will shift 4,000 jobs from London to Frankfurt. In January, HSBC said it expects about 1,000 or 20 per cent of the investment banking jobs it has in London to move to Paris.

Insurers including AIG and Hiscox are favouring Luxembourg as an EU trading hub, as does the Prudential’s asset management arm M&G Investments. Paris is also gaining ground as a potential base for asset management firms, especially since the election victory of centrist president Emmanuel Macron. Insurer Standard Life, which is in the throes of merging with rival Aberdeen Asset Management, is plumping for Dublin.

Estimates of how many jobs could ultimately be lost in the UK financial and professional services sector range wildly from 9,000 to 10,000 estimated by Bruegel to more than 230,000 forecast by EY.

There is currently a fierce debate over whether the clearing of euro-denominated derivatives – a major business for London where it supports 83,000 jobs – is going to be forced away by Brexit. The early signs are that the European Commission will enact new legislation which will require UK-based clearing houses of euro-denominated transactions either to relocate to the EU or be directly regulated by the European authorities.

But Catherine McGuinness, head of policy for the City of London, has warned this could cause chaos. “Uprooting and offshoring [euro clearing] would not only be vastly complicated, but also vastly damaging and potentially destabilising,” she says.

Some banks may choose to shrink their European operations or retreat back to Wall Street as a result of Brexit rather than go through with the hassle of preparing for the unwanted divorce, which will reduce competition and diminish access to capital in Europe.

Jonathan Wills, a partner in Oliver Wyman, warns that the cost of financial services will rise as a result of Brexit. He predicts that the return on equity of European investment banks will fall by about five percentage points or by around \$1.5 billion across the industry, as a result of Brexit induced costs, uncertainties and inefficiencies. And bankers, including Goldman Sachs’s Europe head Richard Gnodde, have made no secret of the fact they will pass the extra costs on to their clients. ●

# London and all UK look set to take hit

Hard Brexit would cost the financial services sector and UK economy dear as firms lay plans to relocate thousands of jobs elsewhere in Europe

mented doubts the industry would be able to wring any special favours from the UK government once Brexit talks commence.

The mood music in the City of London has swung from panic, amid rumours of absolute carnage in the Square Mile, to confident assertions that the effects are going to be marginal and London will retain its financial crown.

In recent months, in response to entreaties from regulators on both side of the English Channel, the top management of financial firms, especially in the most affected sectors of investment banking, asset management and insurance, have been working on contingency plans.

In some cases these include physically relocating everyone who deals with EU-based clients, plus all the

associated risk and trading functions, as well as the capital that supports them, to other European countries. The Bank of England has given banks and other financial firms until July 14 to present their plans.

EU regulators have made clear that financial firms will not be able to circumvent Brexit by establishing empty-shell companies in EU member states. “To be clear, we will only grant licences to well-capitalised and well-managed [firms],” according to European Central Bank (ECB) executive director Sabine Lautenschläger. “Any new entity must have adequate local risk management, sufficient local staff and operational independence.”

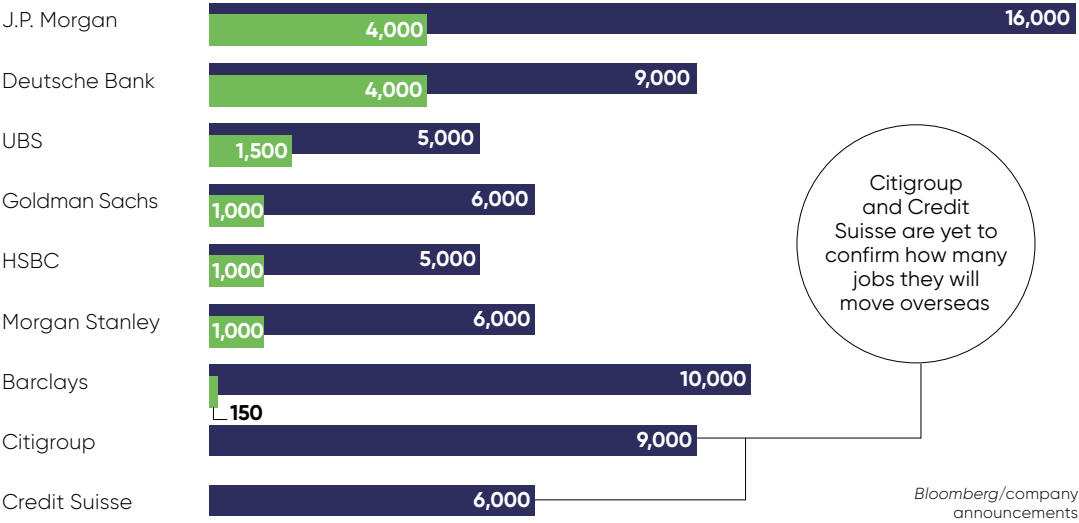
The ECB, in particular, is concerned that the stability of the EU’s financial system could be at risk in the event of a “cliff-edge” Brexit, a chaotic scenario in which firms are under-prepared and the terms of trade for cross-border finance have not been nailed down.

To date, some 30 to 40 per cent of UK-based financial firms have already started to relocate, or to make plans to relocate, thousands of staff to financial centres elsewhere in the EU. The banks currently intending to move the most posts to EU financial centres are J.P. Morgan and Deutsche Bank, each of which intends to transfer up to 4,000 jobs.

Lloyd Blankfein, chief executive of Goldman Sachs, warned that the City of London “will stall” as a result of Brexit

UK FINANCIAL JOBS AT RISK

● Job moves reported ● Total number of UK staff



## CONNECTED RISK

# Management of risk must be a science

The potential domino effect of a crisis is an ever-present risk to UK businesses with supply chains and markets abroad and at home

RICHARD BROWN

Imagine the scene: a flight arrives at Singapore Changi Airport from a provincial city in mainland China. On board a woman has been fighting for her life with a dangerously high temperature, aching muscles and serious respiratory difficulties. Upon arrival she is diagnosed with the deadly H7N9 strain of avian or bird flu.

What happens next?

With more than 100 airlines linking Singapore to 320 cities in 80 countries and territories worldwide, Changi is a phenomenal transit hub. A highly infectious disease like avian flu triggers an immediate emergency at the airport. But it is not sufficient to quarantine the ill woman to contain the disease, because many of her fellow passengers could also have been infected in-flight. And they have now passed through immigration and gone on to the collect their baggage from the carousel.

Each week, some 6,700 flights land or depart from Changi, while more than 54 million passengers travel through the airport each year and almost two million tonnes of freight are shifted annually. One highly infectious person in such an intense dispersal environment could wreak untold damage worldwide.

As an emergency remedial measure, the airport authorities decide, reluctantly, to shut the airport. All flights into Changi are diverted to airports in Malaysia, Thailand and Indonesia, while those preparing to depart are grounded. Similarly, all freight movements are suspended.

Imagine the devastating effect on the reputation of a sparkling international airport boasting a clutch of prestigious awards as Top Worldwide Airport, the World's Best Airport 2015 and the Best Airport in Asia-Pacific. All those cancelled flights, all those redundant tickets, all that lost business, all the incalculable consequential liabilities, all that fear.

With each passing day Changi is under lock-down, regional businesses haemorrhage cash. Time-critical supplies of pharmaceuticals, medical equipment, transplant organs, blood, let alone fresh food and urgent machine, automotive and industrial parts, languish in the freight terminal.

The authorities consider halting all air, land and sea traffic in the vicinity. As the news spreads, the finance and credit markets react nervously to the unfolding in crisis. And the stocks of aviation companies and leasing firms are negatively impacted by the event. In this nightmare scenario, the airport chief executive and several airline bosses separately face the daunting prospect of having to explain the consequences of the scenario live on TV. Bills get delayed or unpaid. The chorus of contract breaches is deafening.

So too are the insurance implications; these are pressing, the potential claims stratospheric. Who is the insurer of last resort in such a catastrophe? How can overlapping liability issues be resolved? Does anyone, anywhere have a calm, balanced insight into all the probabilities for such a doomsday scenario affecting Singapore Changi, one of the best organised airport hubs in one of the most dynamic economies on the planet?

The answer is, perhaps improbably, yes.

View of runway at Changi Airport, Singapore

Russell Group, the UK-based connected risk management and data analytics firm, is among organisations that highlight underlying risk volatility in the aerospace sector and continuously call for a more integrated approach to underwriting risk management by the insurance industry.

Suki Basi, Russell Group's managing director, stresses the need to unify the often fragmented, siloed information stored by insurers in the aerospace "ecosystem" to help them intelligently assess risks posed by multiple "what if" scenarios, such as an airport being quarantined.

He says: "The insurance industry urgently needs to look at restructuring or 'harmonising' the data sets at its disposal to take into account the domino effect upon all liability, financial, operational and purely commercial ecosystems affected by a crisis. The absence of a wide range of potential events and their consequential knock-on effects in many scenario modelling exercises is quite alarming."

As companies and organisations increasingly integrate across industrial sectors, geographies and cultures, they operate sophisticated supply chains and delivery systems

to end-clients and markets. Event complexity and risk drivers, such as cyber threats, political change and violence, supply chain risks, natural perils and credit risks, can affect a corporate at multiple levels as the assets and activities at each level receive risk from the same event.

