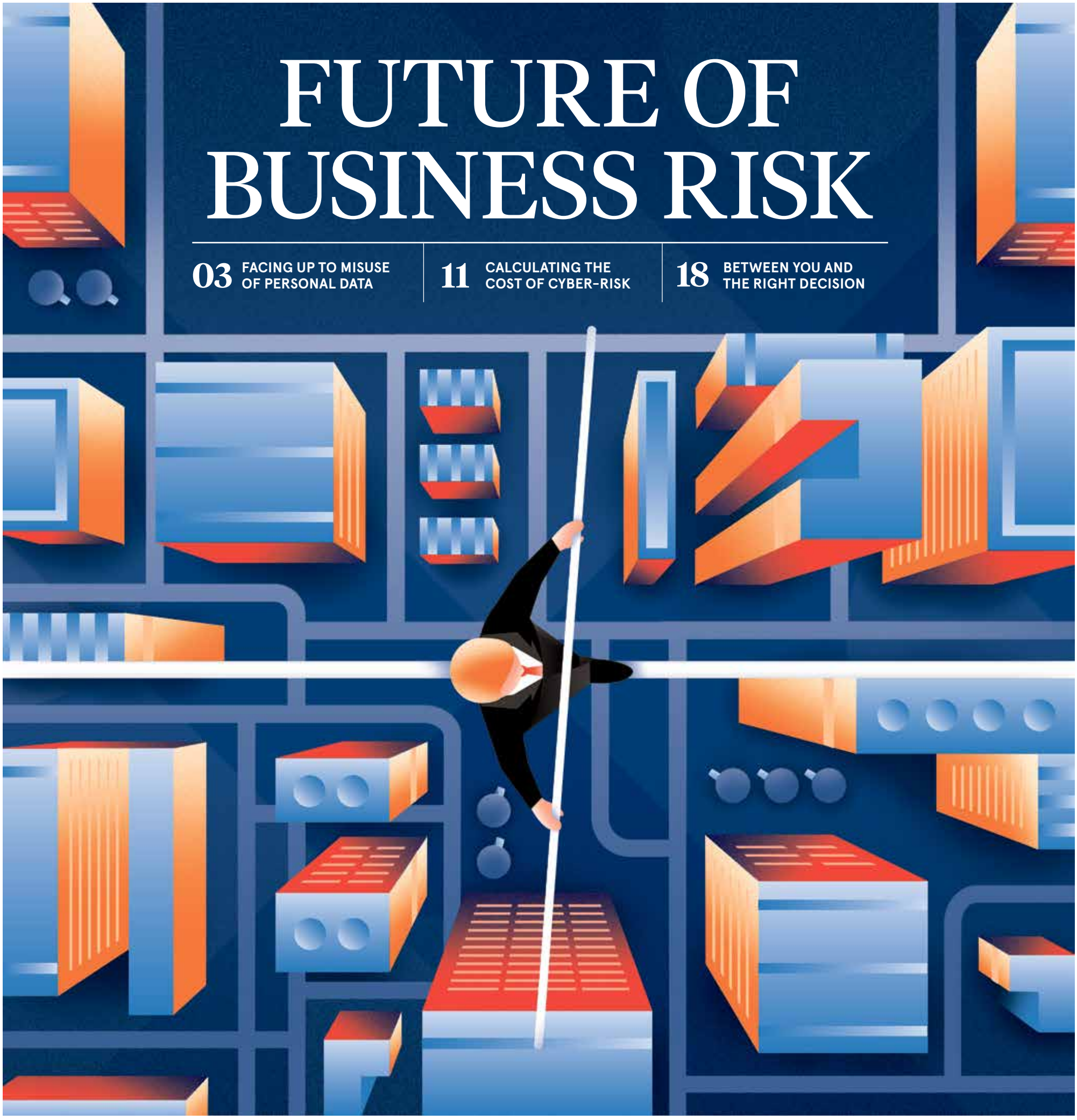
FUTURE OF BUSINESS RISK



Adapt to evolving Integrated Risk Management needs

Take confident action on critical challenges with a consolidated, enterprise-wide view of risk.

Rely on Thomson Reuters Connected Risk to manage and mitigate risk with confidence by utilizing internal and external data more effectively. Organizations benefit from a holistic enterprise-wide view of risk through advanced mapping and an extensible interconnected data model underpinned by streamlined workflows.

With Connected Risk, organizations are able to make informed decisions with greater ease and efficiency, delivering a focused view of their risk, compliance and audit landscape.

Discover more at: **risk.tr.com/connected-risk**

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

FUTURE OF BUSINESS RISK

Distributed in THE TIMES

Published in association with airmic

raconteur reports

Publishing manager
Reuben Howard

Production editor
Benjamin Chiou

Managing editor
Peter Archer

Head of production
Justyna O'Connell

Digital content executive
Elise Ngobi

Design
Samuele Motta
Grant Chapman
Kellie Jerrard

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 email 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

@raconteur /raconteur.net @raconteur_london

raconteur.net /future-business-risk-2018

CUSTOMER DATA

Facing up to misuse of personal data

Facebook's fracas over misuse of its users' data may signal a fundamental rethink of how customers' personal information is treated online

BRIAN GROOM

The 21st century has so far proved a risk-strewn environment for big companies. Facebook's crisis over misuse of user data can be added to the list of corporate disasters such as BP's Deepwater Horizon oil spill, which almost ruined the company, and Volkswagen's diesel emissions scandal.

The world's biggest social network has struggled to overcome concerns about privacy, the spread of "fake news" and political manipulation, particularly since the revelation that Cambridge Analytica, a UK analytics company, may have improperly obtained the data of up to 87 million Facebook users. Facebook's share price took a beating, some users deleted their accounts and regulators paid close attention, raising the prospect of new restrictions.

Facebook's travails are larger in scale than most corporate crises, but the company is far from alone. The stream seems endless, whether it is the Harvey Weinstein scandal, exposing sexual abuse that went way beyond the entertainment industry, or credit-checking agency Equifax's data breach, affecting more than 145 million people in the United States alone, or quality assurance disasters that have hit Japanese manufacturers such as Kobe Steel, Nissan and Takata.

Company chiefs seem confused by the range and complexity of business risks, unsure which are the most serious and what they can do to guard against them.

Business interruption and cyber incidents come top in Allianz's latest annual survey of risks, while surveys by Aon and others have found the risk of reputational damage to be the main concern. Political risk, such as the danger of a US-China trade war threatening supply chains, has also jumped up the scale.

Yet Aon found in 2017 that risk preparedness was at its lowest level since 2007. "With the fast speed of change in a global economy and increasing connectivity, the impacts of certain risks, especially those uninsurable ones, are becoming more unpredictable and difficult to prepare for and mitigate," it says.

Facebook's problems combined an operational vulnerability – unauthorised use of customer data – with the explosive power of social media to amplify reputational damage. "We use to talk about the 'golden 24 hours'," says Anthony Fitzsimmons, chairman of consultancy Reputability, referring to management's window for trying to control a difficult situation. "Now it's about the 'golden 24 seconds'. It's almost impossible to control it."

Al Drago/Bloomberg via Getty Images

Facebook chief executive Mark Zuckerberg testifying before the Senate Judiciary and Commerce Committees in Washington

The Facebook crisis is notable because it may have long-term repercussions that threaten its fundamental business model: selling personal data to advertisers, which allows them to micro-target their message to customers. If regulators restrict the way data can be harvested, Facebook may find it harder to make profits.

Has the company simply misread what its customers will tolerate and misunderstood its role in society? André Spicer, professor of organisational behaviour at London's Cass Business School, says Facebook's social contract with users – "you give us your data, we give you online services you like for free" – seems to be weakening.

"Users are asking whether they want to give away data. Now Facebook will need to ask how much of its services it gives away for free. Alternatively it will need to ask what a new social contract with users might look like," says Professor Spicer.

He adds that Facebook's response was too slow. "It took a week to do the basics of crisis management: say what happened, acknowledge their role in it, say sorry, then tell us what they are going to do about it."

Christopher Williams, reader in management at Durham University Business School and author of *Venturing in International Firms*, says the affair carries wider lessons for companies that collect user data and share it with other organisations. "The service attributes that companies develop and use to reassure users that 'we will not exploit you or insult you' are critical and determine winners from losers," he says.

Dr Williams adds that Facebook "has an opportunity now to show that it has learnt from the episode and can take a true leadership position in the industry on issues around user trust". That should include transparency and clear communication about how external organisations may access and analyse user data.

Companies can usually survive crises, but occasionally they prove fatal. The Enron scandal destroyed accountants Arthur Andersen, while construction and outsourcing company Carillion collapsed this year as a result of problems with public-private contracts.

Studies suggest the rate at which big companies are disappearing or losing their independence has speeded up, driven by deregulation, competition from emerging markets and technological change. The British Standards Institute, which has clients in 193 countries, says resilient companies are defined by strategic adaptability, agile leadership and robust governance.

Mr Fitzsimmons, co-author of *Rethinking Reputational Risk*, says: "Most crises are essentially system failures. Even if particular crises are hard to predict, the systemic weaknesses that cause them can be found and fixed before a crisis happens."

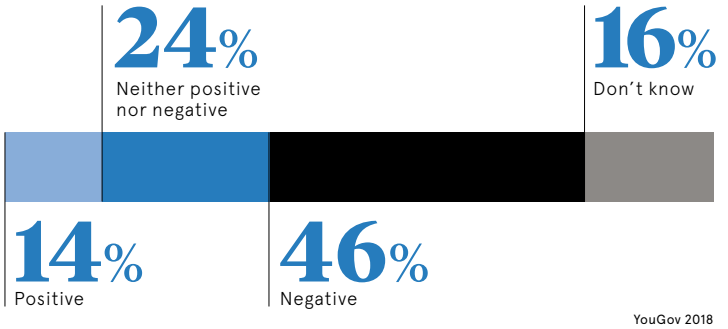
In many cases, insiders are aware of a company's weaknesses, but the message does not get through to leaders or warnings are not heeded. Sandy Parakilas, who was responsible at Facebook for compliance and data protection for apps from 2011 to 2012, claims he had warned the company that it was losing control of data to third-party developers.

Mr Fitzsimmons says companies should carry out crisis planning, including having "a leader who is trained and has the guts to go upfront if necessary". They should also analyse where threats might arise, if necessary with outside help. One problem is that "when you talk to leaders, they readily accept that bad stuff might happen, but they think it only happens to other people", he says.

Too often, leaders have fragile self-confidence, making them over-sensitive to internal criticism and reluctant to heed warnings. The best ones have "self-confidence sufficient to have room for humility", Mr Fitzsimmons says, so they can take and welcome criticism. ◆

Social media platforms face a shift in sentiment

Public opinion of whether social media has a positive or negative effect on society overall



YouGov 2018

Commercial feature

Real-time monitoring essential to commercial risk management

Businesses are piloting new monitoring technologies, reshaping how risk is assessed and enabling highly accurate underwriting

A revolution in data is enabling insurers to predict risk precisely, empowered by businesses' digital footprint gathered from property and operational monitoring systems. Insurers can also use the technology to identify trends and help clients prevent accident "events", reducing the frequency and severity of claims.

Sensors linked to the internet of things enable information to be drawn from within organisations and workplaces, then fed into businesses' and insurers' risk management systems. The technology works by sensing everything from air conditioning, heat, water and electricity, to movement of workers and the operation of lorries, planes and ships. Underwriters can then analyse risk continuously, predict events and understand the cause of claims.

Insurer Zurich and several of its large clients are among those highly advanced in this area. The opportunities are immense; in property alone, 31 per cent of the insurer's UK claims are around water leakage, 19 per cent accidental damage or loss, 12 per cent storm damage and 6 per cent fire or explosion.

Developments in monitoring could help prevent hugely costly and sometimes dangerous situations resulting from faulty electrical cabling, burst water pipes and contractors not following safety guidelines when dealing with "hot work", any maintenance or construction producing a spark, flame or heat. Monitoring can already help client businesses take action before an accident happens and eventually there is even the opportunity for insurers' underwriting to be automated based on machine analysis of the constant data.

To this end, Zurich is conducting a pilot for commercial building telematics, capturing data from infrastructure networks. Among the organisations signed up are universities, real estate owners and shopping centre managers. The aim is primarily to inform the businesses in real time how their buildings and activities are operating. Ultimately, the output will also be shared with Zurich's underwriting processes in real time to enhance the understanding of dangers and improve risk management. Zurich can also learn about clients' needs.

David Roberts
Group relationship leader, Zurich

"We're looking for actionable risk insights, where we know through monitoring that the customer is able to take immediate steps," says David Roberts, group relationship leader at Zurich Insurance UK. "Whether it's a machine heating up or moving too much, a flow of water or an electrical fault, these things are all starting to connect and create a digital risk profile that can be measured."

Although monitoring and related analysis are still at an early stage of evolution, Zurich is expecting to see hugely impactful changes to risk management, including much more streamlined service offerings. Mr Roberts explains: "We could effectively tear up 32 lines of business and only have one insured response that says 'we will put our capital at risk against your exact digital footprint shown today'."

> **Real-time monitoring data will prove to be a crucial competitive differentiator for firms in the industry**

Meanwhile businesses "will see a better return on investment in terms of how they manage risks", he says. Generating more data on building use and physical infrastructure will fundamentally improve how businesses present risks to insurers, increase operational efficiency and reduce dangers.

But while the benefits of increased data creation and sensor usage within workplaces could be helpful both to businesses and the insurance industry, there remains a degree of concern about the potential ramifications. These worries are "principally around data security and who is using the data and for what", Mr Roberts says, with businesses not always eager to share information until they see the benefits in action.

"There have been user-experience lessons through this; situations where people are saying 'we're not prepared to share', and they've had to take each test point and prove that everything's secure and delivers benefit," he says. "So we have to demonstrate to them that if their business is better managed, then this differentiation brings them something back from Zurich, which they wouldn't have had before."

Benefits include better insurance pricing for firms that consistently operate with low-risk, tailored advice on how to reduce risk further and real-time information on emerging dangers so they can prevent accidents.

The monitoring also helps eliminate any discrepancies or errors between the risk information that businesses present to insurers and the reality. "Insurers can use the power of the internet of things to understand the business risk on a continual basis, which has to benefit not only those who manage the risk, but also those who underwrite it," Mr Roberts says.

An important aim of Zurich's work is to "get the data talking" and move towards the integration of its own and clients' risk management systems. "If the customer is feeding in richer, more accurate risk management information, it makes sense that this should be going directly into our platform and straight to the underwriter's desktop," he says. This makes processes much more agile, streamlined and transparent.

It is assessing the most effective real-time data interfaces between insurers and clients, potentially including the use of secure, distributed ledger technology, such as blockchain, to share the information. Zurich has an advantage in this space given its investment in B3i, the industry's blockchain initiative that has broker and client support.

Greater risk management demands are expected to be placed on businesses and insurers in the coming years as the scope of data creation continues to grow. But for Zurich, the upside is that the changes are opening up these important opportunities for the industry to change fundamentally its ways of working.

Real-time monitoring data will prove to be a crucial competitive differentiator for firms in the industry. Mr Roberts concludes: "Digital risk has myriad advantages from an insurer's point of view, but for the traditional underwriters, if they don't go into their own eco-systems and look at the monitoring available, they could get left behind."

To find out about improving risk management by using operational and facility monitoring please visit zurich.com

ZURICH

CRISIS MANAGEMENT

Matt Cardy/Getty Images

Kentucky fried crisis 'triumph'

Companies with a well-prepared strategy to deal swiftly with a crisis can do much to limit financial and reputational damage

JOE McGRATH

A chicken restaurant without any chicken was how KFC pointedly described its supply issues in an advertisement in the UK national press. The company was forced to close hundreds of its UK restaurants in February after it switched delivery companies, leading to a poultry shortage.

At its peak, the shortage reportedly forced the company to close 646 of its 900 UK outlets. But while the incident could have exposed the company to brand damage, lost revenues and disgruntled customers, its well-executed public relations strategy repaired the damage with speed.

Within hours of the initial problems coming to light, customers knew exactly what had gone wrong, how it was being resolved and, importantly, when it would be fixed.

The company's response and that of Freuds, its appointed public relations agency, was labelled a "triumph" by *PR Week*, while reputation experts said the response was a masterclass in crisis communications.

"The advertising and supporting communications were genius," says Emma Evans, founder of Wylie Communications. "Not only did they recognise mistakes had clearly been made, but they also used that to their advantage by injecting some humour and keeping the language simple."

It would have been easy for KFC's directors to hesitate. In the early hours of the supply chain breakdown, little was known about when normal service would be restored, but the group decided it was better to recognise the issues being experienced by customers and build the narrative as facts became available.