Connected risk can traverse through and across all industrial sectors by existing and contingent business relationships. Corporates can and will be exposed to these events.

The aviation industry is particularly open to the disruptive forces of connected risk because it links travellers, economies, businesses and

“The absence of a wide range of potential events and their consequential knock-on effects in many scenario modelling exercises is quite alarming”

insurers at the same time. An October 2016 IPSOS Mori global survey of more than 1,000 professionals across 75 countries responsible for their organisation's travel policies found the vast majority had modified itineraries due to health or travel security concerns in the past year. This is a prime symptom of connected risk.

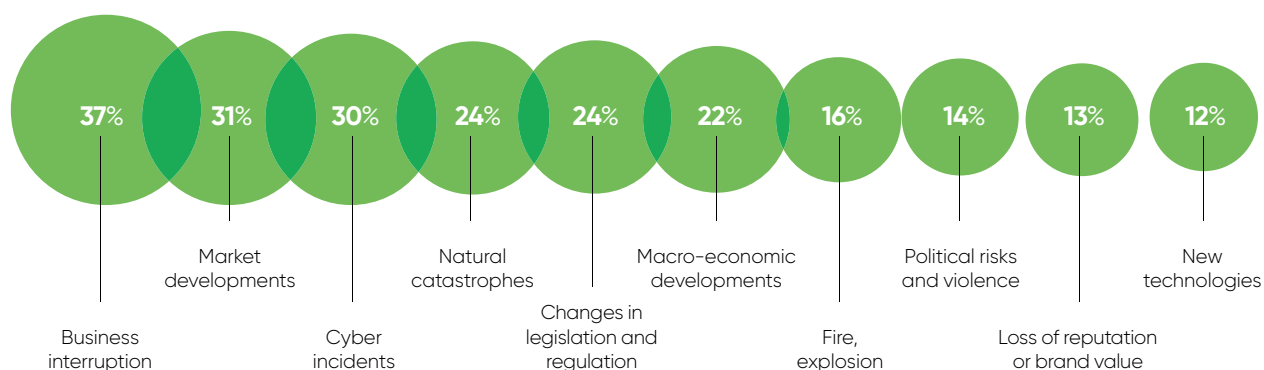
Clearly, business risk is of critical concern for corporates. The latest Cambridge Centre for Risk Studies' *Cambridge Global Risk Index* predicts that this year the global economy will face an expected loss of \$1.17 trillion as a result of increased connected risks.

Take this month's co-ordinated international WannaCry ransomware cyber hack against parts of the UK's National Health Service and a range of other organisations in 150 countries. There is no clearer example of how the interconnected nature of public, private and governmental sectors are globally vulnerable to sophisticated digital attacks.

Exposures created by the growth of global connectivity demonstrate the need for scalable and integrated analytics and actuarial modelling capabilities that, underpinned by reliable data, can help transform 21st-century risk management into a real science. ●

## TOP 10 BUSINESS RISK OF 2017

PERCENTAGE OF GLOBAL RISK EXPERTS RATING THE FOLLOWING AS ONE OF THE THREE MOST IMPORTANT RISKS FOR COMPANIES





COMMERCIAL FEATURE

# What is connected risk?

Our world is more connected than at any time in history – and business has never been so exposed to connected risk



With a simple tap of the keyboard, multi-million-dollar deals are struck across continents and consumers can order almost anything from almost anywhere in the world to their doorstep. We have never had it so good.

Companies with operations spread out across the world can situate their production or headquarters in areas of low tax or low labour costs. The likes of Exxon-Mobil, Walmart and Apple straddle the planet in a manner befitting colonial European empires with the sun never setting on the ring of the cash register or the spinning cogs of the production line.

Yet, as history has proven, no empire is everlasting, especially as it overreaches itself, resulting in decay and ruin. In this new era, organisations are vulnerable to the whims and rhythms of the connected world. A world connected by hazards or risk drivers such as political volatility, cyber hacking or supply chain exposures caused by terrorism, piracy, inadequate safety controls and other critical factors which can create a rapid path to ruin.

This time it is not the barbarians at the gate, but a new business risk, what we call connected risk.

Connected risk is the systemic exposure of commercial organisations, their partners, suppliers and clients to cumulative and cascading financial, operational and reputational vulnerabilities. It is caused by an inherent weakness in the inter-connected architecture of today's business-to-business relationships. These are increasingly digital and allow a single negative event to exponentially spread disruption and paralysis, and wreak severe economic damage both within and between organisations.

The key drivers for connected risk are the ways in which political, environmental, supply chain, cyber and credit risks combine to cause financial, operational and reputational loss.

In an increasingly connected world,

corporates and their networks need to prepare for more unpredictable "black swan" events which are caused when a local event produces a so-called butterfly effect and unleashes a cascade of further events through the network, impacting numerous corporates along the way.

This exposes a raw nerve in corporates' sophisticated global supply chains and/or delivery systems as they are now vulnerable to extreme events and systemic risk.

“ Connected risk is the systemic exposure of commercial organisations, their partners, suppliers and clients to cumulative and cascading financial, operational and reputational vulnerabilities

To illustrate the power of connected risk, imagine an international oil company called xConnect. The company has taken out a substantial loan to fund large-scale oil exploration in Asia. So the networks involved in this deal are xConnect's boardroom, the bank, oil traders, specialist exploration companies, drilling companies, rig contracting companies, pipeline operators, the insurers underwriting the deal, refineries and distributors.

Imagine an event where a determined government nationalises xConnect's oil leases and those of others within its jurisdiction in Asia. These are the connected risk effects: there is a shock in the oil price as supply volatility causes concerns for traders in the oil markets; across equity markets the share price plummets for all oil companies involved in the Asian event as investors move their money elsewhere; the bank

seizes collateral in exchange for losing millions; insurers worry about the prospect of resulting claims; and the drilling and rig contracting companies also lose assets and the resultant revenue loss causes some to default on their loans, triggering further volatility in oil and equity markets, with consequential negative impact on future exploration costs.

At xConnect, the risk management division had not expected such a scenario could take place and had not devised counteracting continuity measures which therefore left the board in an untenable position.

This is but a taste of the power of connected risk. It is happening now. And it is the new normal of business risk.

Retailers' principal market risks centre on their globally connected presence. A chief challenge of any corporate with locations in many countries is the cost of regulatory compliance, which is different from region to region. The world's largest supermarket brand, for example, must enforce different workplace standards in China from those in the United States. In so doing, the company is subject to acute regulatory uncertainty.

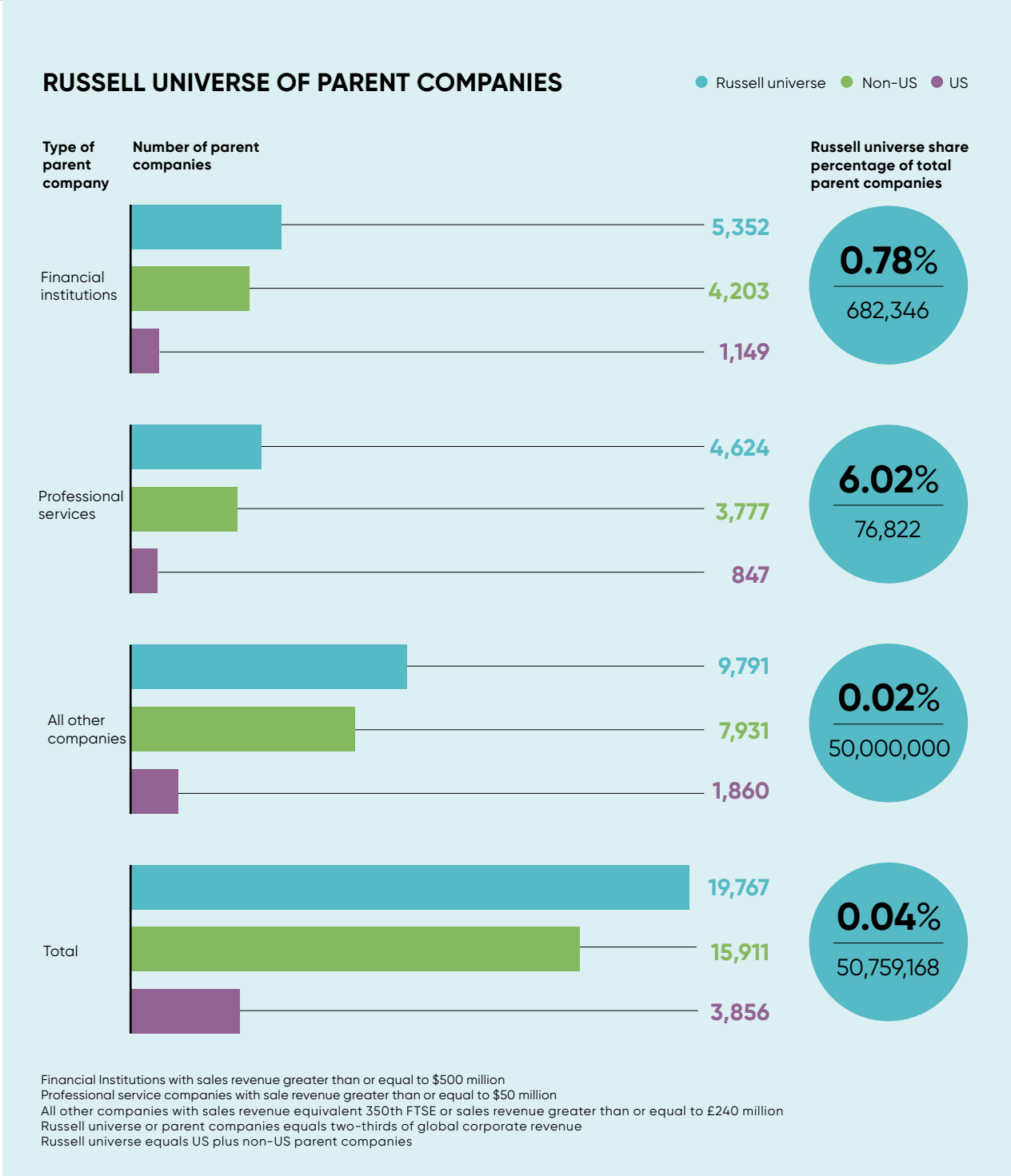
Aside from the financial implications, a company is exposed to profound reputational risks through its

supply chain. The collapse of flimsy buildings in Bangladesh, which housed contractors and sub-contractors sewing clothes, negatively affected many US corporates, unaware their brands were being manufactured in such conditions.

The new risk landscape ushered in by connected risk is one riddled with greater event complexity and less risk foresight. Corporates need to recognise that new and established business relationships, whether with suppliers, manufacturers, traders, financiers or consumers, are the entry point for connected risk.

The ultimate connected risk is the emerging cyber peril that threatens to swamp business in a tsunami of digital disruption. The internet of things and increasing reliance on mobile technology is a wonder of the modern age, but it is also an existential threat affecting individuals, organisations, governments and even great trading

“ The key drivers for connected risk are the ways in which political, environmental, supply chain, cyber and credit risks combine to cause financial, operational and reputational loss



blocs like the EU, NAFTA and ASEAN. Hackers and new forms of malware have the potential to access personal, sensitive data, shut down critical infrastructure or ground aircraft.

Today's organisations are becoming increasingly interconnected and embedded in the same network. Thus systemic risk poses a real threat. The failure of a single firm from a connected risk can have a disproportionate effect on both the organisations connected to it and the entire industry. It's a real concern for chief executives who are aware of the urgency of connected risk, yet are unsure how to proceed.

The solution for corporate risk managers navigating the rough seas of connected risk is to have an integrated risk management framework. A framework that quantifies bottom-up exposure, manage risks and in so doing delivers superior return on equity. Combining the power of data analytics with the latest integrated risk modelling, led by companies such as Russell Group, it is now possible to price and value our hitherto unknown connected risk exposures much more accurately.

For more information please visit [www.russell.co.uk/connectedrisk](http://www.russell.co.uk/connectedrisk)

# WANNACRY

## The biggest ransomware attack in history

Admittedly not everyone is a cyber security expert. But, if you hadn't heard of ransomware before this month, chances are you've heard of it now. The WannaCry ransomware has rocked every corner of the globe over the past two weeks, affecting more than 250,000 victims across 150 countries in one of the most aggressive and widespread cyber attacks in history. Whether directly affected or not, boardroom nerves the world over have been rattled as decision-makers face up to the risk cyber threats present to their organisation.

### COUNTRIES HIT BY WANNACRY

● Affected ● Unaffected

#### UNITED STATES

Delivery company FedEx's logistical operations affected

#### UK

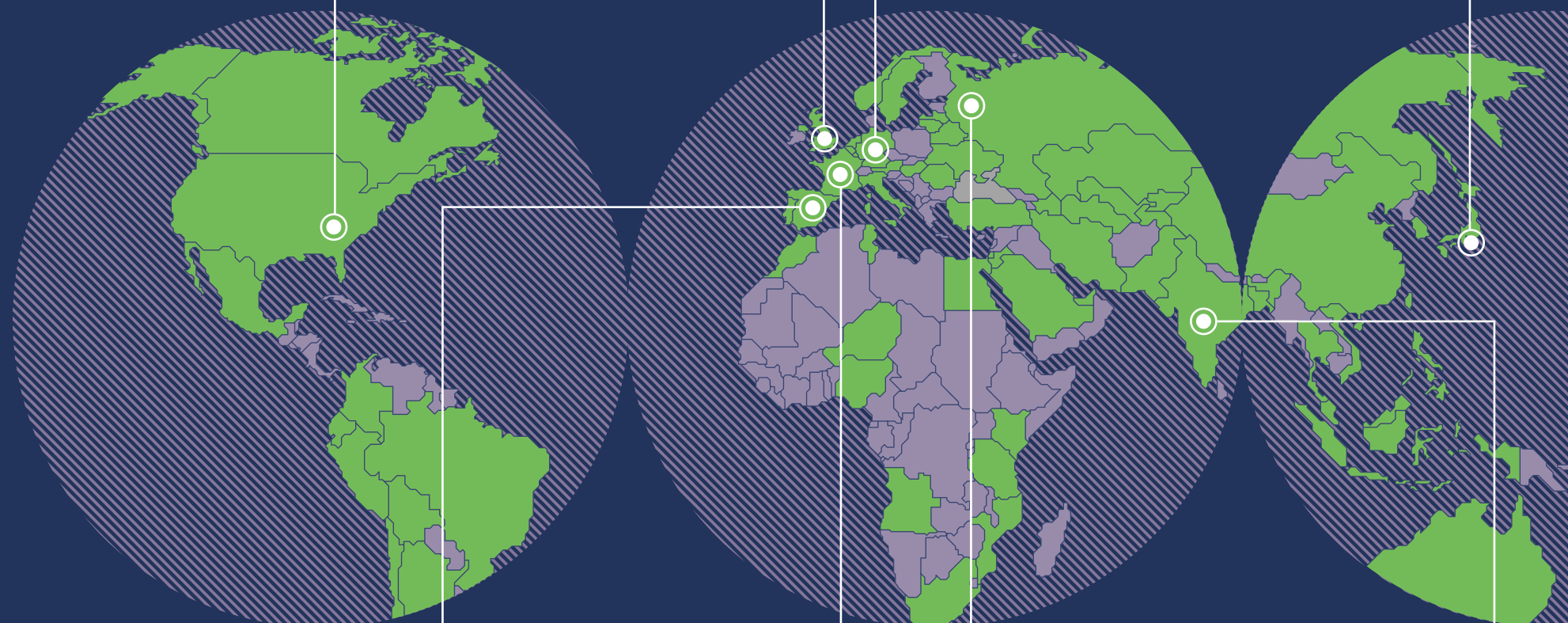
NHS organisations disrupted and many operations cancelled at short notice

#### GERMANY

Deutsche Bahn confirmed ransomware had disrupted train station departure boards across the country

#### JAPAN

Electronic carmaker



#### SPAIN

Telecoms and gas companies struck

#### FRANCE

Some Renault factories had to stop production

#### RUSSIA

Largest number of incidents reported, including disruptions at the Russian interior ministry

#### INDIA

One of the

### BACKGROUND

WannaCry (also known as WanaCrypt0r and WCry), a new variant of the Ransom. CryptXXX family of ransomware, hit companies and individuals across the globe on May 12. WannaCry exploits a vulnerability in the older Microsoft Windows XP operating system, security updates for which were stopped in 2014.

It can encrypt 176 different file types and asks victims to pay \$300 in bitcoins to one of three bitcoin wallets to release the data. If payment is not made, the ransom would double after three days; if payment is not made in seven days, the encrypted files would be erased. While victims have been advised not to pay, funds are still being sent to the ransomware attackers.