"Our instinct was that we had to face the issue head on: a chicken restaurant without chicken. Not ideal," says a spokeswoman for KFC. "We were responding live as we received new information. We acted fast in assessing the issue and working out the best approach."

KFC's speed of response was core to managing the unfolding crisis successfully. "Any company caught up in a disaster or pending disaster needs to take early control of the situation, but this is not the same as admission of guilt." says Henrietta Hirst, managing director of City PR firm City Savvy.

Ms Hirst says the KFC incident shows the importance of rapidly recognising that a crisis situation is unfolding. However, she warns that companies should not be too eager to apologise or acknowledge blame until all the facts are known.

"Rapid recognition of a crisis situation, whether impending or unfolding, is important," she says. "This recognition and appropriate response helps a company capture authority and convey a sense of corporate responsibility and reassurance to those affected."

In the aftermath of the distribution errors, KFC made jokes on social media platforms and reorganised the letters of its brand-name to FCK for a national advertising campaign.

While the company's response was applauded for its simplicity by commentators, the decision to employ humour would have been the result of evaluating plenty of other ideas, according to Richard Berry, a senior lecturer in advertising, marketing and communications at Solent University, Southampton.

"When you look at the response at face value, it looks incredibly simple. But someone has had to reject 99 other solutions to select that approach," he explains. "They could have gone for something more conservative or chosen a very rational approach, with an open letter to their customers."

KFC closed hundreds of restaurants in February due to a chicken shortage, thought to have cost the chain £1 million a day

However, Dr Berry says the decision to use humour was smart, given the amount of criticism the company was initially receiving on social media. There is no doubt that the story could easily have been far worse for KFC.

As increasing numbers of restaurants were affected by the supply shortages, hungry customers took to social media to lambast the fast food chain. But the company's response to social media was just as swift as its interaction with traditional media outlets, responding to customers directly and with humour, handling the situation in public.

"With some quick, clear thinking, the narrative changed from relentless negativity to a balanced one that cleverly gained empathy," explains Wylie Communications' Ms Evans.

> **Not only did they recognise mistakes had clearly been made, but they also used that to their advantage by injecting some humour**

Many of the responses that the company were receiving through Twitter, Facebook and Instagram were emotionally driven, with the police even reporting calls from distressed customers unable to get their fast-food fix.

The fact that the company identified emotion was driving a large part of the narrative was key in justifying a humorous response, according to Dr Berry.

"A large number of customers shared memes and other content, which was the negative side of the story. But there was a stronger chance that a humorous response would have been shared widely. It was an unbelievable one-off."

While KFC's adept use of social media to inject some humour into the narrative and defuse the situation is now being held up as a case study by corporate communications academics, there is still a wider reluctance by some companies to embrace social media to connect with their customers during a crisis.

Lou Dolan, a founding partner at PR agency Camarco, says when companies are drawing up their crisis communications strategies, social media remains an element that is overlooked, despite being a crucial part to modern-day crisis management strategy. "You may not want to engage with it, but you certainly need to know what is being said," she concludes. ◆

Vulnerabilities in a crisis

PwC 2017

PROTECTIONISM

Trump's tariffs represent a new

A looming trade war between the United States and China could boil over into a global trading crisis


David Paul Morris/Bloomberg via Getty Images

01

BURHAN WAZIR

As fears grow over a looming trade war between the United States and China, American manufacturers are already experiencing the cost of protectionism.

CP Industries, which makes steel cylinders for the US Navy and Nasa, has revealed new tariffs could add more than $0.5 million to raw material costs over the next six months. "How long can we last?" asks Michael Larsen, the company's chief executive. "We could go down relatively fast."

"China has carefully targeted US exports from swing states with powerful lobbies in Washington

President Donald Trump's recent tariff announcements seek to impose a 25 per cent penalty on steel imports and 10 per cent on aluminium imports from China. The tariffs are designed to fulfil the president's 2016 campaign promise to protect the US steel industry while returning jobs to Rust Belt communities.

But as US and Chinese rhetoric over trade has intensified, taxes on hundreds of additional agricultural and industrial goods have been announced by both countries. Within 24 hours of the White House unveiling an additional list of 1,333 Chinese products also subject to tariffs of 25 per cent, Beijing responded in kind with a list of 128 US products, including exports such as cars, aircraft, soya beans, dried fruit and nuts, modified ethanol, pork and wine.

A list, published by China's Ministry of Commerce, shows 120 American products will be subject to an extra 15 per cent tariff, while seven different types of pork products and aluminium scrap will carry a 25 per cent hike. The value of US exports to China subject to raised tariffs amounts to nearly $3 billion, according to the ministry.

In America, the tariffs have been welcomed by the steel industry, which employs 140,000 people and has long campaigned for a reduction in imports from China. According to the American Iron and Steel Institute (AISI), an association of producers, China sent 800,000 tonnes of steel into the US in 2017; in return, 96,000 tonnes of steel were exported from America to China. The AISI says only 0.1 per cent of all US steel exports went to China.

According to Thomas J. Gibson, AISI president and chief executive: "We are grateful to the president for his continued commitment to the steel industry and to ensuring the country's national security interests are defended by combating the flood of imports that have been eroding America's steel industry over the past several decades."

But according to figures released by the US Bureau of Labor Statistics, increased tariffs on American steel could have an outsized effect on another 5.4 million workers employed in a host of other industries which rely on steel, such as car manufacturing and construction. A study by the Council on Foreign Relations shows that higher prices for imported steel could lead to a 4 per cent drop in car sales and jeopardise as many as 45,000 jobs in the US car industry.

Another consequence of tariffs on steel can be traced to employment in those industries which use a lot of steel, such as building fabrication. "We have seen these tariffs impact the cost dynamics of the steel supply chain, but it's important to remember that there is a lot of steel in almost every type of construction project," says Brian Raff, director of government relations with the American Institute of Steel Construction.

"In fact, there is nearly 80 per cent of the amount of steel in a concrete-framed building as there is a steel-framed building due to the density of steel reinforcing bar required, so construction costs will impact concrete buildings similarly."

Mr Raff points to a study conducted by The Trade Partnership, a consulting group which researches the impact of trade policies. It shows that while tariffs would increase employment in the iron and steel industries by 33,464 jobs, they would also cost up to 179,334 jobs in other sectors throughout the economy – a net loss of almost 146,000 US jobs.

"For the Chinese, the reason for replying to US tariffs is very simple; they are increasingly expanding international trade," explains Dr Ulrich Volz, head of department and senior lecturer in economics at London University's School of Oriental and African Studies. "I think there is a high chance that the range of products affected will expand. In the US, there are already companies which have been directly affected – companies importing aluminium. That will have a negative impact on the US economy."

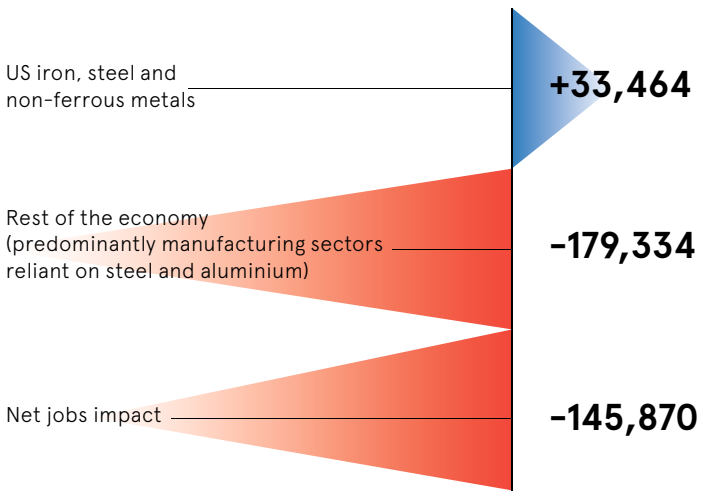
While Trump appointees such as commerce secretary Wilbur Ross have played down the prospect of a trade war, and other officials have indicated the proposed tariffs are meant to signpost a new round of tough trade negotiations, analysts say US farming is also vulnerable to tariff hikes. For example, China is the largest consumer of American soybeans, which are largely produced in Illinois, Iowa and Minnesota. China buys around 61 per cent of American soybean exports.

The concerns of soy farmers have also been echoed by car manufacturers and aviation firms. China

01
US tariffs on steel imports could result in a net loss of manufacturing jobs, particularly in sectors heavily exposed to the steel price

02
US President Donald Trump holding the Section 232 Proclamation on steel imports

Estimated jobs impact of US metal tariffs



Trade Partnership 2018

In an effort to boost domestic production, President Trump intends to impose tariffs of

25%
on US imports of steel

10%
on US imports of aluminium

geopolitical risk

imports nearly 270,000 American vehicles each year, worth $11 billion. US imports of Chinese cars are negligible. Ford alone ships about 80,000 vehicles a year to China. The American aviation sector, worth $13.2 billion in exports to China in 2016, has also urged both countries to resolve their differences amicably.

China analysts think Beijing would ultimately benefit from a protracted trade dispute. "I think the conversation in China is muted because President Xi Jinping has consolidated power and policies emerge from whatever the state wants," says Ann Lee, author of *What The US Can* Lea*rn from China* and *Will China's Economy Collapse?* "I think there would have been a more intense debate before, but now that Xi has consolidated power, the Chinese are trying to come across as more united."

Ms Lee says China has carefully targeted US exports from swing states with powerful lobbies in Washington. "The steel and agriculture lobby is very powerful, and Boeing has a strong voice as well. So the Chinese have targeted where it could hurt most, in poorer states. I think this was a calculated decision with a view on Rust Belt states in the mid-terms. Affecting jobs there is where the Chinese feel they might have most leverage with President Trump," she concludes. ◆


Glowimages/Getty Images

Case study

Three key US sectors targeted by proposed Chinese tariffs

01 Manufacturing
Auto sales are the most affected by China's proposed tariff hikes and equal to 7.7 per cent of US exports into China. Around 81 per cent of vehicles and 70 per cent of railway industry exports will be subjected to new tariffs, both areas where China is trying to grow its own global market share. States such as Michigan and Ohio are big players in vehicle production and important Trump constituencies.

02 Advanced instruments
Technical instruments such as optical and medical instruments, and specialised machinery and industrial appliances make up 6.4 per cent and 6 per cent respectively of US exports to China. In the most extreme case, 90 per cent of optical, measuring and medical instruments will be affected by Chinese tariffs.

03 Agriculture
China's threat to put tariffs on soybeans directly targets a key aspect of US agriculture. China purchases more soybeans than any other country in the world and buys around one third of America's annual soybean harvest. The biggest soybean producers in the US include Ohio, Iowa, Missouri and Indiana. Other products, such as ginseng, which is grown in Wisconsin, another vulnerable state, have also been targeted by proposed hikes.


Chip Somodevilla/Getty Images

02

REGULATION

Cleaning up the third-party data market

New European Union regulation, aimed at restoring online data privacy, will impose safeguards which will challenge some company business models

SHARON THIRUCHELVAM

If the unfolding Facebook and Cambridge Analytica scandal teaches us anything, it is how little everyday people understand of how the data brokering, adtech and digital marketing industries work.

According to the Economist Intelligence Unit, 92 per cent of people want more control over their data privacy and yet, in 2017, US companies spent $10.05 billion on third-party data, say the Interactive Advertising Bureau Data Center of Excellence and the Data & Marketing Association.

Much of that data would have been collected, sold, modelled and resold several times over without the knowledge of the people it was taken from. The European Union's General Data Protection Regulation (GDPR), which is effective from May 25, 2018, promises to change all that.

Arguably the most complex piece of regulation the EU has ever produced, the GDPR is a radical and far-reaching human rights provision that fundamentally resets the rules of engagement between individuals and companies online.

"The philosophy underlying the GDPR is to privilege privacy by default, as opposed to openness, data-sharing and monetisation," explains Eoin O'Dell, associate professor of law at Trinity College Dublin.

Crucially, the GDPR defines personal data much more broadly, giving greater emphasis to individuals' ownership of the trail of data they leave online, which currently fuels the third-party data market.

What was once deemed anonymous data – cookies, device IDs, IP addresses and other online identifiers – that was about users, will be reclassified as personal data that belongs to users and as such will be given the same safeguards as personally identifiable information, such as name, date of birth, mobile number and email address.

Currently, third-party data is traded by data brokers, ranging from market-leading, households names such as Experian, Oracle, Acxiom and Epsilon, whose primary business interests are credit scoring, database management and marketing technology respectively, to small and medium-sized enterprises, and even individuals such as the data scientist at the heart of the Facebook–Cambridge Analytica episode, Dr Aleksandr Kogan.

> **The GDPR signals a huge normative shift in online marketing, but the third-party data market will not disappear completely**

The third-party data market is shrouded in opacity. The data itself is often acquired through undisclosed means, aggregated from multiple datasets and subjected to excessive extrapolation, often producing misleading conclusions. Susan Bidel, senior analyst covering data brokerage for the technology research company Forrester, reveals that it is commonly believed within the industry that only 50 per cent of this data is accurate.

Despite its questionable provenance and quality, the use of third-party data is ubiquitous in online marketing. While falling short of industry best practice, it is considered useful by companies that haven't developed their own consumer data.

In adtech, it is a staple resource. Its uses include enhancing media buys, which in plain English means helping advertisers target relevant consumers, look-alike modelling helping advertisers find internet users that resemble their customers and audience extension, a tool that enables publishers to generate revenue by giving advertisers permission to follow their audiences, for example through tracking cookies across multiple sites.

The principle of consent is likely deliver a fatal blow to the majority of third-party data brokers. The GDPR stipulates that personal data can only be collected, controlled or processed with the explicit consent of its owners and owners must opt in to specific uses, which would include the sale of personal data to third parties.

Consequently, there will be no room for ambiguity. "Consent to use must be genuine consent, not buried in illegible terms and conditions, so the GDPR is likely to lead to awareness among consumers about how their data is used," says Professor O'Dell.

Website visitors are likely be faced with a pop-up box asking them to opt in to having their personal data tracked and sold. Given that a 2017 survey conducted by the adblocking analytics firm PageFair found that 81 per cent of respondents if given the choice declared they would opt out, there is little reason to believe this is something they would choose voluntarily, especially in the current climate with consumer concerns over privacy at a record high.

What is more, GDPR provisions will apply retroactively to companies' existing data, so up to 75 per cent of all marketing data in the UK could be rendered obsolete, according to the data cleaning firm W8Data.

Companies in contravention of GDPR rules could face a ruinous fine of up to 4 per cent of their global annual turnover. And GDPR compliance rules stipulate that in the event of a breach occurring, every link across the supply chain – data brokers, data management platforms and companies using illegitimate data – will be liable.

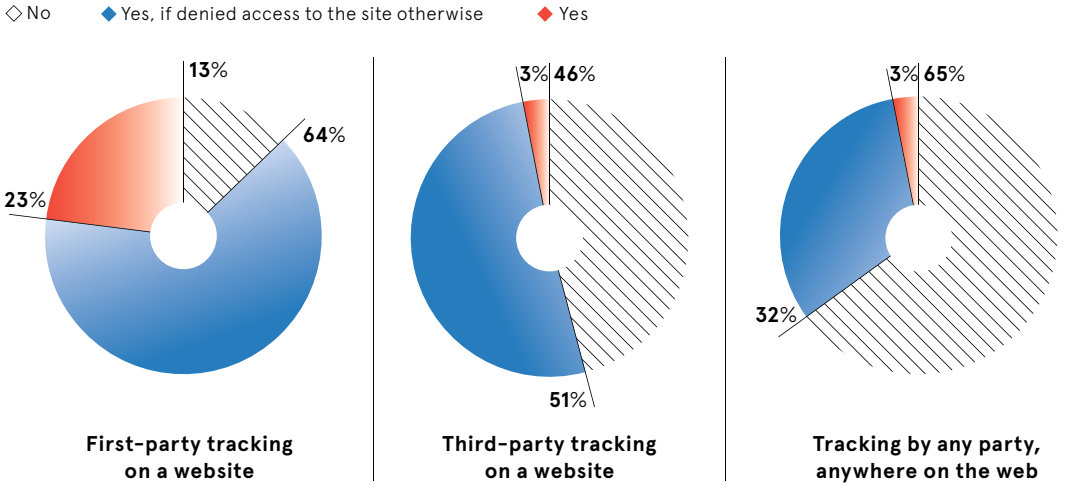
"Businesses that rely on adtech for their main source of revenue may have to re-examine their business model, in so far as it is feasible, sustainable and ethical under a regulatory regime that prioritises people's human rights," says Dr Katherine O'Keefe, lead data governance consultant at advisory firm Castlebridge.