**+250k**

systems affected by the WannaCry ransomware



**150**

countries affected



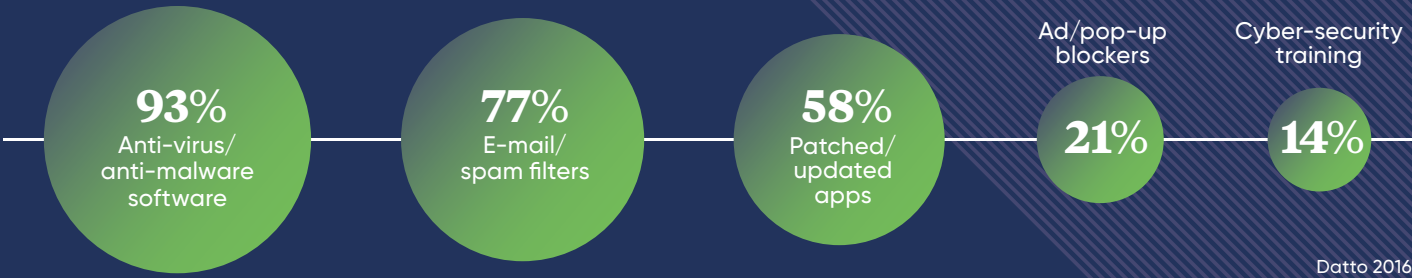
**\$300**

ransom requested per system



RANSOMWARE OUTSMARTING CYBER-DEFENCE MEASURES

DEFENCE STRATEGIES IN PLACE WHEN RANSOMWARE ATTACKS OCCURRED

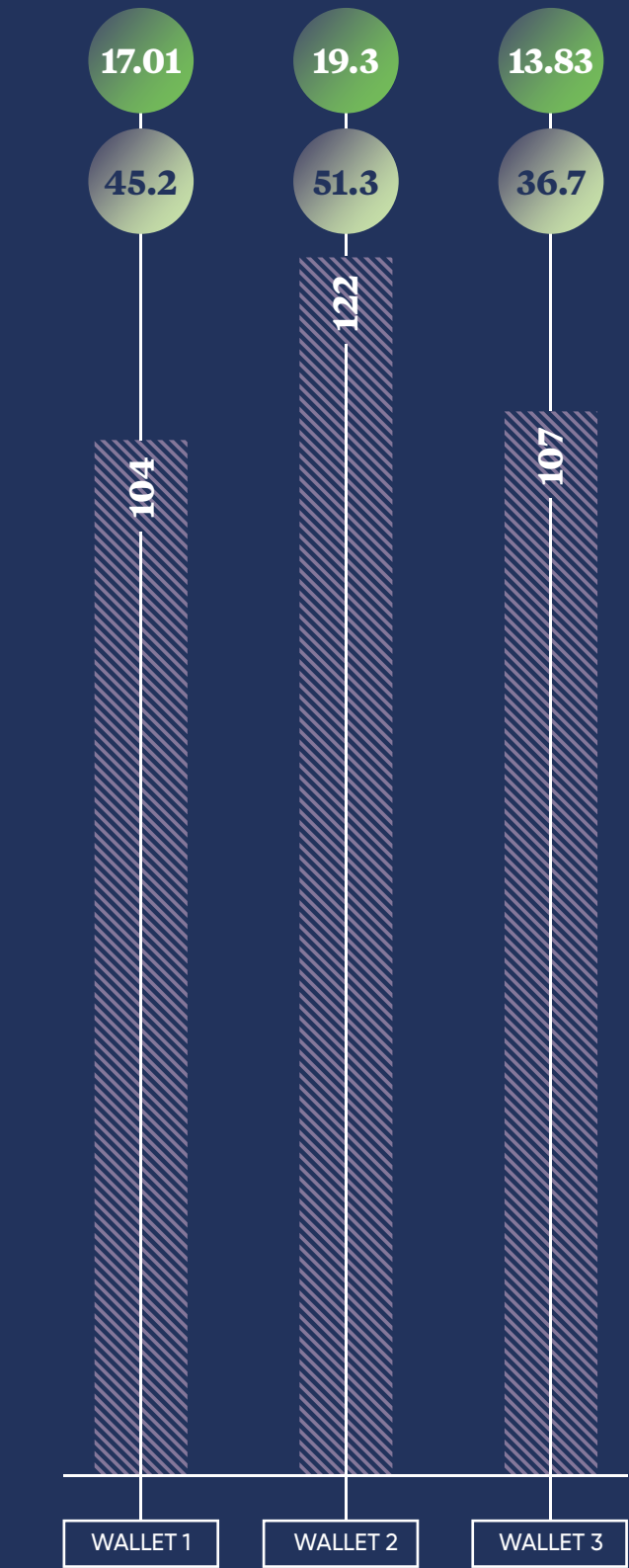


Datto 2016

TOTAL AMOUNTS PAID TO WANNACRY ATTACKERS

Balances of the three bitcoin addresses linked to the WannaCry ransomware up to May 25

● Balance in bitcoin ● Balance in \$k ▨ Total number of transactions

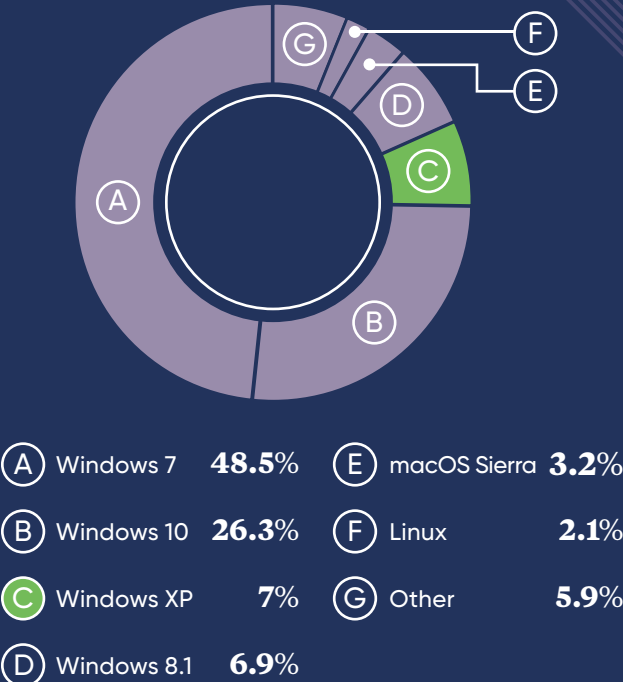


Bitref.com

GLOBAL DESKTOP OPERATING SYSTEM MARKET SHARE

APRIL 2017

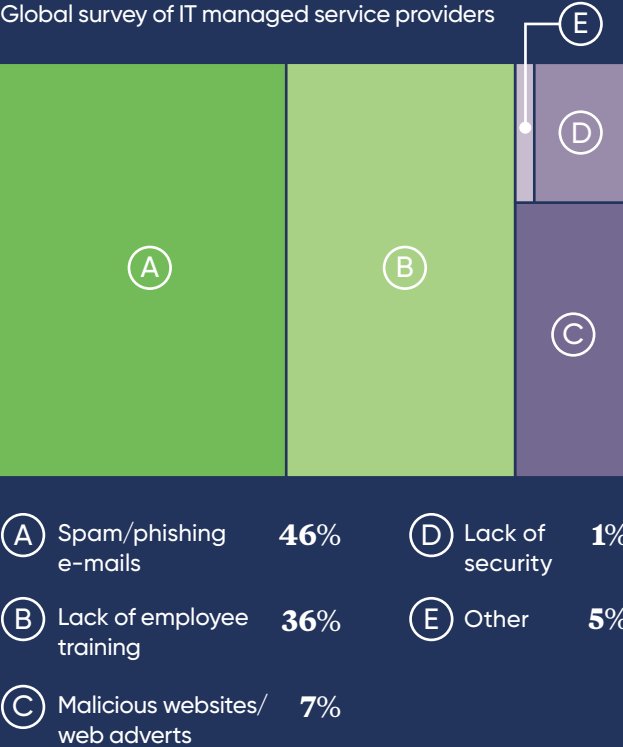
Millions of PCs still run on Windows XP, the third most popular desktop operating system worldwide



NetMarketShare 2017

LEADING CAUSES OF RANSOMWARE INFECTION

Global survey of IT managed service providers



Datto 2016

e heard of it now.  
across 150 countries  
world over have been

cs company Hitachi and  
r Nissan were both targeted

f the worst hit nations with tens  
ousands of computers affected

Kaspersky/BBC



176  
different file  
types encrypted

# GDPR, WannaCry, Incident management the list goes on...

At the ISF our consultants are working on solving these and others cyber security headaches, helping businesses handle today's security challenges with confidence

Unlike many other big consultancies our goal is simple – assess the problem, help you to resolve it and leave you with the ability to take it on from there.

We come in, do the work and get out again as quickly and as painlessly as possible. That's it. Job done.

Or, if you prefer, we provide customised, professional support to strengthen your organisation's cyber resilience and information risk management arrangements against emerging threats.

## What have we done recently?

We've had teams working on:

- > Identifying and protecting mission critical information assets in the retail sector
- > Developing roadmaps to EU GDPR compliance for financial services companies
- > Building cyber resilient frameworks that give you the how to on policies and procedures in manufacturing
- > And plenty more...

Visit the website and check us out or give us a call:

**Steve Durbin**

Steve.durbin@securityforum.org

+44 (0)778 595 3800

[www.securityforum.org/consultancy-services](http://www.securityforum.org/consultancy-services)



**Information  
Security  
Forum**



# Time for bosses to sit up and take notice

If C-suite executives continue to bury their heads in the sand, new European Union legislation will force them to take the threat of cyber attack seriously

DAVEY WINDER

The recent global ransomware worm, infecting more than 250,000 computers in 150 countries and as many as one in five of all NHS Trusts in the UK, is proof of the disruption that a cyber attack can bring to an organisation.

Nick Coleman, global head of cyber security intelligence at IBM Security, hopes that those in the C-suite can learn from the events of recent weeks and take the risk of cyber attack seriously. But here's the thing, why should it take such an event to get the C-suite sitting up and taking the cyber threat seriously?

Darren Thomson, chief technology officer and vice president at Symantec, says recent breaches have made it evident businesses of all sizes are failing to implement integrated, holistic security programmes.

"Organisations often claim to be keen to invest in data-breach prevention, but in reality, operating a standalone project does not solve the complex cyber-security challenges businesses face today," says Mr Thomson.



Screenshot of the NHS website when a ransomware attack disrupted health services on May 12

"Our *State of European Data Privacy Survey* revealed only 14 per cent of IT executives and decision-makers believe that everyone in an organisation has the responsibility to ensure that data is protected." What the other four out of five think should be seriously worrying to all organisations.

Brian Lord, managing director of PGI Cyber and the former deputy director of GCHQ in its intelligence and cyber operations division, blames "excessive scare sales tactics and incoherent advice over real focused business risk, supported by huge prices for solutions" for a C-suite decision-making paralysis. It's a paralysis often only broken by a breach.

David Emm, principal researcher at Kaspersky Lab, agrees that the board "needs to understand the core issues surrounding se-

curity and that there is executive buy-in to the measures needed to secure the company". This is, after all, what makes the job of the chief information security officer (CISO) so important. They act as a bridge between the board and the IT department.

How to engage at this level, then, becomes paramount. Quentyn Taylor, director of information security at Canon Europe, has a good point when he says to properly engage with the C-suite "you need to put the risk in terms they understand and

I've seen multiple breaches in the same organisation

that link to competencies they will engage with".

Martijn Verbree, cyber security partner at KPMG, agrees that it's all really about improved communication. "The board will often talk in business speak while the cyber team will talk in tech speak," he says. "Both sides need to know what is the organisation's risk tolerance, which things are top priority to protect and how well developed are the company's defences."

All this said, does becoming a victim usually lead to the implementation of security measures that should have always been in place though? Amanda Finch, general manager of the Institute of Information Security Professionals, says CISOs and security teams that have been through a serious breach are more confident in dealing with these occurrences and take a more flexible and pragmatic stance towards risk management and prevention.

"First-hand experience of crisis management helps to be better prepared to deal with future breaches both at CISO level and in the way they work with the board to set up the dependencies and information flows upstream," she says.

Greg Day from Palo Alto Networks sits on the UK National Crime Agency steering committee. Mr Day is adamant that any significant cyber incident should always lead to learnings and improvement; the question should be by how much? He says: "When an attack does get through and a business becomes a victim, the organisation must ask why didn't we see it quicker?"

However, this is not always the case. Dr Guy Bunker, senior vice president at cyber security company Clearswift, says: "I've seen multiple breaches in the same or-

ganisation, so evidently what they do after the first breach is not always enough to drive up security to prevent the second and subsequent breaches."

So what is enough? While there is no cyber-security silver bullet, Bharat Mistry, principal security strategist at Trend Micro, has put together a checklist of essential threat mitigation options:

**01** Make sure cyber security is a board-level concern, and cyber risks should be reported and treated as any other business risk.

**02** Cyber security is not just the responsibility of the IT department; stakeholders from all areas should be involved.

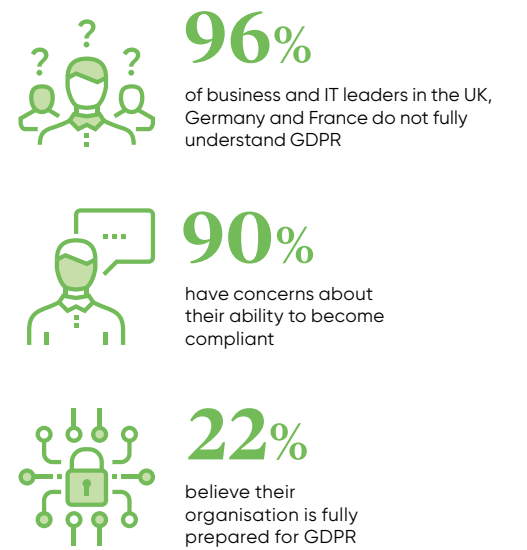
**03** Undertake a cyber-security maturity assessment to identify holes in your current cyber-defence strategy and initiate a programme to remediate; this is not just a technology problem, it's having the right skills and processes.

Terry Greer-King, director of cyber security for Cisco UK, Ireland and Africa, thinks the whole debate could soon become moot anyway, courtesy of the European Union General Data Protection Regulation (GDPR).

"If a cyber attack doesn't get leaders to sit up, GDPR will force them to," he says. "Data breaches of the most important provisions could lead to fines of up to €20 million or 4 per cent of a company's global annual turnover."

Indeed, GDPR specifies that organisations have to appoint a specific data protection officer, who is distinct from a risk officer and all IT functions that currently exist. "It's a role that has to sit outside IT and outside the boardroom to have the independence to ensure the business adheres to the regulation," Mr Greer-King adds. ●

**BUSINESSES UNDERPREPARED FOR GDPR**  
GENERAL DATA PROTECTION REGULATION TO COME INTO EFFECT IN MAY 2018



Symantec 2016

INSIGHT

## SOFTWARE LIABILITY



Dave Clemente, senior manager at Deloitte cyber risk services, says you can forget about phishing and ransomware; the next big thing in cyber risk will be the introduction of software liability requirements for developers and manufacturers of connected systems, such as medical devices or driverless vehicles.

"The two worlds of safety and security are rapidly overlapping, increasing the risk that insecure systems will be hacked and result in injury or worse. Where safety is concerned, the legal considerations around software take on a new level of importance," he says.

"When this happens it will undoubtedly make headlines and receive intense public scrutiny, turning up the regulatory heat on software developers. This may raise the cost of software, delay innovation and disrupt the open source community, but will be worth it to ensure public trust is maintained and increase the reliability of critical software and services.

"Cyber-physical systems aren't just pacemakers and robots, but include everyday systems that are used in homes, offices and public places. Software liability is coming and many sectors could be impacted."



## TRANSPARENCY



David Henderson/Pictoir



People working on the ground are uniquely placed to comprehend and communicate the specific threats they face

# Find clarity in a world of unknowns

In a changing environment, only open communications, decision-making and protocols can steer organisations away from damaging events. But how do you ensure a high level of transparency across your business?

DAN MATTHEWS

On April 18, prime minister Theresa May announced a snap general election. On May 11 recruitment website Hired.com published figures suggesting that the UK's foreign technology talent pool, which draws heavily on workers from the European Union, has halved since the June referendum last year.

The following day, on May 12, a computer virus was unleashed which spread quickly across the world, crippling corporate systems and, in the UK, disrupted NHS networks.

These events and hundreds more show how, in the space of a few short weeks, the business environment can alter radically. Seismic events happen suddenly or can percolate gradually and in a connected world the impact is often widespread and profound.

Risk strategies have moved with the times. The best ones are fluid, agile and incorporate the understanding that threats appear with a regularity you can depend on. Small businesses, as well as corporates, understand this and on the whole attitudes to risk have matured.

A crucial part of an organisation's defence is its workforce's alertness; people's ability to contain risk and move decisively should something unforeseen happen. A crystalised strategy is one thing, empowering people to act is another.

Transparency, then, is all-important. It is a buzzword thrown around by C-suite executives, but in private some underplay its significance, says Stephen James, partner at law firm Clarkslegal.

"Risk management must be more than a box-ticking exercise. Organisations at the centre of recent corporate scandals had risk structures in place, but they were

not followed in practice," he says. "There must be allocation within the organisation for primary responsibility for risk management and from this central point must flow a clear chain of responsibility, to cover risk across the entire organisation."

Kevin Lester, managing partner at Validus Risk Management, believes the number of out-of-the-blue threats, so-called unknown unknowns, is growing in the current climate. The situation requires a highly developed strategy with multiple touchpoints across the organisation.

Creating such a strategy begins with setting out clear objectives that everyone can understand, incorporating company goals and appetite for risk. This is to be enshrined in a formal policy, but must also flow informally through the organisation's culture.

Risk management should have a strong link to the commercial strategy with areas of responsibility given to individuals who are charged with "owning the risk". These individuals must be equipped with the resources and power to manage change.

Top executives should create mechanisms for risk reporting up and down the chain of command. Risks must be reported in an intuitive way and qualified where possible, says Mr Lester. Lastly, cost-benefit must be measured and reported regularly, to gauge whether the system works and is value for money.

Val Jonas, chief executive of Risk Decisions, agrees each organisation's risk profile should be embedded rather than offered up as a fringe exercise. In particular, she says it's vital for individuals to be clear on how much risk the management team is willing to take.

"Build this into your risk management targets and establish the mitigated level you need to achieve for your risks. This includes not over-managing risk that might be beneficial. After all, companies are in business to take some risk to max-

imise their returns," she says.

"In large organisations, each division, department, business unit, functional area, programme and project team will tend to have its own identity. So the challenge is to combine those identities together into a shared, holistic organisational culture."

In essence, transparency means imbuing an organisation to enact change. Those with well thought out risk procedures will nevertheless blunder into problem areas when a crisis looms unless people in the right areas are kept abreast of policy and feel confident acting on initiative.

Business throws up a vast tapestry of risk and managers at the very top of the chain have neither the time nor the competence to keep it all in check. People working on the ground are uniquely placed to comprehend and communicate the specific threats they face.

Each department – finance, human resources, marketing, IT – has a different profile. People in charge must recognise the fact and open channels

of communication so information can flow freely, says Emma Carr at law firm Gowling WLG.

"At senior management and board level, an organisation must be clear and transparent about risk strategy and governance, provide adequate oversight and be accountable for risk management practices," she says.

"At an operational level it is key that those risk management practices are implemented and adhered to, regularly monitored and regularly appraised with results fed back up the chain."