The GDPR signals a huge normative shift in online marketing, but the third-party data market will not disappear completely. "The GDPR will shake out a lot of sub-standard actors, clean up the supply chain, lead to consolidation of vendors, and allow consumers to better own and control their data," says Gareth Davies, entrepreneur in residence at Digital Capital Advisors.

As the unpermissioned data market diminishes, it will become increasing critical for marketers to invest in building and maintaining their own first-party data assets. "This will mean more time engaging with consumers directly, making it clear what data they want to capture, why and for what purpose, and explicitly gaining users' consent to do so," explains Mr Davies.

Ultimately, if we are to arrive at a "smart" future, in which commerce, public health, infrastructure and government services are enhanced by data analytics, then we will require data that is accurate, verifiable and reliable. The GDPR is a crucial step in that direction, and will help build an internet regime founded on transparency, consent and trust. ◆

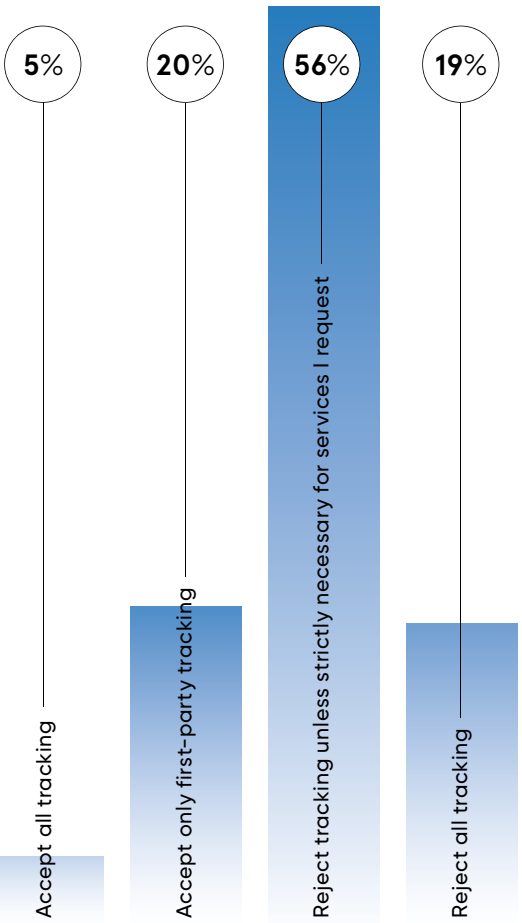
Do you believe website users will opt-in to tracking for the purposes of advertising?



Based on a survey of publishers, adtech firms and brands on the impact of GDPR PageFair 2017

Thinking of yourself as a visitor to websites, what would you select if shown this message?

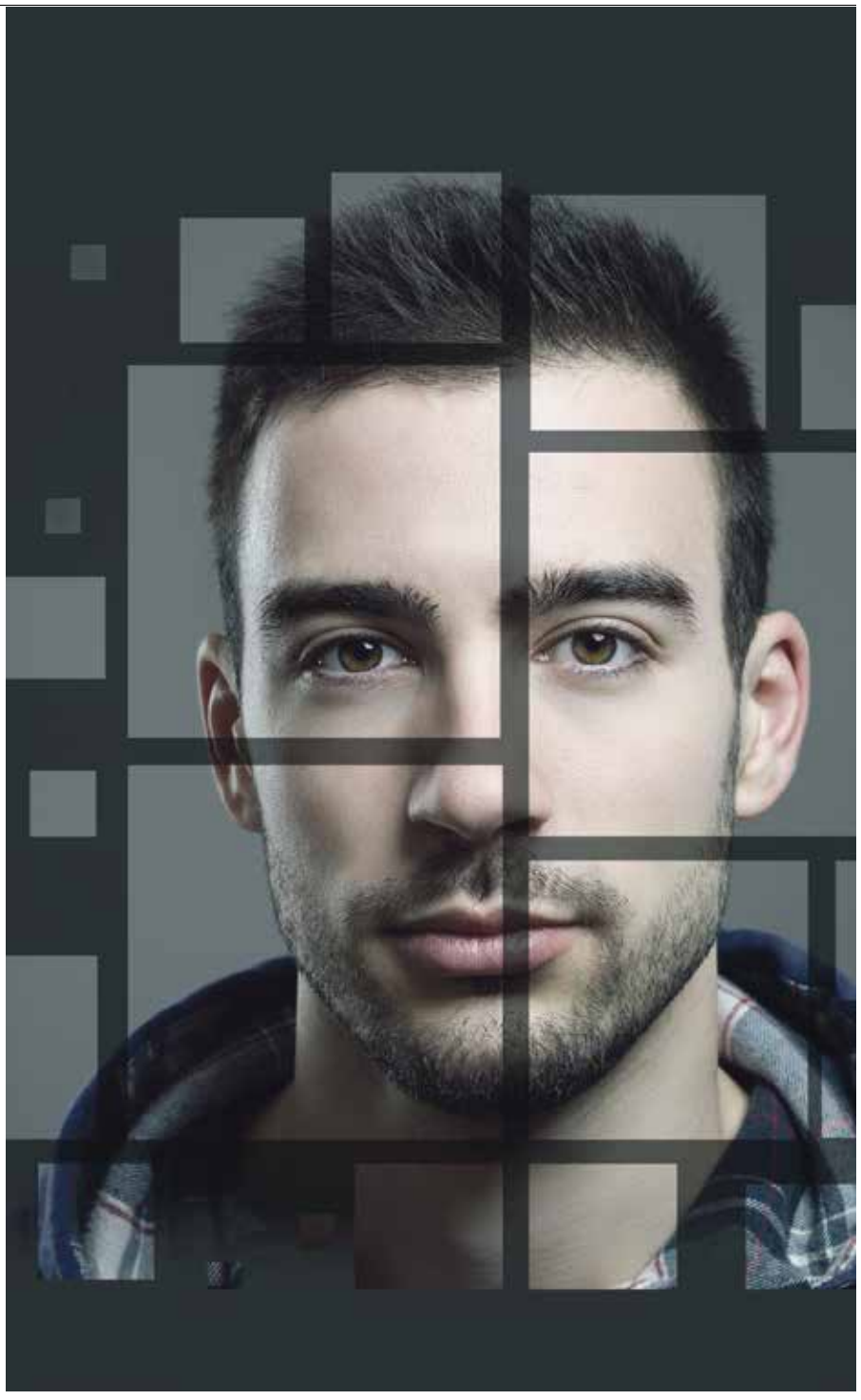
Tracking preferences



Based on a survey of publishers, adtech firms and brands on the impact of GDPR PageFair 2017

Smart identity checks intercept digital fraud without slowing down real transactions

Businesses are using analytics from an advanced, crowdsourced database to empower full online checks as identity fraud rises



The use of stolen identity data is on the increase. In the first quarter of 2018, more fraud attacks were noted than in the same period for each of the last three years, with a particularly large volume of automated attacks, according to the latest *ThreatMetrix Cybercrime Report*.

As breaches increase, Europe and the United States are no longer the only especially large cybercrime zones. South America has become a hub for new account origination fraud and Southeast Asia is witnessing large amounts of identity spoofing. In addition, the proliferation of mobile usage has led to an expanding weak security point in new account creations via mobile phones.

Online identification presents a challenge as it is hard to know if the person is who they say they are. By contrast, when a person attempts to sign up in a bank branch, for a mortgage or other financial product, the employee can verify their identity with physical documents and watch for any suspicious behaviour.

This contrast has prompted firms that handle online applications to seek a quick but thorough assessment of customers signing up for important products where identity is essential.

Data, technology and analytics firm LexisNexis® Risk Solutions already helps such businesses verify the physical identity of customers. In January, it acquired digital identity management firm ThreatMetrix to expand this to full, yet rapid, online identity verification and authentication.

"The combination of these skills will be essential to online businesses," explains Paul Weathersby, UK senior director of product management at LexisNexis Risk Solutions. "It is important to connect online and offline identity management, and enable companies to have a quick, full view of the people they are transacting with.

"Normally when a person is signing up online, a company is trying to obtain basically a name, a date of birth, and a current address – those attributes are often accepted as an identity that can be verified against authoritative data sources. But it is easy for levels of fraud to creep in here, so businesses need to do much more to assess the real risk."

The new way forward assesses "digital identity", essentially as the online footprint of a person, cross-referencing data points such as the device being used, in which area the person appears to be located and known usage or behaviour patterns. Mr Weathersby explains: "We are in a strong position to assist businesses in knowing their customers, in the digital world, and then in verifying that it really is them."

This approach is the only way to keep pace with fast-changing cybercrime patterns, says Alisdair Faulkner, chief products officer at ThreatMetrix. Given the growing scale and sophistication of identity fraud, he says, any systems attempting to tackle the threats "can no longer function in operational silos, but must have the ability to incorporate online and offline data in this way to build a more holistic view of a customer's digital identity".

An essential aspect of the technique is that it does not slow down transactions by asking people multiple questions. Instead, it automatically assesses identity aspects against known information. Consumers benefit from an effectively frictionless experience.

The ThreatMetrix network is crowdsourced and constantly updated, providing businesses with instant access to "a multi-layered approach to distinguishing between good customers and potential fraudsters", Mr Faulkner says. "While a static, rules-based approach to detecting fraud may have worked in the past, it was catching good customers in the net, penalising them for behaviour that may operate on the outliers of 'normal', such as high-value spending or frequent travel."

Crucially, this information is captured through standard use of online consumer services, with the benefit to the consumer being that they can more quickly, easily and reliably be identified and protected against fraud. "Data is captured as part of the fraud prevention process implemented by our customers," Mr Weathersby says. For privacy, LexisNexis Risk Solutions system encrypts the data and uses a hashing process.

LexisNexis Risk Solutions has the aim of robustly addressing widespread fraudulent activity online and offline, including closing any other loopholes in identity assurance as they are discovered. Looking to the future, the company is optimistic about the prospects of building added assurance into online experiences. It is aiming in the medium term to enable "passive authentication", a means through which retailers can immediately be given assurances about the identity of someone visiting their website, even if that visitor has arrived for the first time.

> **It is important to connect online and offline identity management, and enable companies to have a quick, full view of the people they are transacting with**

Given the rise in cybercrime and spoofing, behavioural analytics will become an increasingly important aspect of these checks. LexisNexis Risk Solutions expects online application processes to soon be bolstered by systems that pick up on signs of unusual behaviour, such as individuals applying for loans suspiciously quickly or much more slowly than would be considered normal. The idea is to mimic or recreate the behavioural vetting processes that would traditionally have been carried out by individuals face to face.

Mr Weathersby explains: "If you think back to what a bank employee would normally do in a loan application process, for example, if they had the person sitting in front of them, they'd be looking at their behaviour, how they talk and whether they seem hurried or stressed. For us it's about creating a level of analytics capability that effectively replaces an in-person experience, so that we can assess real digital risk from all angles and at speed."

For any business needing to check identity online, it is only truly capable when it has a process that equals or exceeds anything it would have done in person. Thorough and fast analysis, against constantly updated user data, is the only answer.

To find out more about smart identity management online please visit risk.lexisnexis.co.uk

LexisNexis® RISK SOLUTIONS

Paul Weathersby
UK senior director of product management LexisNexis Risk Solutions

Alisdair Faulkner
Chief products officer ThreatMetrix

Commercial feature

Risk managers get social to speed up response

Social media is enabling businesses to react faster to incidents and emerging threats, rather than rely on traditional news channels and information providers, enabling them to safeguard their people more effectively and create new opportunities

As advances in technology continue to increase the amount of data in the world and companies send more people to conduct business in remote locations, there is a growing expectation for organisations to gain information faster about incidents and threats that could impact them.

Tim Willis
Director of Europe, Middle East and Africa corporate security
Dataminr

The "golden hour" refers to the critical time to respond to an incident. Naturally, the sooner a business is aware of a problem, the sooner it can start acting to reduce any potential negative impact. Similarly, as soon as a business becomes aware of evolving and emerging threats, it can monitor them more effectively and, if appropriate, implement measures to mitigate and reduce their impact.

By relying on traditional sources of information, such as the news media and some information providers in the security space, there is typically at least 30 minutes between the incident occurring and news reaching a company's security and risk teams. Sometimes that can stretch to a couple of hours or longer before the business becomes aware.

The rise of social media, however, has transformed incident response. Around half a billion posts are transmitted every day on Twitter, which has become a rich source of insights when it comes to crisis response or dealing with potential threats to business.

"Social media has been a big game-changer because suddenly you have billions of people able to instantly transmit information to the world on a smartphone. This is something that ten years ago just didn't even exist," says Tim Willis, director of Europe, Middle East and Africa corporate security at Dataminr, which discovers critical breaking information for clients before it's in the news.

Dataminr uses artificial intelligence and machine-learning techniques developed over the last eight years to discover relevant signals from publicly available social media. This is important because when an incident happens, people aren't necessarily tweeting fully formed, coherent alerts. Instead, there is typically a large cluster of posts asking what's happening in a certain area or reporting people running away from something.

"Organisations must find an automated way to filter through the noise to discover the relevant signals for their business and then dissect quickly"

"It's like setting tripwires around areas of interest to organisations and, when that wire is tripped, it allows you to turn your focus on that and start to dive deeper into what's going on there," Mr Willis says. Discovering relevant content and providing almost instant access to images and videos from the ground is hugely valuable to corporate security and risk teams tasked with understanding the location, scale and implications of a breaking incident. The more content they can get from eye witnesses, the easier that is.

Following the attempted coup in Turkey in 2016, for example, Dataminr's technology alerted its clients significantly ahead of the mainstream news channels and other information providers. This allowed a pharmaceutical company to not only immediately safeguard its people affected in the local area, but also to halt plans to transport pharmaceuticals with the knowledge that the refrigerated units in their vehicles would fail while stuck in traffic, risking millions of dollars' worth of product.

"Social media has driven a massive evolution in the way we can digest information, from relying on a limited number of trusted sources of information in a one-way form of communication, to people on the ground telling each other about incidents and events," Mr Willis adds. "A lot of the opportunity is about the speed of becoming aware of incidents, but that's also coupled with the granularity you can achieve.

"If you're using the right tools, you can be proactively alerted to company-specific threats and areas you are interested in, rather than the traditional way of going to a security information provider, who might be very good at helping you with analysis, but will only ever be able to tell you what they think you need to know. By going direct to social media, you can focus on what you know you need. It puts you on the front foot from an organisational resilience perspective."

The biggest challenge to utilising social media as an early indicator is in the sheer volume of information that is transmitted through the channel. Clearly, manually scanning 500 million tweets each day in multiple languages and looking for the right keywords and clusters of activity to indicate an event type is taking place is not sustainable. Organisations must find an automated way to filter through the noise to discover the relevant signals for their business and then dissect quickly.

To aid this process, Dataminr's technology is powered by machine-learning technology. "When you look at the volume of data we're processing, you have to have machine-learning as part of the process and the right algorithms involved to make sense of that information and find the right bits of information to filter out the noise. Only then can you get relevant content delivered to your security and risk teams."

Analysing social media in this way also poses opportunities beyond risk management. Maintaining your awareness of the wider business environment potentially enables you to achieve first-mover advantage.

"So it's not just about managing risk," Mr Willis concludes. "It's also about identifying opportunities for businesses and the more effectively you use social media to do that, the more competitive you will be as a business."

For more information please visit dataminr.com

Dataminr®

CYBER-RISK

Calculating the cost of cyber-risk

The role of cyber-risk insurance is a complex issue for insurers and remains largely misunderstood by businesses that could benefit from cover

Pexels/Pixabay

Ransomware demand for $300-worth of bitcoin at a retail store in Kiev, Ukraine, where computers were infected by the Petya virus

DAVEY WINDER

Most businesses understand the need to protect networks and data assets if client trust and operational functionality are to be maintained. With the General Data Protection Regulation coming into force on May 25, failure to do so could lead to fines of up to €20 million or 4 per cent of global annual turnover. Ultimately it is all about protecting the bottom line. So why is there far less understanding about the role cyber-risk insurance can play?

Given that calculating cybersecurity risk exposure itself is complex, it shouldn't be surprising insurers face difficulties in creating effective and affordable cyber-risk policies. Technology evolves quickly, as do use-case scenarios, and that's making it increasingly difficult for both businesses and insurers to keep pace.

"Simply put, changes in technology affect how data is collected, stored and used, and the risks to which businesses are exposed as a result," says Tim Smith, head of cyber at commercial law and insurance specialist BLM.

Data type and volume varies enormously from organisation to organisation, as does the risk represented. "Assessing that risk, identifying what the exposures are, then working out how much of that risk the company wants to manage through an insurance product is not straightforward," says Mr Smith. Unlike motor insurance, for example, there isn't a century of claims data to fall back upon.

As the cyber-loss experience becomes less benign, insurers are expected to start insisting on much more qualified risk-exposure data. "Until then insurers are compensating for the problems in submitted exposure data using 'outside-in' third-party data sources, such as cyber-incident data pools and measures of vulnerability of internet exposed IT infrastructure," says Pratap Tambe, business development manager at Tata Consultancy Services.

This is hugely problematical, certainly according to some cybersecurity vendors. Take Nik Whitfield, chief executive at Panaseer, who argues that outside-in is a highly limited approach "similar to doctors assessing patients without the benefit of X-rays, blood tests or MRI scans".

Better to be using "inside-out" information for risk assessment; think of telematics in the motor insurance sector. "This will provide a far better evaluation of the enterprise cyber-hygiene and therefore the risk position of the insured," says Mr Whitfield.

Someone who is very familiar with calculating risk exposure is Visesh Gosrani, director of risk and actuarial solution architect at Guidewire Cyence. "The cyber-risk model needs to look beyond pure technology and extend the problem to people and processes," he says. "A holistic data-driven approach is necessary to get a complete view of the multi-faceted cyber-risk of companies."

Given the rapidly changing environment also requires a continuous loop between data collection and risk-modelling, this represents a challenge when these are performed in silos, Mr Gosrani admits.

When it comes to specifics, the economic modelling metric must be broken down to address frequency as well as severity, financial loss and recurrence. The latter, asking if a company experiences a breach what is the probability of a follow-on event occurring, requires insight into organisational cybersecurity policy and process.

The insurance industry must also consider performance across portfolios, so any cyber-risk model must look at the economic impact of risk accumulations, aggregate events and disaster scenarios, and then translate these into probable loss curves. Otherwise insurers would be unable to deploy capital and justify their decisions to shareholders, regulators and rating agencies. "This requires a revolutionary approach to how insurers utilise data-listening and artificial intelligence to create the right models for tracking risks that are extremely dynamic," Mr Gosrani adds.

Ask most organisations about cyber-risk insurance and the lowest common denominator response will be along the lines of how likely is a pay-out if a breach occurs? Neira Jones, senior adviser for financial services with the Centre for Strategic Cyberspace and Security Science, says: "Whether a cyber-insurance policy will pay out will depend on how much businesses understand their environment, their vulnerabilities and their consequences."

Ultimately, it's about fostering partnerships between the organisation seeking cover and their insurance provider. "The financial services and information services industries are prone to assaults on their infrastructure such as denial of service or hacking attacks on servers, while the public sector exhibits patterns of compromise due to misuse and errors or cyber-espionage," Ms Jones points out.

The devil, therefore, is almost always in the detail. Sjaak Schouteren, partner at global insurance broker JLT Specialty, warns that the importance of exclusions is particularly acute in the technology and cyber-arena, even down to specific aspects of software being used.

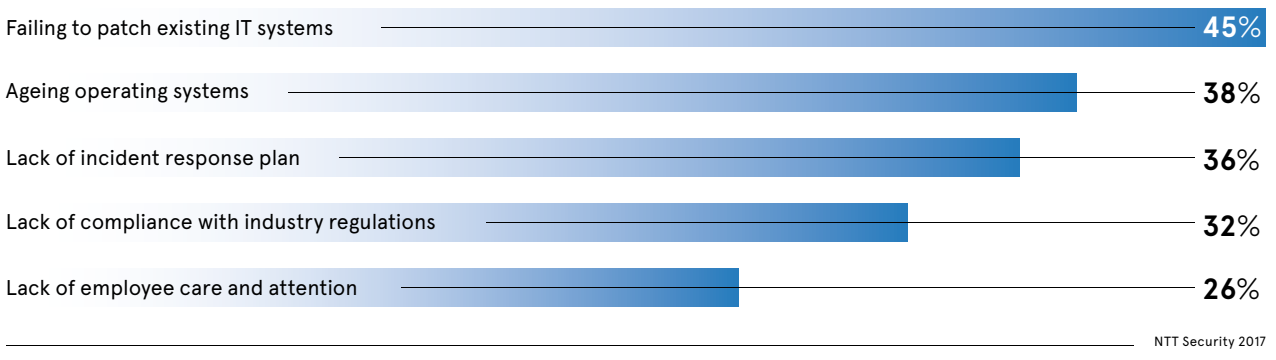
> **Cyber-insurance has a lower decline rate for claims than most other lines of insurance**

"If a company uses Windows XP on their system and suffers a breach, it may still be able to claim if the breach occurred outside of Windows XP," Mr Schouteren explains. "If the breach occurred via a Windows XP vulnerability, there is not likely to be a rightful claim because the software itself cannot be updated, having been left behind by Microsoft."

The good news is that it's extremely likely a cyber-insurance claim will be paid, according to Graeme Newman, chief innovation officer at CFC Underwriting. "Cyber-insurance has a lower decline rate for claims than most other lines of insurance," he says. "We paid more cyber-claims in 2017 than ever before and 2018 is already looking to eclipse that by a considerable amount." ◆

Poor practices put cyberinsurance at risk

If companies can't demonstrate competent basic cyber-risk management, it could invalidate their insurance



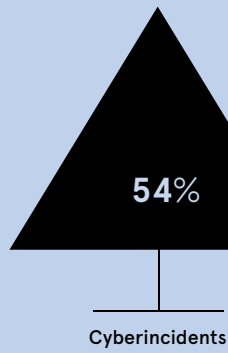
NTT Security 2017

PREDICTING FUTURE RISKS

Risk forecasting and management by their very nature are evolving practices. Yet, as the business landscape continues to transform due to groundbreaking new technology, geopolitical uncertainty and an increase in public scrutiny, to mention just a few, preparing for the next major corporate risk will continue to become more challenging - and harder to predict

Top three most

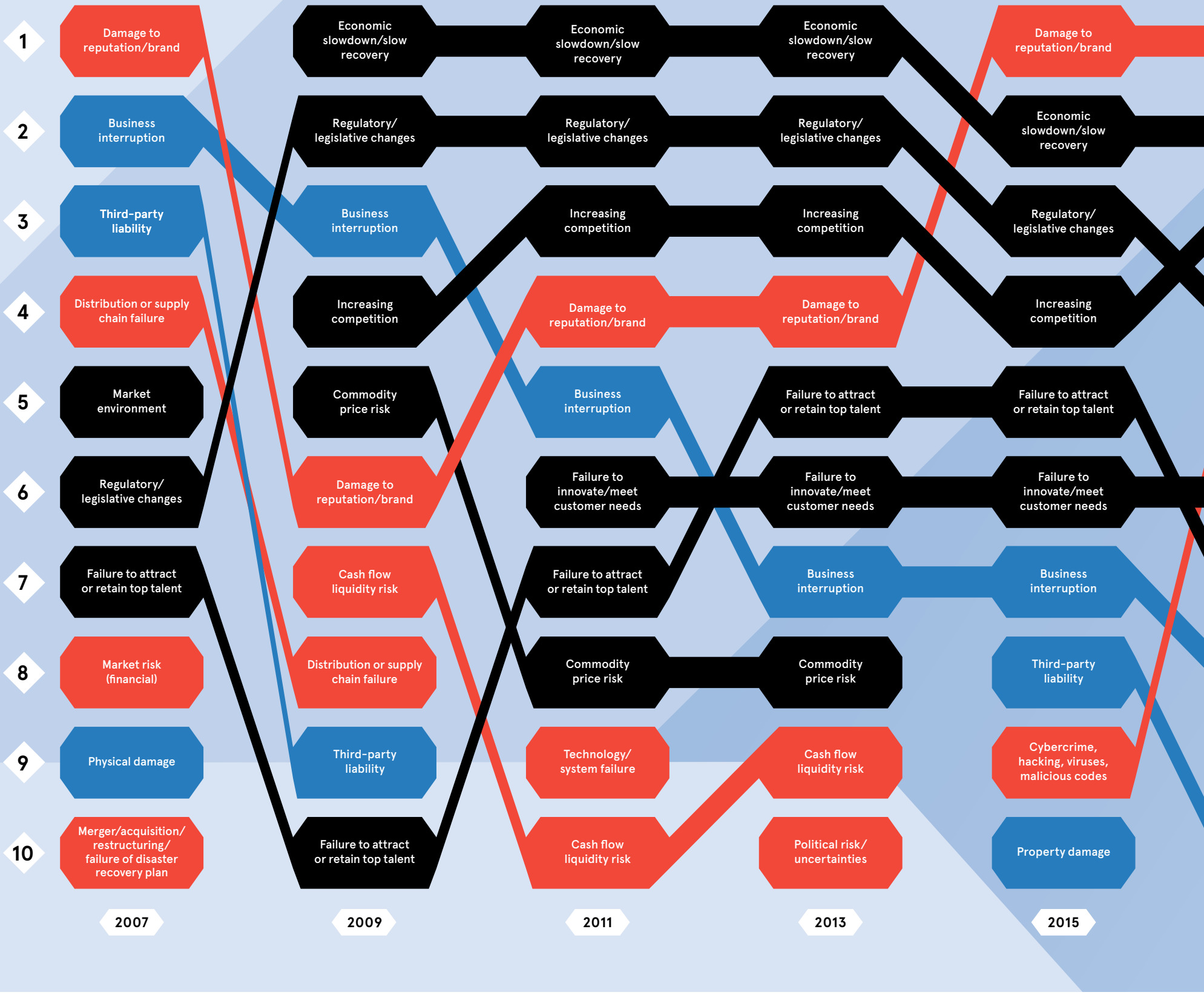
Percentage of globa
are currently undere



Allianz 2018

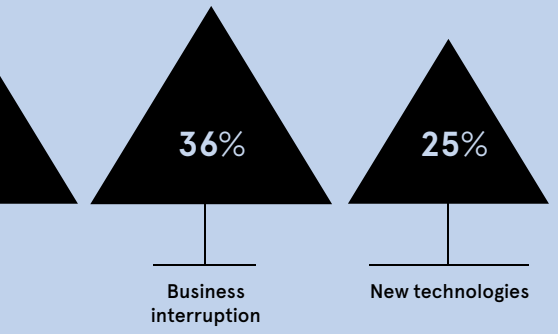
Uninsurable risks continue to gain precedence

Top ten risks to businesses, based on a global cross-industry survey of risk and financial executives from public and private companies



underestimated business risks

al risk experts who believe the following
estimated



59%

of global executives and academics expect an increase in business risks this year

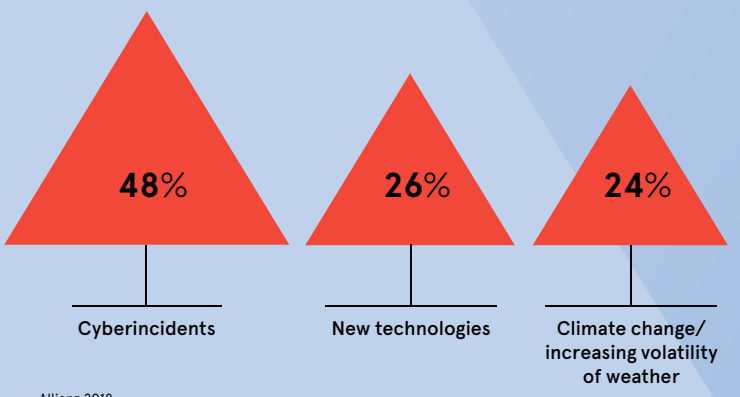
7%

expect a reduction

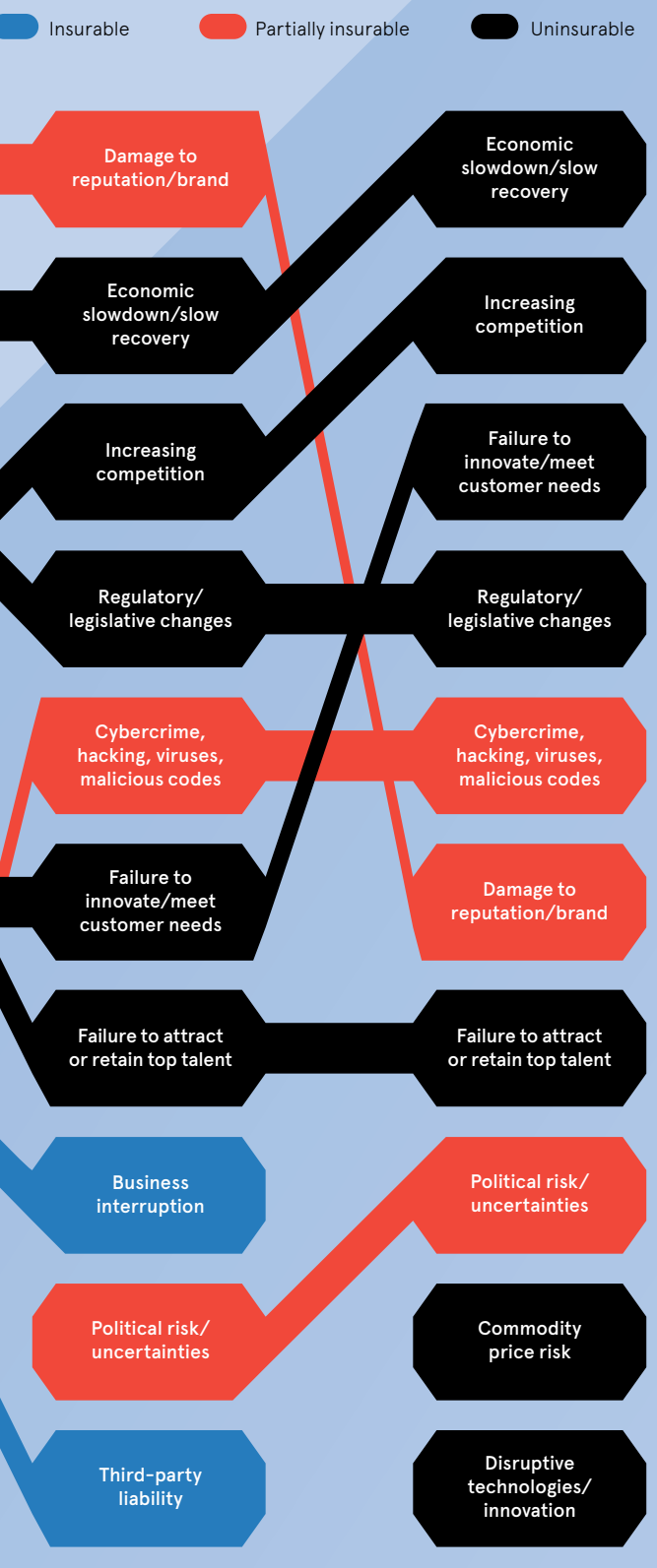
World Economic Forum 2018

Top three long-term business risks

Percentage of global risk experts who selected the following as top risks in ten years or more

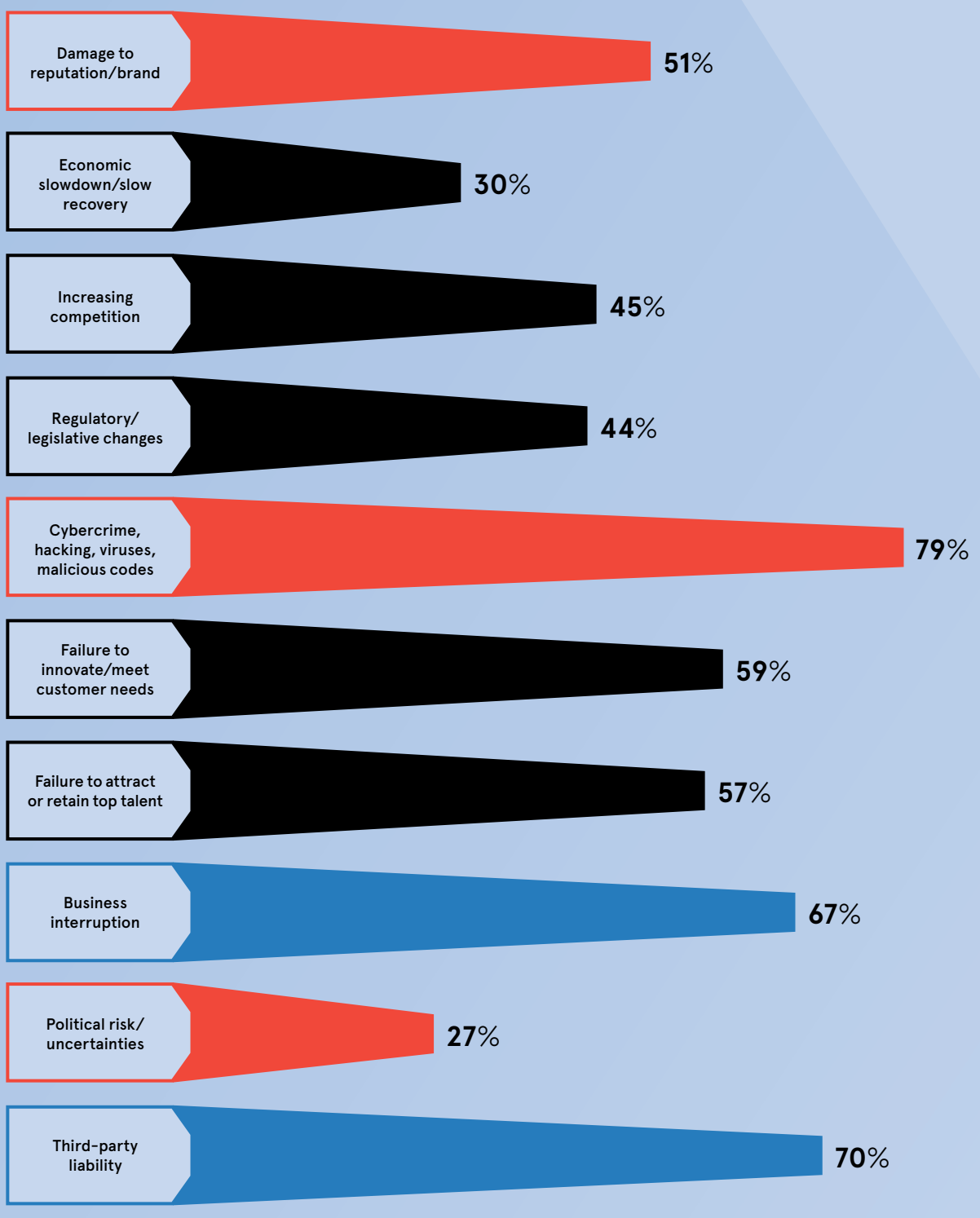


Allianz 2018



Readiness for top business risks

Percentage of risk and financial executives who said their company was prepared for the top ten business risks in 2017



Aon 2017

Boards must play key role in rollout of artificial intelligence

As artificial intelligence continues to disrupt industries and open new opportunities and challenges in risk management, **Rob Walker**, leader of EY's Risk Advisory practice, discusses what this means for boards

To what extent is artificial intelligence (AI) currently on the agenda of boards across the UK?