This structure's importance is summed up in the so-called Noah Rule coined by the world-renowned investor Warren Buffet. It states: "Predicting rain doesn't count. Building arks does." At the end of the day, execution is everything.

"A risk strategy is only as good as the organisation's ability to act upon it," says Campbell Macpherson, author of *The Change Catalyst*.

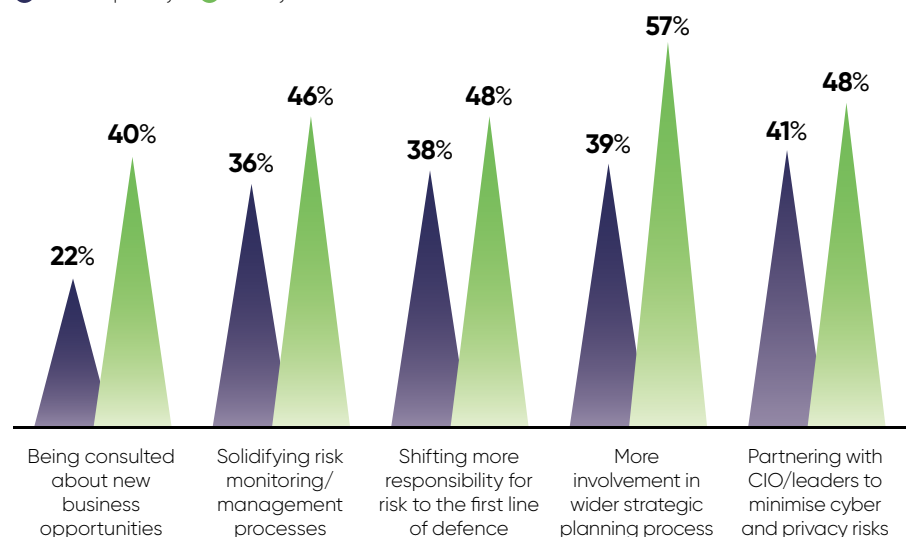
"Execution risk is arguably the greatest risk of all, because without the ability to implement, the most comprehensive risk strategy is not worth the paper it's written on. Your ability to execute will boil down to the capability of your people and the culture of your organisation," he says.

By empowering employees, organisations can insulate themselves from the nasty surprises that block progress. Conversely, by walling up responsibility for risk prevention, the C-suite deny themselves a robust defence against the future's volatility. ●

## CURRENT AND FUTURE PRIORITIES FOR RISK LEADERS

GLOBAL SURVEY OF GLOBAL CHIEF RISK OFFICERS

● Current priority ● Priority for next 18 months



Robert Half Management Resources 2016



# 'Boards should explore ways to bring risk evaluation into all aspects of the business and build agility into management culture'

JOHN HURRELL  
Chief executive  
Airmic

The boardroom approach to managing risk has been transformed over the past decade. Risk management is now firmly on the C-suite agenda and is increasingly recognised as central to a successful business.

And yet despite this, time and time again, businesses are finding themselves exposed by a crisis, often resulting in significant financial and reputational damage.

Very often, it is not the event itself that causes the most harm, but the response of the organisation. Crises unfold and enter the public domain with terrifying speed. This is one of the defining changes in risk management in recent years, but most executive teams are still failing to react quickly or decisively enough when a threat or incident emerges.

What is going wrong? Most traditional risk governance and identification processes presuppose that the operating environment is relatively stable, predictable and slow moving. The typical focus for risk mapping and planning is therefore on compliance and rigour. Boards might visit their risk register on a quarterly basis or review their risk management procedures once a year, for example. The result, however, is that board-level engagement with risk management is based only on a series of snapshots.

This unfortunately does not reflect real life. Worse still, it can result in a false sense of security as organisations feel they have risk management covered. Compliance and structured risk mapping are important, but will not equip boards to deliver an effective real-time response when a crisis unfolds.

Take, for example, the incident in April when a passenger was filmed being dragged off an overbooked flight. Within hours, the video was shared globally via Twitter to widespread criticism and even calls to boycott the airline. The chief executive's initial decision to defend the actions followed by a belated apology only fanned the flames, and made the leadership look indecisive and insincere. Within hours, the organisation was facing a legal battle, a tarnished reputation and a drop in share price.



Ten years ago, this event would probably not have even surfaced, but today social media lays bare corporate shortcomings in an instant. Board leaders will be asked for instant responses and will need to appear prepared, transparent and in touch with both their business and the expectations of their stakeholders, including the public.

Most boardrooms today are not empowered with the right risk knowledge to respond effectively in this pressure-cooker environment – what is missing for so many is agility. Instead of receiving static risk information at predetermined intervals, boardrooms need to view risk as a series of continually evolving threats, any of which could erupt at any moment. It is therefore essential that senior management have the information and rehearsed crisis plans to respond quickly.

Moreover they must have the authority and understanding to adapt those plans as needed. According to one of Britain's most experienced generals, Sir Richard Shirreff, some boardrooms are now looking at how the military handle fast-moving crises and how they rapidly switch gears when the situation dictates. According to Sir Richard, on the front line, as in business, you can never predict the future or control chaos, you can only adjust strategy to take into account unforeseeable events.

None of this is easy, but boards will have a significant head start if they continually have a finger on the risk pulse of their organisation and operating environment, even when it feels benign. Boards therefore should explore ways to bring risk evaluation into all aspects of the business and build agility into the management culture of the organisation.

This requires a different way of thinking because it is about culture as much as processes. But the rewards are clear. Research by Airmic has shown that an ability to adapt and respond quickly to a changing environment is a key pillar of a resilient business. Too many company directors think it will not happen to them, but it could happen today and in a matter of hours.

# Strengthening business resilience in our turbulent times

From the security incidents of recent days and weeks to natural disasters and medical emergencies, employee safety and security is never far from anyone's minds



The need to prepare, protect and assist employees whenever and wherever needed has never been more evident.

Not only is it a duty of care for any organisation, and increasingly has potential legal implications if employees are not appropriately protected, it is also high on the agenda to help business continuity planning and strengthen business resilience through a protected workforce.

Rob Walker, security expert at International SOS, says: "Security events have resulted in a sense of increasing challenges, even in travel to places once thought secure. While risks are changing, organisations must ensure their actions to mitigate those changes are proportionate, and based on reality and not perception.

"With many organisations increasing their business travel activity,<sup>1</sup> it is essential for decision-makers to be able to communicate that objective advice to their people, including in an actual crisis. Keeping informed and taking into account all risk factors will enable business travel to proceed successfully, resulting in a protected workforce and business continuity."

Travel risk professionals have told us the biggest challenges that organisations face in protecting their mobile workforce are education about travel risks, communication during a crisis and tracking travellers.<sup>2</sup> These are

vital elements to keeping your workforce safe and an indication of what is preoccupying managers.

They also indicate something else as managers are in danger of being drawn into details that could be addressed more efficiently; time spent tracking people down and trying to communicate could be reduced to make additional time for addressing the bigger picture.

We know travel risk professionals are often multi-tasking across a number of business objectives and that risk responsibilities are shared across an organisation, so co-ordination and identifying responsibilities is essential, whether that is managing additional staff for a business objective or ensuring corporate data is protected. The impact of this is, of course, amplified during a major crisis, such as an extreme weather event or a terrorist attack which could affect a number of personnel rather than an individual.

So how do you save the time you're losing? It all comes down to something that may be commonly known, but is often not prioritised, putting in place an optimum business continuity plan for business resilience in a crisis.

Business continuity planning can be complex, so the effort of building and maintaining it can be daunting, but is essential, looking after your people, managing client relationships and not just protecting your reputation, but enhancing it by embodying good practice. There are some simple steps that any organisation can take.

## TOP TIPS TO IMPROVE RESILIENCE Think ahead: how will you respond?

Think through likely scenarios and review appropriate sources such as a risk map ([www.travelriskmap.com](http://www.travelriskmap.com)). You probably have previous experience you can draw on too. What was best practice? What are the likely pitfalls? What happens if you or your immediate team are unavailable?

Educate your managers on what they need to do. Remind people of the role they need to play. Protecting your workforce is everyone's responsibility, but you cannot assume people will take this on intuitively. Spend time creating awareness and support so your managers feel a sense of ownership. This gives you more help to draw

on and, if your people have a duty of loyalty, they will help you too.

## During an incident: track, communicate, assist

Set up a system that will alert your people. Make sure you have a traveller tracking tool in place that will do the bulk of the work for you. You should also think about how and when you will get a message out to your whole organisation.

Work out how you will check your people are OK. It is essential to have this linked to your traveller tracking tool, to ease the overall management of what's happening. Ideally you will get the message out through two-way communication to improve the response rate.

Have a back-up plan in case you can't manage the crisis alone. Even the best organisations may be out of their depth if the worst happens. You will need a solution that can emulate your role if you are not in the office. One option is to nominate alternatives; another is to outsource the checking process completely.

## The wash up: template your management reports

This is simple but very important if you want to show you are in control of the situation. Setting up a report template will help you communicate to your leadership and give you all piece of mind. Once again, hooking this into your traveller tracking tool will mean you can report and communicate in a matter of minutes.

Flexible response templates are key, enabling fast modification in a crisis, from cyber security incidents to national political upheaval.

Be prepared to support and protect your workforce with unparalleled advice and assistance. Travel risk management tools and services are key in helping organisations protect their mobile workforce in the most efficient way and mitigate risks to strengthen business resilience.

For more information please visit  
[www.internationalsos.com](http://www.internationalsos.com)

<sup>1</sup> Talent Mobility 2020 and Beyond, PwC

<sup>2</sup> International Travel: Risks and Reality: The New Normal for Business is an Ipsos MORI research study conducted among 1,119 business decision-makers across 75 countries. Research was conducted online using representative panels, October 6-26, 2016

## BIGGEST CHALLENGES TO PROTECTING TRAVELLERS FACED BY ORGANISATIONS



49%

Educating employees about travel risks



47%

Communicating with employees during a crisis



42%

Tracking employee travel

# How data analytics is reshaping risk management

For data analytics to help improve risk and insurance processes, companies need clearly defined goals and a single claims platform, says **Van Ameyde**



**D**ata, data, everywhere – industries across the globe are now swimming in the stuff. The risk management and insurance industry is no different. Many of us are aware that data should be put to good use, processed and interpreted intelligently, but the burning question for most corporations and insurers is how?

The customer service industry is awash with examples of how consumer data is used effectively to personalise experiences, brands and product offerings. However, practical examples for the risk management and insurance industry are harder to find.

"Big data should be a key tool for our industry, but it's become a nightmare," says Willem van der Hooft, business development director at Van Ameyde, a Europe-wide company that has been working on claims management solutions since 1945.

"It's one thing to collect and interpret as much data as you can get your hands on, but to do it in a way that makes a difference to your business goals is the challenge. End-to-end digitisation helps. The more the claims process is digitised, the more data you have available, the more insight you will have for risk management and market segmentation."

Van Ameyde is at the forefront of the revolution in IT-driven claims and risk-related services, successfully modelling analytics programs for risk managers and insurance providers. The company has found that data analytics serves many purposes with respect to claims. For instance, loss statistics allow companies to identify repetitive causes. Once these are solved you can reduce their frequency and save money in the process.

"This requires complete insight into all losses wherever they occur," says

Mr van der Hooft, whose company has 46 offices in 28 countries. "The same goes for more sophisticated predictive risk models. You need a complete and consolidated data set you can mine for information."

That's why Van Ameyde set up its pan-European Incident Management System (IMS). This is a platform that all Van Ameyde's customers and their suppliers are connected to. The aim is to process data from all incidents across Europe, at scale, in a uniform way. Information ranging from losses to policies and customers' personal details is logged.

"IMS is empowering industry players' insight to make informed decisions. This system is also the foundation for our analytics capabilities,"

“The insurer could take on a new role as the policyholder's risk manager offering advice to reduce claims



360° insight in claims and risk

says Ruben Snepvangers, data analyst at Van Ameyde.

Van Ameyde has created a predictive risk model for a multi-national car hire company. The results are to be used in the company's pricing strategy, including insurance premiums offered to clients.

"We've created a model that encompasses losses relating to age, car model, insurance cover, days hired and location. Despite limited sample sizes and data points, predictions using this model are correct in 70 per cent of cases. When segmenting low and high-risk customers, the model had an even higher success rate," says Mr Snepvangers.

Van Ameyde found that the key to designing a successful predictive model involved setting clear goals. "We asked our client the question what exactly do you want to achieve? A clearly defined end-game makes all the difference when determining what information to use in the analyses," Mr Snepvangers explains.

Risk profiles are also used in the insurance industry. This enables insurers to segment consumers based on their desirability and design customised solutions. It involves using enriched customer profiles, which are based on policy details, insurance application information and any claims someone may have had. All this data is used to build up a detailed picture of each customer.

The type of insurance policies each of us takes out tells us a lot about our respective lifestyles. If you combine claims and policy information you can see that there's a connection between risk appetite, defined by the level of insurance taken out, and the actual risk posed, defined by the number and extent of losses. Profiles can now be enriched further by additional information that's available from voluntary sharing schemes such as car telematics.

"We tend not to speak of big data because we don't actually use all the data available. While customers may be willing to share data if they see substantial benefits, such as lower insurance premiums, sensitivity over privacy is crucial," says Mr van der Hooft.

"In some European countries, it's perfectly acceptable to use social media to detect fraud, but in others it's against the law. Mining data from social media for marketing segmentation purposes, even if it's legal, may still raise eyebrows among some potential customer groups. A voluntary survey may work just as well."

Detecting fraudulent inquiries is also a big industry issue. Van Ameyde now uses machine-learning algorithms. These improve the company's ability to detect fraud, but they also predict possible deceitful behaviour. All this information is then fed back into the analytical model.

Creating risk profiles for certain customer groups also allows accurate market segmentation and the design of more personalised services and pricing schemes. Take safe-driving and usage-based schemes for motor insurance, these have paved the way for more accurate tariffs for motorists.

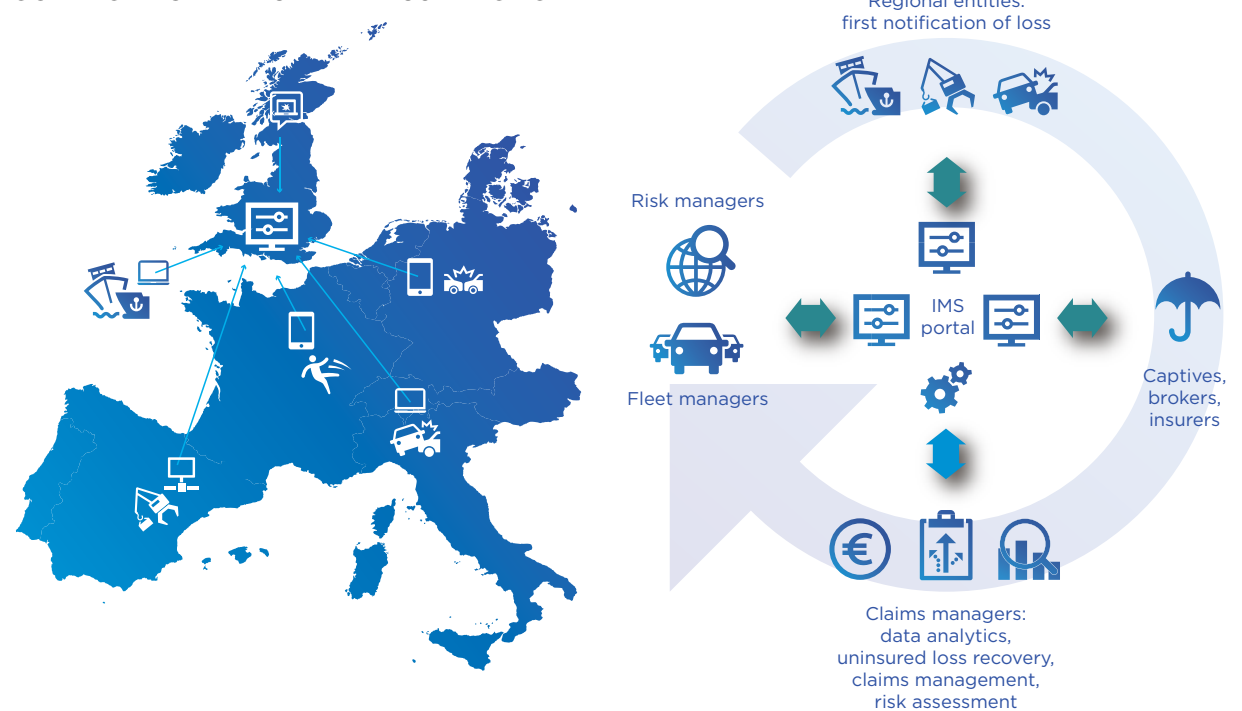
Van Ameyde believes there is more the industry can do with risk profiles. The insurer could take on a new role as the policyholder's risk manager offering advice to reduce claims.

"Take those people who live in flood-risk areas, they could be advised to adopt measures at their property that will increase flood resilience and at the same time reduce their premiums, such as raising thresholds, putting in airbrick covers or storing expensive household items on the first floor rather than in the basement," says Mr van der Hooft.

"In the risk management industry, the accuracy of pricing hugely impacts the risk transfer strategy. Get it right and both risk managers and their insurance providers benefit. The key to all this is information. If data is structured, centralised and reliable, you can make comprehensive risk assessments. You will also have a complete picture of the losses incurred throughout the company. This is the basis for a robust pricing, risk mitigation and risk management strategy."

**To find out more call in at booth 29 at the Airmic 2017 conference or visit [www.vanameyde.com](http://www.vanameyde.com)**

## CONNECTING THE RISK AND INSURANCE CHAIN





REPUTATIONAL DAMAGE

# Don't make a disaster out of a crisis

United Airlines soared into world headlines for the wrong reasons and not only crashed their public relations but also burnt their reputation

CHARLES ORTON-JONES

Airlines are accustomed to examining incidents to learn lessons. This year the big lesson is nothing to do with flying, but how to cope with the fallout from a public relations disaster.

The United Airlines passenger fiasco was front page news for a week and has gone down in history as a textbook example of what not to do.