Some boards are really aware of it and some are behind where we think they need to be. It varies in terms of how relevant digital disruption has been to boards. Those who are aware of it tend to be in sectors that have been disrupted. For example, technology or media and entertainment sectors, where there has already been a high degree of change, or in highly regulated industries such as banking. Others are far less aware or, if they are aware, it's more about its application in other areas. Most boards are not considering AI and the opportunities presented by it as it relates to improving risk management.

At board level, is AI currently viewed more as an opportunity or a risk?

Generally more as an opportunity, but they tend to see it as an efficiency play rather than an opportunity to enhance risk management procedures and processes. Sometimes they are surprised by the increase in visibility it gives you and the consistency you get across a wider reach of your business. A combination of AI, automation and analytics enables you to drill risks up and down in a much more detailed way, and to get into far greater depth of issues at a sub-reporting or sub-business unit level than has ever been presented. We are seeing, for example, digital dashboards being put in front of boards that provide the ability to assess risks at a group level, drill down into subsidiary business units, geographies or components of the business and understand how those risks are presenting in detail. This gives boards a huge amount of richness and greater insight around the way risks are being managed, and the opportunities for the business to take on more risk. But not many boards have had that kind of digital dashboard put in front of them; it's the exception rather than the rule.

What are the risks of ignoring AI or not giving it the attention it deserves at board level?

Boards need to navigate a path between thinking AI is the panacea for all ills and rushing into it without being aware of the risk. Even if AI might be further out in terms of priority or risk, the velocity at which it's coming isn't constant. If boards aren't thinking about how they start to update skills and dip their toe in the water, by the time it's actually upon them, it's going to be too late to have built those skills. There's a real risk around either leaping in head first or leaving it too late. Our recommendation is that all boards should be thinking about what they should be doing to get started. You can't wait until it's the number-one risk to your business before you start thinking about how you respond.

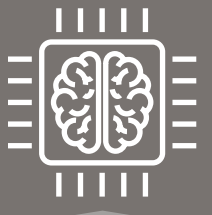
What ethical issues does AI create that directors should be aware of?

There's a real concern that bias may get embedded into AI. Sometimes it may be developed by a group of people who have really good ideas, but find themselves operating in isolation, either as technical specialists or product developers. Boards needs to challenge management on how they bring diversity of thought into the process. As they're going through and starting the AI journey, have they brought in the whole view of the organisation in terms of what it means for the people whose data is being utilised, and what are they doing in terms of what it might mean for their customers and reputation? It's about thinking as broadly as possible around where this is eventually going to impact, rather than what it might be designed to do in the first instance. The best way of countering bias is making sure you have a diversity of people and thought in terms of what it means to the organisation.

AI: to manage risk or a risk to manage? Both

AI to manage risk

- Deeper understanding of the business – allows the board to ask better questions
- Automated and more regular insight – improved decision-making ability
- Ability to free teams to focus on what really matters – efficiency and effectiveness of risk function



Managing AI risk

- Risk of being overtaken by speed of technology – dip toe in the water
- Risk of of bias and damage to reputation – increasing diversity of thinking
- Risk of not delivering benefits – continued challenge to management

What are the implications of that on the board's role in the business?

We see a potential emerging issue that if you have a fully automated risk environment, it takes out the professional scepticism boards still need to have. You may be able to define a risk appetite and monitor that effectively using some quite sophisticated skills, but boards still need to exercise challenge to management. They still need to trust their stomach and look for the impact of longer-term trends and exercise judgment in terms of holding management to account. That is the principal role of a non-executive board. Technology can enable this, but you shouldn't be blinded by the data or technology such that it prevents you exercising professional scepticism.

What is the future of AI in risk management, and what role will EY play in helping boards understand its importance and impact?

We are really optimistic for the future of AI to accelerate the benefits of effective risk management. We think it will empower boards, provide visibility to risks and opportunities, and give boards a far wider and consistent set of data points to make judgments. Our overall starting point is incredibly optimistic around what can be done. Our role at EY is firstly to bring emerging tools and combinations of technologies into the boardroom, and demonstrating the art of the possible. We can help companies stand up more effective risk management, either as a standalone service offering or as a managed service. EY is uniquely placed in terms of risk management and commercial acumen to make tools relevant to boards, as well as the right governance and regulatory levels that boards need to operate under.

Rob Walker is an EY partner and the UKI risk leader. He is also a member of the content steering group for the EY UK Centre for Board Matters, a programme delivering insight, thought-provoking discussions and facilitating connections for non-executive directors. **For more information please visit www.ey.com/uk/boardmatters or email neds@uk.ey.com**

EY Building a better working world

PREDICTIVE ANALYTICS

Data-driven firms push smarter products

The rise in predictive analytics is revolutionising the insurance industry by enabling savvy insurers to predict risk


John Lund/Getty Images

BEN ROSSI

Dramatic advances in artificial intelligence and machine-learning technologies have accelerated the ability of insurers to predict risk. Algorithms can find trends and patterns that help forecast the probability of a risk situation occurring again.

By utilising internal and external data sources, algorithms are selected according to how a specific model fits with the insurer's data. This model is applied to predict or detect the likelihood of an event happening, such as a person needing medical attention abroad for travel insurance or a house flooding for home insurance.

Insurance and assistance provider The Collinson Group uses a variety of predictive analytical tools to flash through terabytes of data to find variables, some of which it hadn't considered, to help predict customer risk and purchasing behaviour.

With this technology, the company is able to identify fraud and the different networks of fraudsters acting in the market, as well as increase its understanding of customers, and ultimately tailor its offering to provide them with better products and services.

"Predictive analytics has enabled a more scientific approach to analysis, allowing us to analyse more data in little or no time, and to explore parameters and factors we could not have identified with the human eye," says Jean Ortiz-Perez, the company's head of analytics. "The concept and objective of what we do have not changed, but the mechanisms and techniques are now much more sophisticated."

The role of predictive analytics in insurance can actually be traced back two or three decades in the area of natural catastrophes and climate. Analysis of 50 years of data on hurricanes, for example, has proven extremely powerful in terms of helping insurers to predict future hurricane behaviour and its likely impact.

However, this has required a large amount of human input and oversight. More recently property and liability insurers have been playing catch-up with the life insurance sector, where a rich trove of available data, including longevity, gender, country and quality of life, has allowed for clearer analysis and confident predictive outputs.

The rapid evolution of machine-learning capability and the wider availability of data through connected devices are now set to make the use of predictive analytics ubiquitous across the industry. And to accelerate the necessary collection of data, new health insurance models are emerging that actively link premiums to analytics.

> **The potential of these technologies is huge, with scope for insurers to change their business models as compensators of accidents to preventers**

In the automotive sector, for example, telemetry and driving apps are not only encouraging people to drive safely by incentivising them with reduced premiums, but they're also arming insurers with the necessary data to power predictive analytics. Healthcare insurers, such as Vitality, reward members with a free Apple Watch if they commit to trackable daily exercise goals.

"The potential of these technologies is huge, with scope for insurers to change their business models as compensators of accidents to preventers," says Roy Jubraj, UK insurance strategy and innovation lead at Accenture. "Insurers can even use analytics, with data pulled in from smart homes and connected devices, to intervene before an incident happens in the first place. It'll see insurers plugging into their consumers' lives and wider eco-system to look after the asset or risk they want to protect."

Matthew Grimwade, senior partner at insurance broker JLT Specialty, adds: "The next and very exciting chapter, driven by artificial intelligence and ever-improving technological capability, will drive down costs and continue to improve the quality of the predictive outputs, and enable the industry to deliver insights and predict risks even faster."

Insurance companies are operating in a difficult market, facing disruption from startups shaking up the status quo, while having to transform their operations to meet the increasing demands of a real-time digital world. They need to innovate to survive.

The sophistication of predictive analytics will increase rapidly over the next few years, as truly data-driven insurers emerge that are able to make better decisions faster. Such innovation will improve predictions of loss and enhance consumer response to new products, driving positive business results that boost both the top and bottom lines.

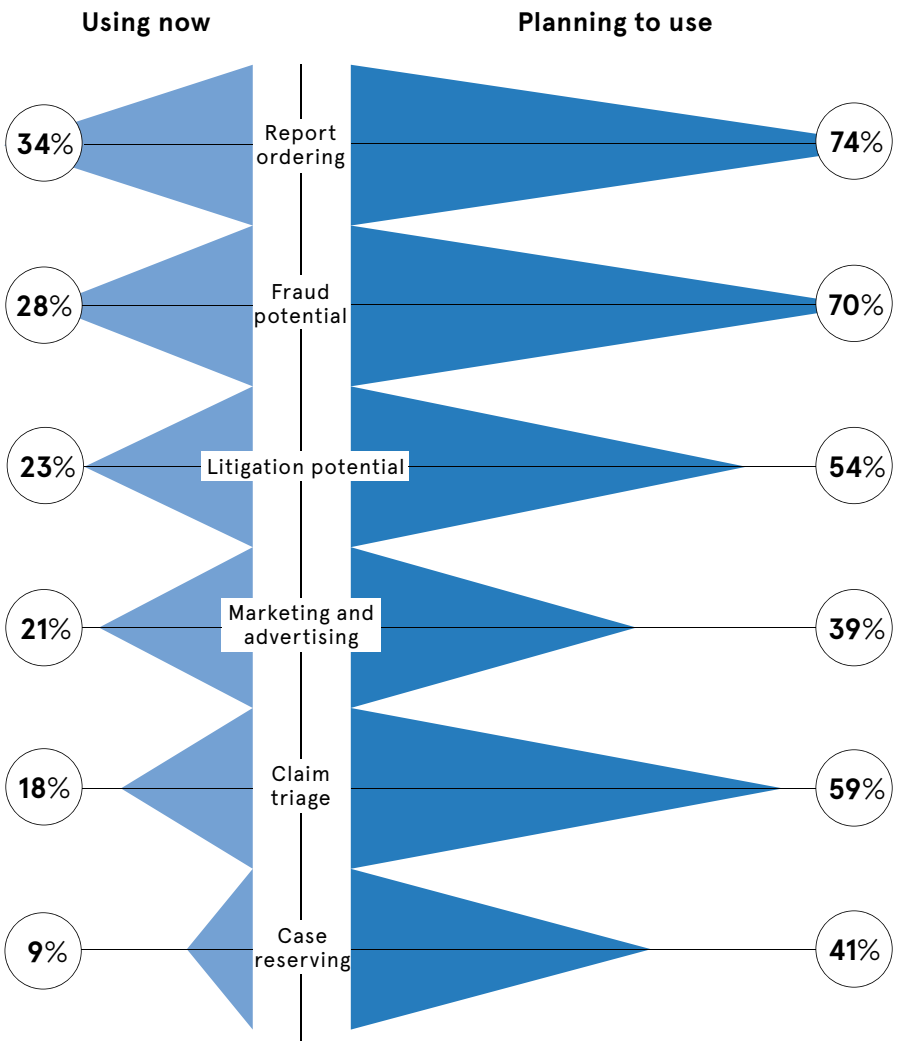
One large global insurer, which manages a motor insurance portfolio of a million policies through 200 large agencies, implemented demand-based predictive models through technology from analytics firm Earnix. The insurer saw a profit improvement of 2.8 per cent, while maintaining existing customer retention levels.

"As more insurers operationalise these new methods, current insurance product offerings will be revolutionised," says Udi Ziv, chief executive at Earnix. "Already new products are appearing in the marketplace, such as car insurance by the hour or temporary home insurance. Combine these with customer expectations for more personalised levels of service and it's clear insurers need to adapt to this changing market. They will need to harness predictive analytics to become customer centric at levels previously unseen."

Done responsibly, with consideration for concerns over the use of personal data, insurers can shift their relationship with customers from a grudge purchase to one of value. But this approach hinges on maintaining consumers' trust. Using analytics to identify which customers will value this capability and service is beneficial, but insurers must always use these new methods and algorithms responsibly. ◆

Top uses for predictive modelling

More than two thirds of insurers currently use predictive models for underwriting and risk selection*

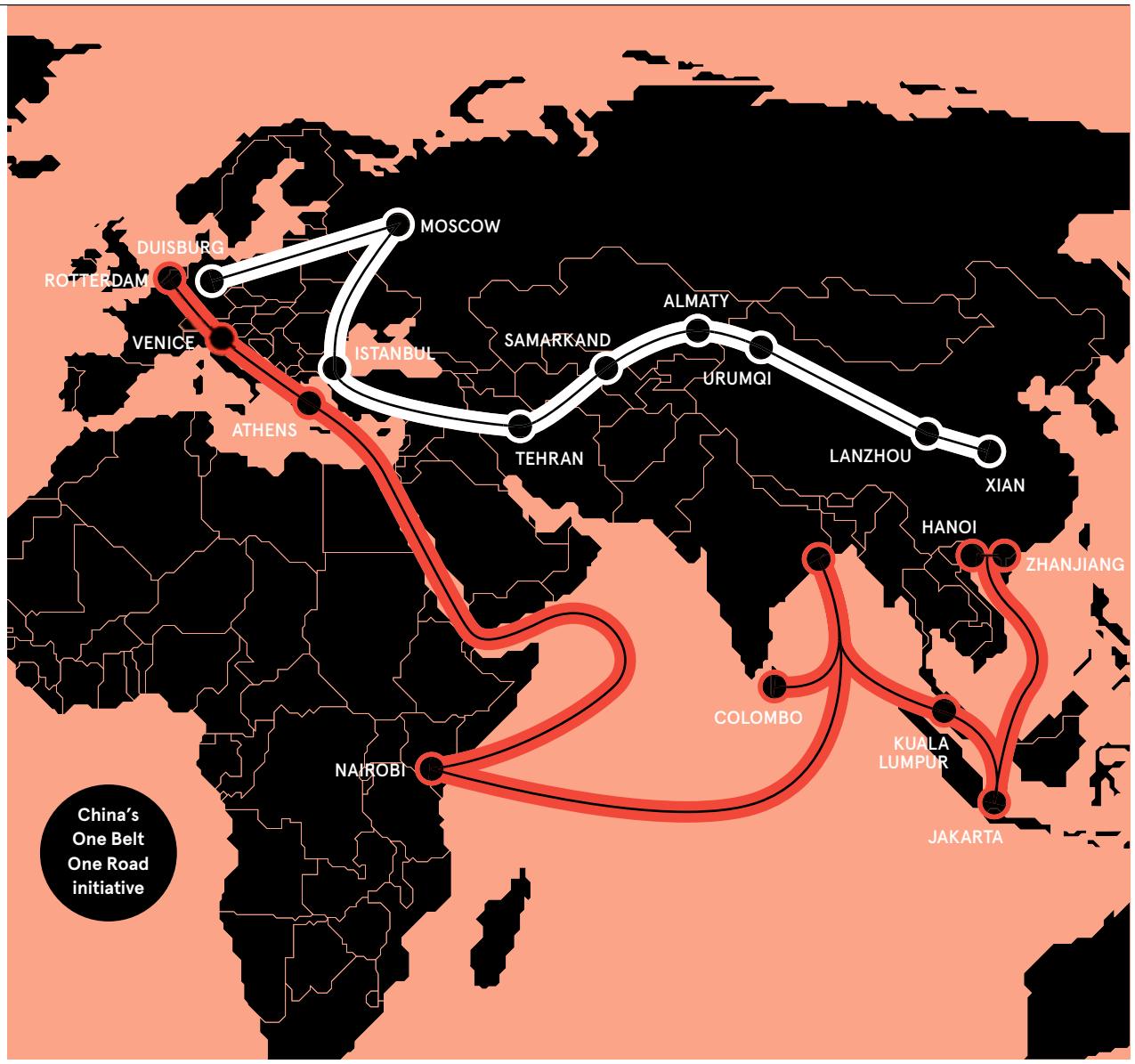


*Survey of property and casualty insurers in the United States

Willis Towers Watson 2017

Mid-market leaps into unfamiliar territory

UK mid-market companies are increasingly seeking global expansion to secure faster growth and diversification, but understanding the risks that come with entering new territories is vital to take their business to the next level



The UK's mid-market companies are the unsung heroes of business. Despite representing just 1 per cent of companies, research by law firm Gowling WLG forecasts their contribution to the economy will reach £335 billion by 2020, an 18 per cent rise on 2015. Much of that contribution will come from international expansion.