The event was brief. United needed to fly four staff from Chicago to Kentucky and wanted to bump four passengers to make room. Three complied with the request. One did not. David Dao sat tight.

The 69-year-old doctor explained he needed to see patients the next day at his clinic in Kentucky.

Dr Dao was forcibly removed by security officers, suffering multiple injuries including a broken nose and two broken front teeth. The chaotic scenes were filmed by passengers and uploaded to social media, and viewed seven million times in a day.

So far, so bad. Then it got worse. United chief executive Oscar Munoz issued a begrudging apology, blaming "over-booking", an inaccurate claim. American talk show host Jimmy Kimmel spoke for millions when he said: "That is such sanitised, say-nothing, take-no-responsibility, corporate BS speak."

Rumours circulated about Vietnamese-American Dr Dao being selected for his ethnicity. Emirates airline launched a parody ad campaign. A poll three days later of 1,900 people said 79 per cent who'd heard of the incident would chose a non-United airline. The affair had spiralled out of control.

The PR industry is now obsessed by the incident because it's such a perfect case study. The impact of poor reputational risk management can be seen in glorious detail.

What are the lessons? The first is that the initial reaction is critical. Tim Bond, group head of PR at the Direct Marketing Association, singles out United's atrocious first apology as the catalyst. "When that story broke, imagine the change in tone if the CEO had come out immediately and said, 'This shouldn't have happened. We're going to stop the practice of over-booking flights so this never happens again.' How different the subsequent media storm could have been, but how different the business's bottom line too," says Mr Bond.



When disaster strikes the impact can be crippling

A dose of human sympathy helps. Holly Underwood, crisis communications lead at Access London, advises: "Be personal in your response; especially on social media the most important thing is to not ignore what is happening. If the public are asking questions, try to respond. Even if you don't necessarily have all the information yet, letting them know you are listening is the first step to rebuilding trust."

Words must be matched with action. The problem needs to be fixed. United didn't get on top of the story until it promised to hike compensation for removing pas-

sengers and to lower over-booking to reduce incidents.

A major incident on a roller-coaster at Alton Towers theme park is often cited as the correct way to handle a potential PR disaster. Anokhi Madhavji of crisis management company PLMR says: "The Alton Towers chief executive was quick to issue a statement that was genuine, warm and compassionate. He apologised to victims and their families."

Mr Madhavji adds: "A highlight for me was when he was asked about how the incident would affect the share price of the company. He responded, 'You'll forgive me if I'm not really focused on the share price at the moment.'"

Above all, reputation management needs focus. United made mistakes early on by not getting PR officials to verify the details of the story. United then needed to apologise for the resulting errors in its statements – a nightmare scenario. The company should have realised the scale of the problem and devoted more resources to it.

When disaster strikes the impact can be crippling. FTI Consulting recently examined 100 high-profile PR catastrophes, such as the VW emissions scandal and Talk-Talk's hacking disaster, in a report called *Anatomy of a Crisis*. The report shows that 23 per cent of companies never recovered their pre-crisis share level and 14 per cent went out of business.

Where there is malpractice, the impact is far larger. A financial mismanagement story generates 44 times normal press coverage levels, a cyber breach just seven times and a product recall less than four times. The public aren't stupid; they know when a company is malicious or just a bit dozy.

Demonstrators at Chicago O'Hare International Airport last month

Naturally, not all incidents will explode like the United story. It was a rarity – a perfect storm.

"Business leaders and PRs are often guilty of mistaking the media's agenda with reality," warns Paul MacKenzie-Cummins, managing director of Clearly PR. "You can't allow others to set your agenda and to do so could see the hole you are in grow wider and wider."

In lesser cases no action may be the best action. "There are times when a rapid response is called for, and inci-

dents when it's best to simply warm your hands on the fire and let the flames subside naturally," says Chris Gilmour, director at Beattie Communications. "Often you'll be pleasantly surprised that the expected scorch marks don't appear and attention is then dragged elsewhere."

The United incident is fascinating because it's so unlikely. The next 99 times out of 100 there's a kerfuffle nothing will happen. It's why risk management is such a tricky business. ●

## INSIGHT HOW TO HANDLE A MEDIA STORM



"Put the kettle on. Don't panic. Employing a knee-jerk reaction by just distributing an ill-considered public statement in the heat of the moment can do more harm than good without considering the subsequent ramifications."

**CONNOR MITCHELL**  
Labour Leave EU campaign press office co-lead

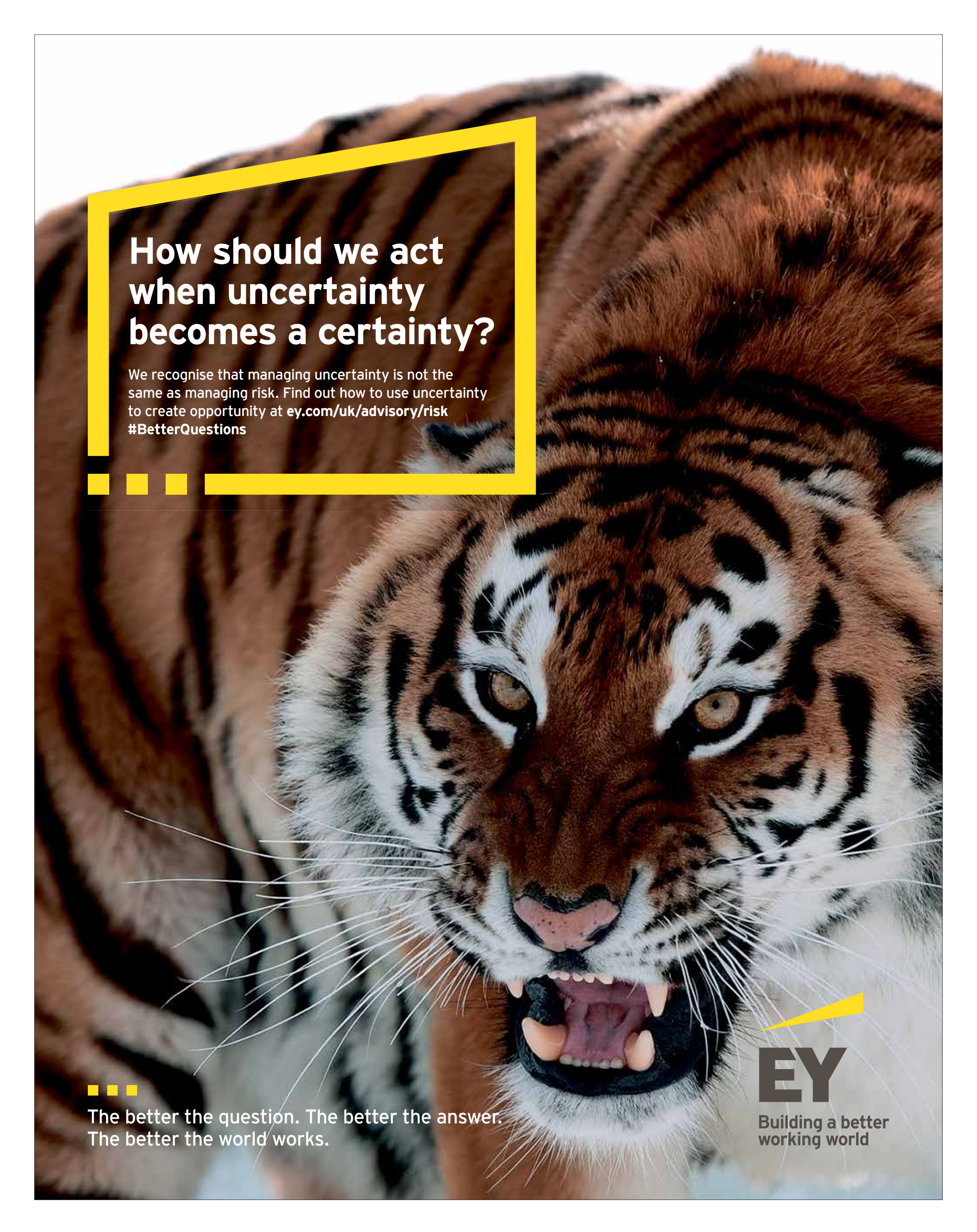
"With the exception of genuine villainy, most disasters fade away: consumers' outrage about high-profile tax avoiders, corporate bullies or those engaged in financial shenanigans almost never amount to much. Put simply, for almost all of us, a crisis exposing behaviour we don't like isn't enough to make us change our ways."

**NICK BISHOP**  
Golin PR head of corporate communications

"PR disasters are vastly misunderstood. They are not quick events; they happen slowly. A couple who haven't communicated well for a long time and have begun to drift apart years ago can apparently be destroyed by a very minor tiff. But it's not the tiff that did the damage; it's the prior lack of attention or perhaps a complacency creep. Likewise, company reputations usually die slowly before they're pushed over the edge."

**LIEF SCHNEIDER**  
Chief executive of reputation consultancy SBC London





# How should we act when uncertainty becomes a certainty?

We recognise that managing uncertainty is not the same as managing risk. Find out how to use uncertainty to create opportunity at [ey.com/uk/advisory/risk](https://ey.com/uk/advisory/risk)  
**#BetterQuestions**



The better the question. The better the answer.  
The better the world works.



**EY**

Building a better  
working world