Around 35,000 companies make up the UK's mid-market and 62 per cent of them plan to increase investment in exports beyond the European Union because of Brexit, according to a survey of 500 medium-sized businesses by Mills & Reeve. But Brexit isn't the only driver of expansion.

Cloud computing and mobile technologies have removed barriers that previously made entering new territories too expensive and complicated to consider for many mid-market companies. The ability to transact on a world stage is much easier and as such, opportunities for growth and diversification overseas are bigger than ever before.

A greater multinational footprint, specifically outside Europe, brings new and arguably heightened risks.

Many mid-market companies are increasingly looking to the Far East for expansion and to China in particular, with the One Belt, One Road initiative opening up a wide range of opportunities and markets. While UK mid-market companies might be largely undeterred by the prospect of a US-China trade war, they need to bear in mind that the laws and exposures they face outside Europe are often very different to what they're used to at home.

Sara Mitchell
Head of corporate division UK and Ireland, Chubb

The ability to navigate and manage these multinational risks is increasingly important, particularly when companies are expanding in lesser-known or emerging markets. So businesses need to work with experienced partners who can help them deal with the complexities of this risk landscape.

"The mid-market space is so diverse and organisations are even braver today," says Sara Mitchell, head of corporate division, UK and Ireland, at insurance firm Chubb. "The world feels a lot smaller for business because of the infrastructure that's in place, whether it be through insurance or other financial institutions. Companies are utilising the experience they've got in different sectors and finding it less frightening to grow in another country."

Mid-market companies operating on a multinational footing for the first time need to tackle the local regulatory requirements for insurance policies and cover, and what needs to be evidenced in each territory. Most mid-market companies don't have an insurance department to look after this so require somebody to do the heavy lifting for them.

The prospect of a large uninsured loss is not the only thing that keeps executives awake when entering new territories; the risk of reputational damage can be just as terrifying. Such damage can be easily suffered if the company doesn't have a policy which is legal or valid when trying to operate in other regions. Businesses also need guidance on taxation and local premium payments issues.

"Particularly outside of the EU, you can't wave a piece of European paper and expect that to be accepted in the US, for example," says Mark Roberts, property and casualty (P&C) chief underwriting officer, UK and Ireland, at Chubb. "Mid-market companies want an insurance policy that is aligned with local regulations and local expertise." With operations in 54 countries and territories, Chubb is able to tap into local offices to provide local risk engineering support and claims handling.

> **Businesses need to work with experienced partners who can help them deal with the complexities of this risk landscape**

Companies also need to consider the new risks they are likely to face in unfamiliar environments. These could include natural catastrophe, new and previously unknown liability exposures, terrorism and the growing threat of cyber. Natural catastrophes and cyber rank among the biggest and potentially most damaging risks for businesses operating in the Far East.

Wherever organisations have operations, they have computer systems that can be exposed so it is of paramount importance to ensure those systems, as well as any data belonging to both the company and its customers, are secure. Damage following a data breach can be severe both financially and reputationally. Strict new laws on cybersecurity and data privacy have been introduced recently in several countries in the Asia-Pacific region.

"Data regulations can and will vary in different territories and we can advise our clients on the exposures in this regard, while also ensuring that their insurance covers are reflective of this," says Karen Strong, UK and Ireland head of industry practices at Chubb. "Cyber is such a short word and it's bandied around easily and increasingly, but there are so many different elements to cyber-exposures, both for the client themselves and for the impact on their customers. This introduces first and third-party risks for our clients.

"An example of growing exposures in this regard is the fact that many mid-market companies utilise hosted services for the efficiencies they provide while enabling growth into new territories and this introduces new concerns to a company's risk register."

If the worst does happen, it is important to be able to rely on an insurance partner that has the ability to pay claims promptly and locally.

Companies also need to consider issues in specific territories. As well as dealing with language and cultural changes, becoming more global can open up heightened litigation risk for product liabilities. Companies exporting products abroad for the first time or opening up overseas offices need to be aware of additional and potentially more onerous obligations.

The need to label goods correctly for the local market, warn about possible hazards, and comply with the relevant local safety and regulatory standards must be considered. To deal with this, Chubb's multinational experts from underwriting and risk control are able to provide advice on a country-specific basis.

A policy sold in the UK would not necessarily be fit for purpose somewhere else, so Chubb has local offices and operations in many of the countries that mid-market companies are expanding to, providing people on the ground who can help them navigate the legal and regulatory environment.

"For a lot of our clients who buy directors and officers (D&O) policies, they actually buy what we call local policies," says Hilda Toh, UK and Ireland financial lines manager at Chubb. "So if they're a UK mid-market company and they're setting up operations in China, India, Japan, Mexico or wherever it may be, we can help them with issuing a D&O policy for that local jurisdiction as well. That local policy would be written in a local language, and with local laws and regulatory environment taken into consideration."

Suresh Krishnan, head of global accounts division, Europe, at Chubb, concludes: "An off-the-shelf single-policy response is simply not prudent, particularly in a multinational context. Clients need partners with the capability to craft solutions with local policy, local risk engineering, local claims and local compliance capabilities that fit an individual company's profile, tailored precisely to its specific needs."

For more information please visit chubb.com

CHUBB®

Risk is rising up the board's agenda

No longer purely custodians of caution, the role of the chief risk officer is transforming to accommodate the demands of corporations and investors

JOE McGRATH

DANNY HU/Getty Images

Major scandals have traditionally been a precursor for regulators, companies and governments to rethink their approaches to corporate risk. It took a seismic event for risk approaches to be altered and for new protective measures to be adopted.

In the early nineties, the collapse of FTSE 100-listed textile group Polly Peck, the Mirror Group pension scandal and the liquidation of BCCI led to the formation of the UK Corporate Governance Code.

More recently, the 2008 financial crisis, which claimed Lehman Brothers, Northern Rock, Bradford & Bingley and many others, saw the code revised and radical changes to how risks are assessed within financial institutions.

Given the scale of the 2008 crisis, it is perhaps no surprise that the role of the chief risk officer (CRO) is currently more commonly found in UK banks, asset managers and insurance groups than in non-financial sectors.

But the importance of having a chief risk officer, who is able to quantify business risk, is beginning to catch on in other sectors, according to the risk management association Airmic, and it is not purely to satisfy the probing eyes of regulators.

"Risk management is not just about prevention, it is about opportunity," explains Julia Graham, deputy chief executive at Airmic. "Risk management is like brakes in a car. They give you confidence to go faster. The modern world of risk management is about releasing opportunity and allowing you to take more risk."

Ms Graham's sentiments are echoed by institutional investors who are taking an interest in corporate governance and sustainability credentials.

Increasingly, investors are engaging with companies, urging them to identify future threats to revenues, and are even using their votes at annual general meetings to ensure companies carry out comprehensive risk assessments.

Last year, investors made global headlines when they voted at the annual general meetings of Exxon and Shell eventually obliging the companies to do more to assesses the impact climate change will have on their business models.

With business sustainability climbing the agenda for institutional investors, it is becoming more important for larger businesses to have a senior executive that is plugged into different areas of the business and has full oversight of long-term vulnerabilities.

"CROs have much more influence than they did in the past," explains Philip White, a member of the enterprise risk management team at Thomson Reuters. "The CRO needs to have complete oversight of the business and how it is performing. This includes new business decisions, going into new markets or developing new products. It is increasingly the CRO who has that sway."

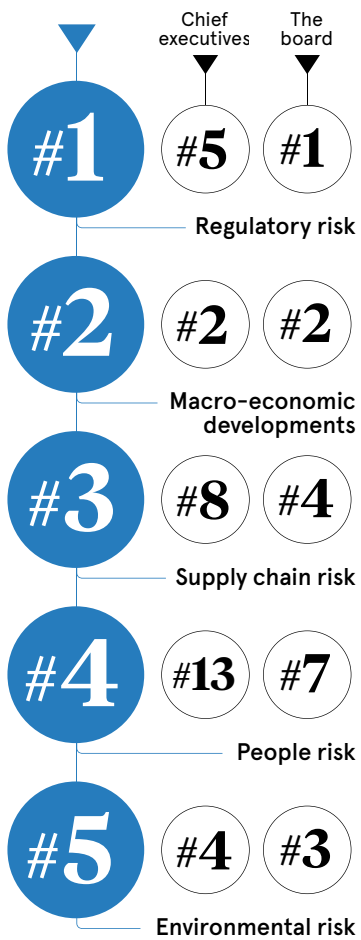
As business needs have changed and stakeholders demand increasing levels of reporting from the executive, the professional profile of individuals holding CRO responsibilities have also changed. At the turn of the millennium, executives in a risk function were typically from a financial background, but the profile of today's CRO is much more varied, according to Mr White.

"The CROs of 20 years ago were very much numbers or 'quant' people. They didn't necessarily have the greatest communication skills. That element is now far more important," he says. "Increasingly you will see the CRO becoming the chief executive of the future. The chief risk officer has to have his or her fingers in so many pies around the organisation."

Airmic has been working with professional consultancy group Oliver Wyman to chart the current responsibilities that fall to the modern-day CRO. The decision to chart the responsibilities, rather than the job title, was a deliberate one, according to Airmic's Ms Graham, who says CROs and the like go by many job titles.

"In many organisations it is the chief financial officer or the chief executive who is running that role and the head of enterprise risk will report to them," she explains. "Risk management is a relatively new profession. It has only emerged in the past ten to fifteen years. Other professions in law, accountancy and personnel directors have been around a lot longer, so not everyone is used to dealing with risk managers as a professional group." ◆

Top five issues chief risk officers are least prepared for



BDO 2017

Case study

Aon UK's Matt Kimber

Consultancy group Aon is among an increasing number of organisations to recruit a high-powered chief risk officer (CRO). In March 2017, Aon announced it was appointing Matt Kimber, who joined the business after more than five years with brokers Jardine Lloyd Thompson (JLT) where he was group head of risk and compliance.

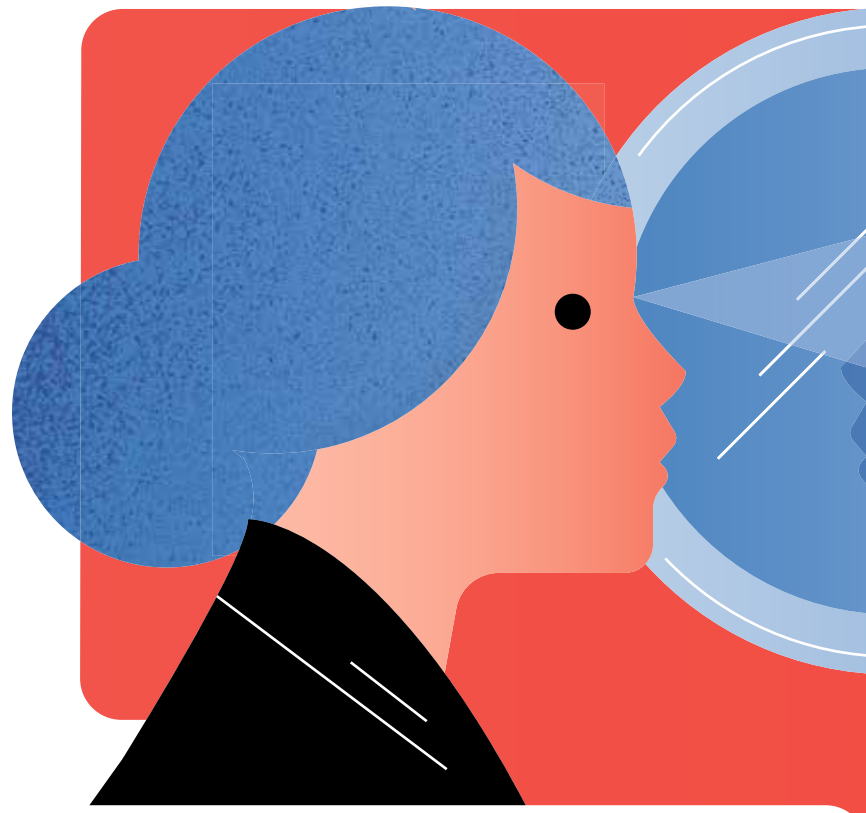
Notably, Mr Kimber's appointment as CRO at Aon UK saw him join the company's board, reporting to chief executive Julie Page, who said he would bring valuable experience to the group's risk and compliance team.

Aon praised their new recruit, saying he had already made some landmark corporate achievements over the past 20 years, including influencing and developing "enhanced risk-aware cultures" at insurance brokers and risk managers Marsh, and Lloyds Banking Group.

Mr Kimber, a graduate of the University of Hertfordshire with a degree in accountancy and financial management, also worked for eight years at Halifax Bank of Scotland, where he was group head of operational risk.

At JLT, his role was truly integrated within the business, including engagement with the enterprise risk management, compliance, financial crime, information risk management, regulatory and quality assurance teams.

COGNITIVE BIAS



Between you and the right decision...

Bias skews perception, leading to foolish decisions – here are nine examples which risk managers should know about

CHARLES ORTON-JONES

02

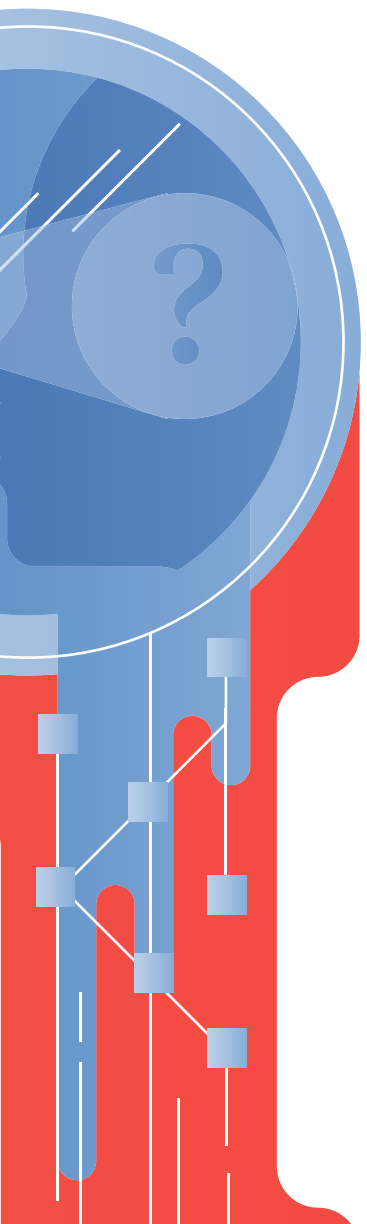
Gambler's fallacy

The original sin of investors is the tendency to assume that bad luck will be compensated by good luck. Karma. Alas, investors are frequently crippled by the belief that the market will magically auto-correct to compensate them for previous losses. Recently the Cboe Volatility Index, known as VIX, which reflects market volatility, tanked. Many investors held on to their positions, praying the market would turn around. It didn't, losing 90 per cent of its value in a single day. "I've lost $4 million, three years' work and other people's money," howled one burnt gambler.

01

Law of large numbers

The godfather of bias detection is Daniel Kahneman, who won the Nobel prize for his work. He revealed that intuition, even in matters we know a lot about, can be awful. For example, imagine two maternity hospitals, one large, one small. In a week, 60 per cent of births are female. Which hospital is more likely to be the venue? It takes time to figure out... the smaller one. Small sample sizes suffer more from deviation from the mean. Kahneman found people of all backgrounds failed to analyse sample sizes adequately. "Even statisticians were not good intuitive statisticians," he concluded.



03 Authority bias

Airline pilots wear smart uniforms for a reason. Not because they belong to a military order. They don't. But because they want to imply authority. This is great for controlling passengers. They obey. The problem is, so do co-pilots. The writer Malcolm Gladwell in his book *Outliers* suggests the Korean Air flight 801 crashed because the co-pilot was too reticent to challenge the pilot about his decisions. Post-crash, British investigators demanded the airline "promote a more free atmosphere between the captain and the first officer" to permit questioning. The air of authority can dupe the best of us. A flash of military insignia, or sharp suit, can short-circuit our normal capacity for analysis.

04 Conservatism bias

It's a misconception that the right approach to risk is solely to minimise it. Risk is a vital and necessary part of life. Conservatism bias is what happens when this is not well understood. For example, consumers leave cash in their current account rather than move to a higher yield deposit. The bias for inaction means they forgo revenue. Conservatism bias is why Blockbuster video turned down the acquisition of Netflix for $50 million. The management found it easier to do nothing than embrace risk.

05 Triviality law

It's exhausting to think about complex issues. Given half a chance, the human mind will make a break for a simpler, trivial issue to distract itself. Politics is dominated by this effect. Major issues, such as a politician's view on the national debt, are rarely discussed or reported. Too hard. Instead the focus is on trivial issues, such as whether they can eat a bacon sandwich with dignity. This is a serious issue in risk. It takes effort to get people to think about critical issues, such as life insurance, or the design of a nuclear power station. Given the chance they'll veer off and focus on something fluffy and trivial, to spare their grey cells.

06 Risk compensation

The British Medical Journal recently came out against bicycle helmets. It's not that helmets don't work. Fall off and you'll be grateful your fragile skull is encased in protective plastic. Rather, the phenomenon of risk compensation negates the benefit. Data from multiple nations shows that when cyclists feel safer they compensate, by taking extra risks, cutting in front of cars and not looking at junctions. Individuals with documented helmet use had 2.2 times the odds of non–helmet users of being involved in an injury-related accident. Furthermore, mandatory helmet wearing reduced cycling, adding to negative effects.

07 Social proof

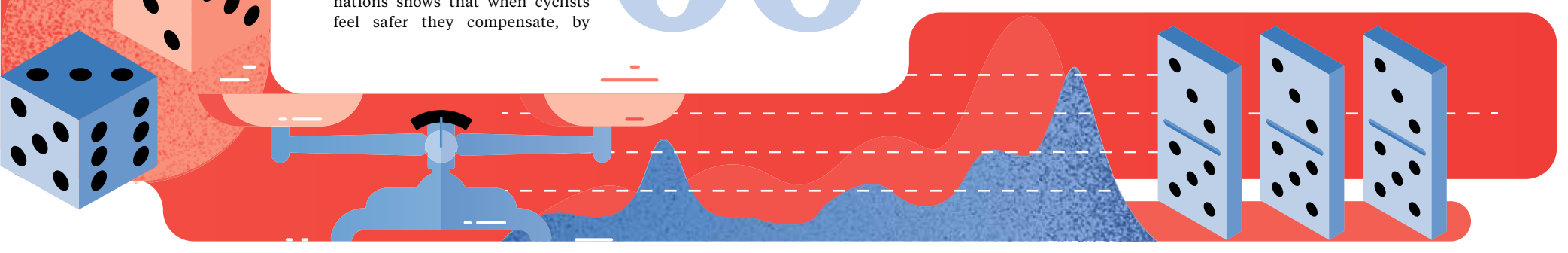
The legendary investor Charlie Munger believed his research into cognitive biases led him to better risk decisions. He marvelled at the beguiling power of effects such as social proof, writing: "Big-shot businessmen get into these waves of social proof. Do you remember some years ago when one oil company bought a fertiliser company, and every other major oil company practically ran out and bought a fertiliser company? And there was no more damned reason for all these oil companies to buy fertiliser companies, but they didn't know exactly what to do and if Exxon was doing it, it was good enough for Mobil, and vice versa. I think they're all gone now, but it was a total disaster."

08 Charm pricing

Human reaction to numbers is riddled with quirks. Richard Shotton's new book *The Choice Factory* examines the ability of businesses to harness these biases to influence consumers. For example, tweaking prices by a fraction can boost sales. Discount stores use charm pricing, knocking a penny off to end in "99". Shotton says: "I surveyed 650 consumers about their value perception of six different products. Half saw prices ending in 99p, while the remainder saw prices a penny or two higher. Charm prices were 9 per cent more likely to be seen as good value than the rounded prices. A disproportionately large improvement for a 1 per cent price drop."

09 Overconfidence bias

Sure, we all know about Dunning-Kruger: the idea that dim people overestimate their skills, while bright people doubt their abilities. But could it be that even experts are overconfident? Alas yes, especially when forecasting. Economist Philip Tetlock spent 20 years studying forecasts by experts about the economy, stock markets, wars and other issues. He found the average expert did as well as random guessing or as he put it "as a dart-throwing chimpanzee". Tetlock believes forecasting can be valid, but only when done with a long list of conditions, including humility, rigorous use of data and a ruthless vigilance for biases of all types. "I believe it is possible to see into the future, at least in some situations and to some extent, and that any intelligent, open-minded and hard-working person can cultivate the requisite skills," he said. It's a challenge at the heart of the risk industry.



NATURAL DISASTERS

Fighting back when a disaster strikes

Hurricanes, flooding, volcanic eruptions, earthquakes, tsunamis, bush fires – all wreak havoc and dislocate global supply chains, but a disaster doesn't have to shut down business

ADAM FORREST

Natural disasters may be unavoidable, but they do not have to be overwhelming. Businesses are not doomed to suffer in the aftermath, so long as plans have been made to minimise the risks and manage the knock-on impacts as effectively as possible.

The huge challenges posed by Mother Nature should not be underestimated, however. As supply chain managers know all too well, an interconnected global economy means the financial consequences of any catastrophe ripple around the world very quickly.

There is also growing concern about the increased frequency of extreme weather events. Reinsurer Munich Re says climate change could mean the fierce hurricanes in the Caribbean and United States, and severe flooding in South Asia during 2017 could be a "foretaste of the future". The latest *Allianz Risk Barometer* puts natural catastrophes among the top three global business risks for 2018.

According to Munich Re's annual review, natural disasters caused $330 billion (£231 billion) in overall losses last year. Such events often result in the interruption of supplies and can leave some companies unable to fulfil their commitments to customers, leading to subsequent losses in revenue and profit. There is also the danger of reputational damage. If a crisis is handled badly, it can mean a permanent loss of market share.

The stakes, then, are extremely high. So what can those in charge of supply chains learn from recent natural disasters? How might they utilise the latest risk management techniques and advances in technology to prepare much stronger contingency plans?

The US response to the hurricane season of 2017 offers plenty of good lessons. Across Texas, roads were badly flooded and the Port of Houston was closed for almost a week after Hurricane Harvey hit, causing major delays in shipments. The three category 4 hurricanes that swept across the Caribbean and America during September – Harvey, Irma and Maria – eventually caused $215 billion (£150 billion) in overall losses, according to Munich Re.

Yet given the enormous scale of these events, US businesses coped reasonably well because of detailed contingency plans. Many companies had arranged for alternative trucking and shipping routes, and managed to move materials, consumer goods and personnel before the worst of the weather hit.

Delivery giant UPS saw profits fall in the third quarter of 2017, partly as a result of problems caused by the hurricanes. The company sought to reassure customers it would be ready to withstand more such weather events in future, announcing major investment in storage capacity for 2018.

Roads across Texas were severely flooded in the aftermath of Hurricane Harvey last summer, with a week's closure of the Port of Houston causing major delays to shipments

"Having excess capacity in place is an expensive decision, but companies have learnt how useful it can be," says Dr Panos Kouvelis, director of the Boeing Center for Supply Chain Innovation at Washington University in St Louis. "I think businesses in the US have become better at anticipating and planning for hurricanes. Many companies were surprised by the magnitude of the impacts of Hurricane Katrina in 2005, but they have learnt a lot of lessons and have been building more resilience in the supply chain."

Building resilience can involve big strategic decisions. If natural disasters remain a strong possibility in part of the world where key suppliers exist, companies may be wise to consider moving a proportion of their business to suppliers elsewhere. "With really critical products, even if it costs a bit more, it's worth thinking about diversifying your suppliers that way," says Professor Brian Squire, who leads the HPC Supply Chain Innovation Lab at the University of Bath School of Management.

Technology has given businesses tremendous opportunities to reduce risk. Advances in satellite imagery have supplied companies with more detailed weather forecasts and the chance to assess likely impacts on particular geographical locations. Data analytics and modelling software let supply chain managers see how a potential problem in one area affects every other aspect of the business.

"The modelling tools can help you to map out your supply chain vulnerabilities with incredible accuracy," says Julia Graham, deputy chief executive and technical director at the Association of Insurance and Risk Managers (Airmic). "I see organisations doing incredibly sophisticated work these days, mapping dependencies and eventualities in great detail."

The larger the business, the greater the need to think holistically about the supply chain. Digitisation can help fuse different aspects of a business together to make sure there are no gaps in information if a disaster should strike.

> **Catastrophes can sink those caught off guard, but a well-prepared company should feel confident about filling the void left by less nimble competitors**

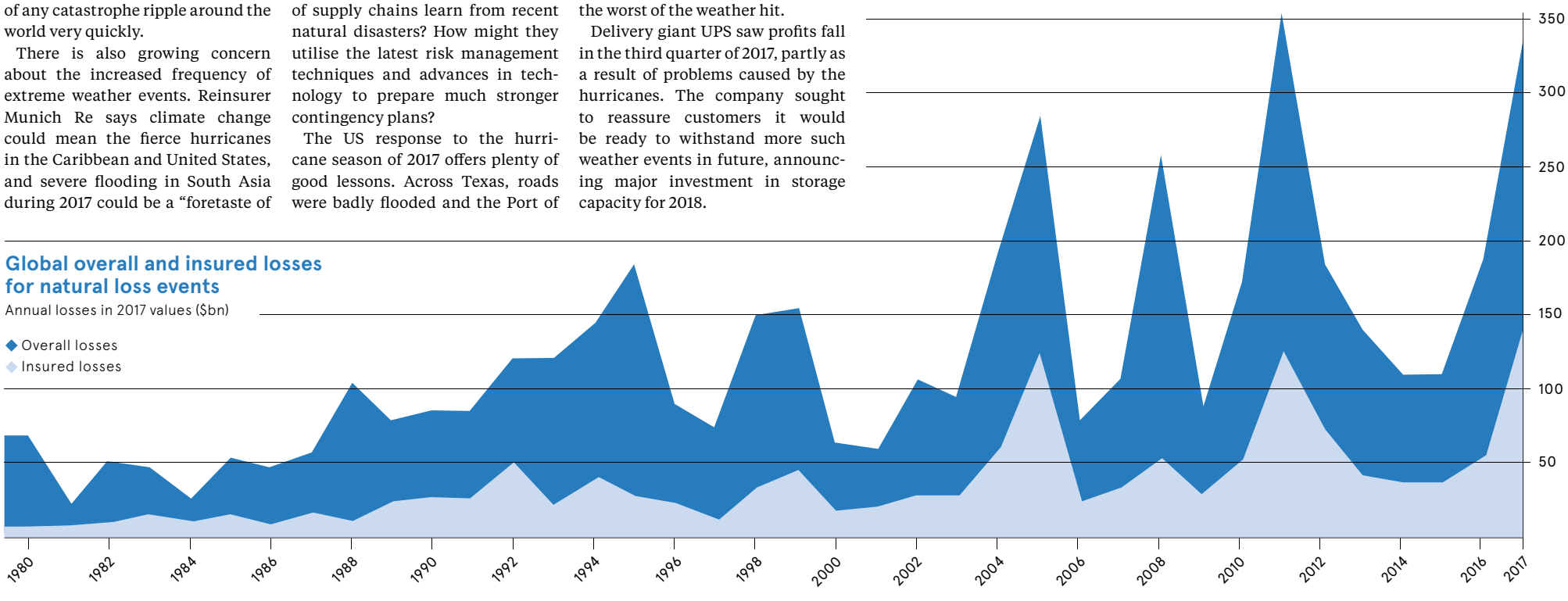
"When an organisation is small, everyone tends to know what's going on," says Suki Basi, chief executive of Russell Group, the risk management and software services company. "As it grows larger, there is a tendency for the left hand not to know what the right hand is doing. But technology can help larger organisations integrate operations and increase the speed of decision-making."

Agility in a time of crisis can also depend on forging relationships with leading charities working on the ground. "Some of the NGOs are heavily involved in data analytics and they can help businesses understand what's likely in the aftermath of an extreme event," says Ms Graham. "Risk is more connected than ever before and if you want connected answers to risks, you have to be open to collaboration."

The havoc wreaked by natural disasters might lead to some mutually beneficial partnerships, but the battle for customers never stops. Catastrophes can sink those caught off guard, but a well-prepared company should feel confident about filling the void left by less nimble competitors. ◆

Global overall and insured losses for natural loss events

Annual losses in 2017 values ($bn)



Munich Re 2018

OPINION COLUMN

‘Time for the C-suite to take a fresh look at risk’

On the office wall at Airmic is a poster for our 1994 annual conference entitled: “Turning risk into opportunity.” The message that risk management is not just about nasty things, but also what businesspeople really want – opportunity, new markets, enterprise – has clearly been around for at least 24 years. However, has it got through to our colleagues and above all to the C-suite?

The frustrating truth for those who care passionately about the benefits of risk management is that the subject remains a turn-off for too many board members and other senior executives. While the profile of risk management is probably higher than ever, it still has negative connotations. In football parlance, we are seen as the defenders who stop goals rather than the creative mid-fielders who hold the team together or the strikers who set the crowd alight.

And, if we are honest with ourselves, we are partly responsible for allowing this misleading perception to develop.

Our message is that a robust risk culture will nourish the entire organisation, providing the board with vital information and creating the platform for it to be enterprising and innovative. *Roads to Resilience*, published by Airmic in 2014 and based on research by the Cranfield School of Management, established a clear link between sound enterprise-wide risk management and commercial success, including long-term profitability.

Risk managers can be a unifying force, enabling an organisation to achieve its ambitions. To be a strategic risk manager is to be an accomplished networker and to have an overview of the enterprise. This means understanding its strengths, its weaknesses, its culture and its objectives. It means using risk management explicitly to support corporate strategy in a positive way, and talking and behaving like a businessperson.

This type of executive does not even have to have the word “risk” in their job title, but for simplicity’s sake let’s call them the chief risk officer or CRO. Such a person should be the eyes and ears of the board, and a key support for the chief executive.

Non-financial CROs are extremely rare in the UK, though they are more common on the Continent and in North America. This deficit needs to be made good if risk management is to fulfil its true potential to help UK plc.

How, then, do we improve understanding of risk? At the heart of the problem is that “risk” is what my old English teacher used to call a lazy word, like “nice”. It is used in so many ways that it loses its power to improve understanding and to change perceptions. People need to make their message relevant, timely, new and nuanced. By simply using the word “risk”, without explaining where it fits into the value chain, it can sound old and tired.

Risk managers often shy away from talking about the value of their work because so much of what they do is to prevent things from happening. The trick is to move beyond something that did not happen and that, in any event, colleagues would rather not think about. Talk as well about the trusted characteristics of a brand that build up over time.

Discussing objectives is a good first step, but it goes further than that. Risk managers must align their message with the purpose of the organisation, its language, culture and objectives. Telling people that, in the worst-case scenario, the end of the world could be nigh does not win friends or gain you influence.

Young risk managers in particular are keen to embrace and indeed help shape the new business world. Airmic is working with its members to build on their already formidable technical skills, and to prepare for the most senior and strategic risk roles. At the same time, it is very much in the interest of the C-suite to take a fresh look at risk and how it can become an even greater force for good.

John Ludlow
Chief executive
Airmic – the risk management association

Commercial feature

Building resilience in travel risk mitigation

A wide range of adverse incidents and geopolitical tensions have highlighted the need to protect an increasingly mobile workforce

Hurricanes in the Caribbean, terror attacks in places previously considered safe, disease outbreaks such as the plague in Madagascar, and even recent political tensions around Russia and North Korea – such events have all been changing actions and attitudes towards the health, safety and security of the workforce.

Increasingly, this protection is also recognised as a critical aspect of maintaining business resilience and sustainability. If you have an international workforce, your business objectives and brand reputation could be at risk from such incidents, in addition to the impact on personnel.

Almost two thirds of business decision-makers perceive travel risks to have increased in the past year, according to the *Ipsos MORI Global Business Resilience Trends Watch 2018*. Travel plans were changed, predominantly due to concerns over security threats (58 per cent), natural disasters (43 per cent) and civil unrest (34 per cent).

While organisations are increasingly implementing prevention and mitigation measures, there are still opportunities for them to improve as major strategic aspects are being missed.

Access to time-critical information is key before, during and after any trip. Travellers with insight on their destination, access to appropriate preparation, and around-the-clock global support and assistance are better placed to identify and mitigate travel-related hazards and threats. For instance, a robust travel risk mitigation programme would include risk-rating indicators supported by additional destination insight and advice. It would also include travel security and medical alerts relating to destinations, both on the ground and supported remotely.

While organisations are increasingly implementing prevention and mitigation measures, 90 per cent are ignoring the impact a wellbeing policy could have on their travelling workforce

While the preventative agenda in medical and travel risk mitigation is on the rise, decision-makers reveal that a strategic and far-reaching view may be a missed opportunity by many organisations. A staggering 91 per cent of organisations have potentially not included their travel risk programme in their overall business sustainability programme.

Also 90 per cent are seemingly ignoring the impact a wellbeing policy could have on their travelling workforce as this fell at the bottom of risk-mitigation techniques implemented in 2017. This is despite an increasing understanding of how these wellness techniques can impact within the context of the Global Reporting Initiative index.[1]

Companies are prioritising risk-mitigation techniques. These include travel security and medical interventions, such as annual health check-ups, which can be key to spotting potential health issues that need managing prior to travel or assignments.

However, organisations report that they continue to encounter barriers to health and travel security. Educating employees about travel risk is the most common challenge, followed by communicating with employees in a crisis and ensuring they have read pre-travel information. All these are critical aspects to protecting the global mobile workforce.

Understanding the risks, and implementing risk mitigation and assistance, are key to keeping the travelling workforce on the go and able to fulfil their business aims.

In future, successful global mobility programmes will also include consideration of the changing demographic of the mobile workforce and new marketplace dynamics, including the increased use of shared economy services such as Uber and Airbnb. The immediate risks, such as hurricanes, disease outbreaks and unforeseeable security incidents, will see organisations scrutinised in terms of preventative measures and recovery.

1 Sancroft and International SOS Foundation, *Occupational Health & Safety and Workplace Wellness Reporting Guidelines for a Global Workforce: A Practical Guide for Internationally Operating Employers*

Changes in risk to travellers

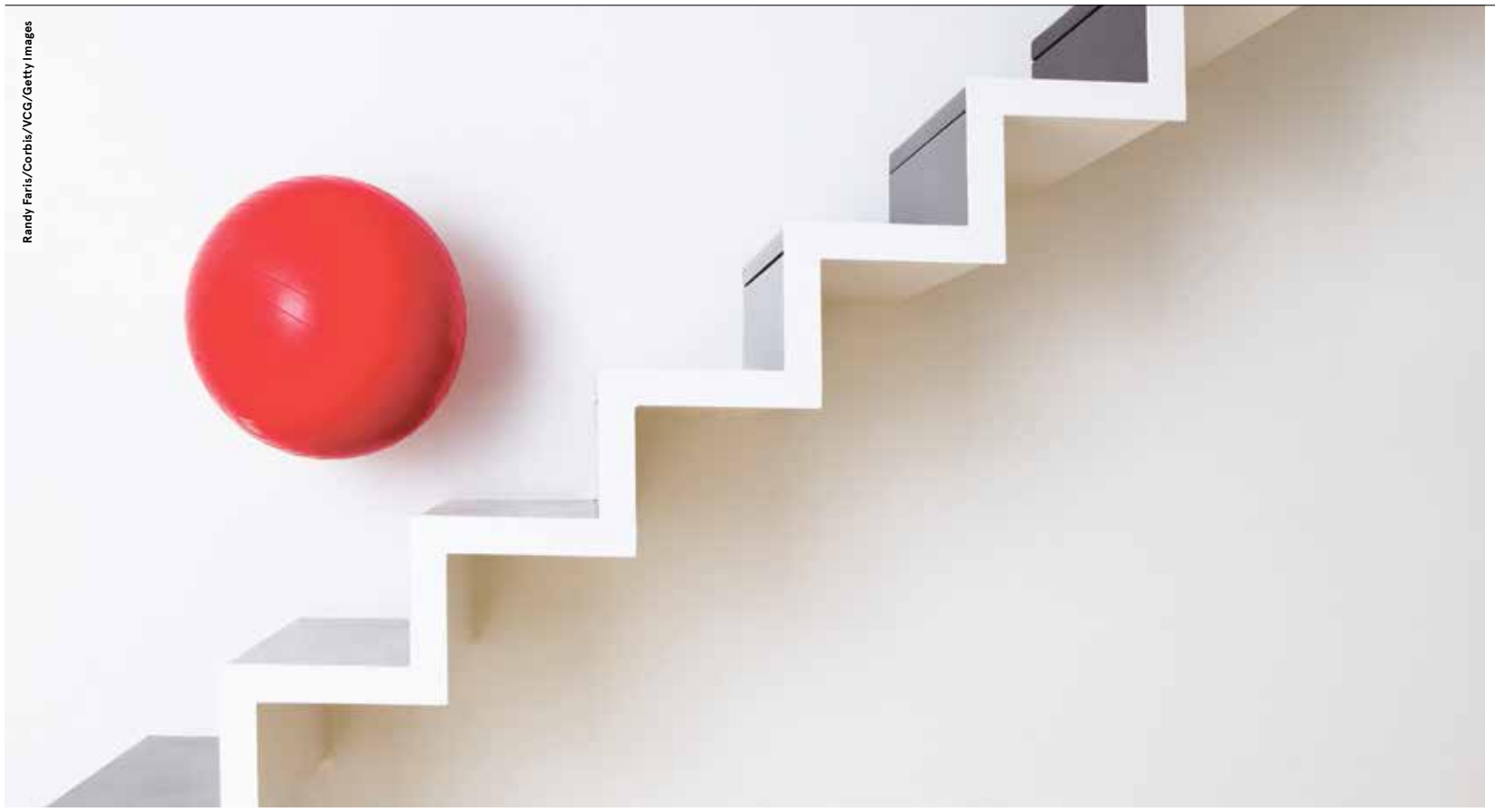
63%
say travel risks have increased over the past year

52%
expect travel risks to increase in 2018

For more information please visit www.internationalsos.com

INTERNATIONAL SOS
WORLDWIDE REACH. HUMAN TOUCH.

COMPANY CULTURE



Randy Faris/Corbis/VCG/Getty Images

Numbers can help develop individuals

Tension remains over whether it's best to run a business with a growth or performance-based culture

CATH EVERETT

Many organisations will find it necessary to adopt a growth culture over the years ahead or risk not being responsive enough to adapt to the change they are likely to face.

On the one hand, reinventing themselves will prove vital to attract the right talent. On the other, making the most of increased automation and artificial intelligence will require a cultural shift that, paradoxically, puts humans and their capabilities at the heart of the business.

According to research published in the *Harvard Business Review*, a growth-based environment comprises four key elements. The first is a safe, rather than blame, culture, in which both leaders and employees are prepared to take responsibility for their own errors and shortcomings.

Next is a focus on continuous learning and development based on curiosity rather than self-protection. The third is a willingness to engage in experimentation, which is treated as an opportunity for individuals to grow rather than be seen to fail if things do not work out.

The final element involves encouraging continual feedback at all levels of the organisation based on a mutual shared commitment to help each other improve.

A more traditional performance-driven culture, meanwhile, is one in which financial results matter more than individual growth and leaders tend to be autocratic rather than pragmatic.

But as James Beazley, chief executive of executive search and leadership advisory consultancy 6 Group, points out: "If you have a pure performance culture, the danger is you're less agile as you're so focused on hitting your numbers, irrespective of what your customers and the markets are telling you. So you might hit them this quarter, but it's a big risk for the future."

Perhaps surprisingly then, the number of companies that have introduced a growth culture is still relatively low. While particularly rare in heavily regulated industries, such as pharmaceuticals, they are more common in fields like manufacturing that are used to not dissimilar methodologies such as lean.

The approach is also coming to the fore among startups, especially in the technology space, which have been using comparable agile techniques for some time.

However, there are risks inherent in moving to a growth-based culture too. For instance, the average tenure of a UK chief executive has dropped from 8.3 years in 2010 to 4.8 years in 2017, according to PwC's *CEO Success Study*. But this scenario presents problems should leaders wish to introduce cultural change, which can take a long time to bed in and show benefits.

"Growth cultures don't necessarily translate into having your financial objectives met quickly," says Mr Beazley "This means you really have to be quite strong to want to start driving a whole new approach that's not purely focused on numbers."

Another point to bear in mind, says Kirsta Anderson, a senior client partner at management consultancy Korn Ferry Hay Group, is when driving cultural change, the number-one success factor is for chief executives truly to believe their personal success depends on it, which most do not.

The second most important is that leaders are open to learning from feedback as well as being able to "demonstrate some level of vulnerability", she says. But underpinning such behaviour in both instances is whether they have a fixed or growth mindset.

People with the former, who account for the majority, think of intelligence as a fixed trait that does not change over time. As a result, they are resistant to feedback, see it as a criticism and are threatened by the success of others.

People with a growth mindset, however, take the opposite approach. Because they believe their intelligence can develop, they embrace challenges as an opportunity to learn and are inspired by others' achievements.

Ms Anderson explains: "Whether an organisation has a performance or growth culture depends on the mindset of their leaders. So when trying to bring about change, the key thing is to realise that your own underlying mindset can drive the wrong behaviour and results."

> **The most successful growth cultures are hybrid ones in that they still have some performance metrics, but they're used only as a tool rather than the final measuring stick**

One company that has taken a growth-based approach from the outset is startup Party Hard Travel, which organises clubbing holidays for 18 to 30 year olds, and took on its first staff in January 2016, of which there are now eight.

Each employee, once they have been hired, undertakes a Myers Briggs personality test. The aim is to discover more about them to help transition them into the job they are most suited to, even if it is not the role for which they were originally recruited.

In a bid to ensure a process of continuous improvement, co-founder Barry Moore also holds weekly one-to-one meetings with each staff member, who is asked five questions. They focus on one thing they love or loathe about working for the company, one thing they or the company could improve upon and one thing the company should start doing.

"It means we can find out about any problems early on and come up with new ways of doing things," he says.

But if not managed carefully, the danger is that Mr Moore's kind of open-door approach and willingness to discuss and review strategic decisions can result in a consensus-driven culture, where nothing ever happens, warns Mr Beazley.

"The risk is that you try to please everyone, but do nothing so there has to be a balance," he says. "The most successful growth cultures are hybrid ones in that they still have some performance metrics, but they're used only as a tool rather than the final measuring stick." ◆

Four elements of growth culture

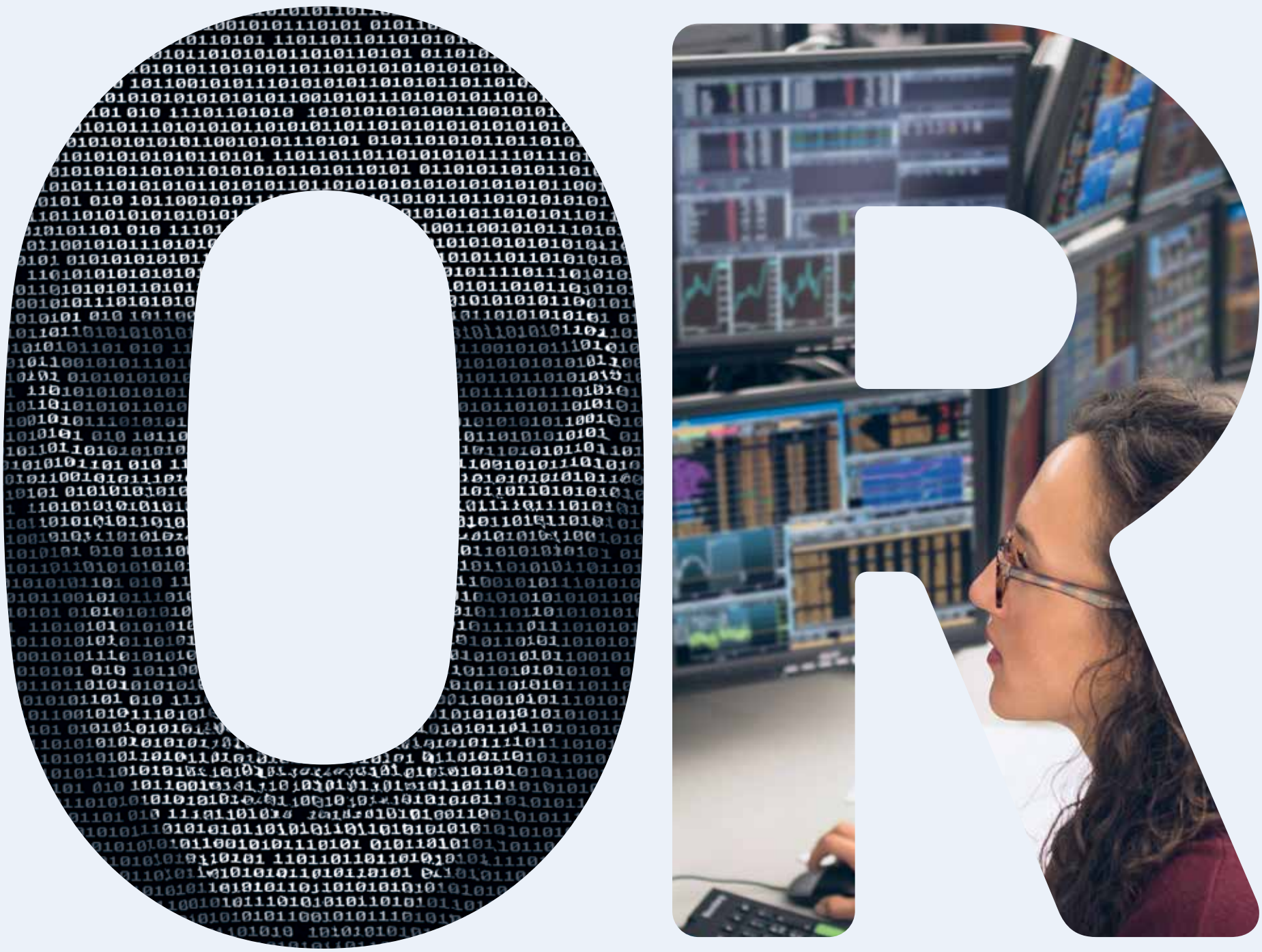
01 **SAFE** Both leaders and employees are prepared to take responsibility for their own errors and shortcomings

02 **LEARNING** Continuous learning and development based on curiosity rather than self-protection

03 **EXPERIMENTS** Treated as an opportunity for individuals to grow rather than be seen to fail if things do not work out

04 **FEEDBACK** Based on a mutual shared commitment to help each other improve

Tony Schwartz/*Harvard Business Review*



CYBER DAMAGED **OR** CYBER RECOVERY?

Cyber security can only do so much to prevent attacks. Fight back with a full suite of cyber insurance products designed to help prevent loss and aid in recovery.

Find out more at fmglobal.co.uk/advantagepolicy

RESILIENCE IS A CHOICE.

Proud partner of airmic

See us at Stand 85

FM Global

COMMERCIAL PROPERTY INSURANCE

WE PAID OUT 99% OF CLAIMS, SO YOU FEEL BETTER PROTECTED.

When you are buying home, motor, life, or business insurance, it's good to know that you'll get the protection you are paying for. From January – December 2017, on average we paid out on 99% of insurance claims our UK customers made. So should you need to claim, you can rely on Zurich Insurance.

SEARCH ZURICH 99

ZURICH®

Business | Home | Life | Motor