Issue 104

Strategic RISK

Risk and corporate governance intelligence

Q1 2016
EUROPE EDITION

CAUGHT IN THE BLAST

For a long time, crisis management dealt with emergencies like fires and explosions – but with outrage liable to blow up any time on social media, the rules have changed **p20**

www.strategic-risk-global.com

Swiss Re
Corporate Solutions

You know your business inside out. You know your markets, your customers, your competitors. Above all, you know the risks facing your business. At Swiss Re Corporate Solutions, we have the capabilities and the financial strength to meet the risk transfer needs of businesses worldwide. But that's only half the story. Whether your risk is basic or complex, whether the solution is off-the-shelf or highly customised, we believe that there's only one way to arrive at the right solution. And that's to work together and combine your experience with our expertise and your strengths with our skills. Long-term relationships bring long-term benefits. **We're smarter together.**

swissre.com/corporatesolutions

Issue 104
Q1 2016
EUROPE EDITION

StrategicRISK

www.strategic-risk-global.com

EDITOR-IN-CHIEF
Mike Jones

EDITOR
Europe
Kin Ly

ASSISTANT EDITOR
Europe
Ilonka Oudenampsen

EDITOR
Asia-Pacific
Jessica Reid

EXECUTIVE EDITOR
Asia-Pacific
Sean Mooney

HEAD OF SALES
Andrew Stone

COMMERCIAL DIRECTOR
Asia-Pacific
Adam Jordan

SENIOR PRODUCTION CONTROLLER
Alec Linley

SENIOR DATA ANALYST
Fayez Shriwardhankar

PUBLISHING MANAGER
Tom Byford

PUBLISHER
Jack Grocott

EXECUTIVE PUBLISHER
Asia-Pacific
William Sanders

MANAGING DIRECTOR
Tim Whitehouse

email: firstname.surname@nqsm.com

Cover image Shutterstock

ISSN 1470-8167

PUBLISHED BY
Newsquest Specialist Media Ltd

LONDON OFFICE
30 Cannon Street, London EC4M 6YJ
tel: +44 (0)20 7618 3456
fax: +44 (0)20 7618 3420 (editorial)
+44 (0)20 7618 3400 (advertising)

ASIA-PACIFIC OFFICE
3/50 Carrington Street, Sydney,
NSW 2000, Australia
tel: +61 (0)2 8296 7611

HONG KONG OFFICE
Suite 1003, 43-55 Wyndham Street,
Central, Hong Kong

email: strategic.risk@nqsm.com

FOR ALL SUBSCRIPTION ENQUIRIES PLEASE CONTACT:

Newsquest Specialist Media,
PO Box 6009, Thatcham, Berkshire,
RG19 4TT, UK

tel: +44 (0)1635 588868

email: customerservice@strategicrisk.eu
Annual subscription (incl P&P)
£249 €399 $499
Two-year subscription
£449 €649 $849
Three-year subscription
£427 €663 $821

Printed by Warners Midlands Plc

Oil collapse affects insurance buying budgets
›P8

Lessons from MH370 and MH17
›P10

Contents

COMPLAINTS – WHO TO CONTACT
StrategicRisk adheres to the Editors' Code of Practice (which you can find at www.ipso.co.uk.)
We are regulated by the Independent Press Standards Organisation. Complaints about stories should be referred firstly to the editor-in-chief by email at: complaints@strategic-risk-global.com or by post at Mike Jones, *StrategicRISK*, 30 Cannon Street, London EC4M 6YJ.

It is essential that your email or letter is headed "Complaint" in the subject line and contains the following information:

- Your name, email address, postal address and daytime telephone number.
- The newspaper title or website, preferably a copy of the story or at least the date, page number or website address of the article and any headline.
- A full explanation of your complaint by reference to the Editors' Code.

If you do not provide any of the information above this may delay or prevent us dealing with your complaint. Your personal details will only be used for administration purposes.

If we cannot reach a resolution between us then you can contact IPSO by email at complaints@ipso.co.uk or by post at IPSO, c/o Halton House, 20-23 *Holborn, London EC1N 2JD.*

Guiding lights in a changing world

We've picked the experts' brains on 'Brexit' and the evolution of crisis management

In just two months, the British public will vote on one of the most important referendums in British history – whether to remain in the European Union or to Brexit.

The consequences for economic growth, trade, British businesses and their European counterparts are being hotly discussed. Both sides are campaigning aggressively, with brash projections offered about how the UK will look, in or out of the EU.

In all of this, the lines between political dogma and good, honest analysis become blurred, making it difficult to identify what the risks for corporates might be. So in a special report on pages 14-19, we spoke to economists, insurers and risk managers to highlight the key threats and challenges.

One issue is how much weight the European migrant crisis will have on voting behaviour (pp14-16). No clear conclusions can be drawn, but the conversation sparked a more detailed discussion about crisis management in general.

With technological advances, social media and 24-hour news cycles, incidents can spiral out of control, leaving corporates more vulnerable to crises than ever. In this socially and virtually connected world, crisis management has evolved. It is no longer deployed only in labour-intensive sectors for managing physical emergencies, but is used to mitigate intangible threats too. Control Risk and Deloitte, along with corporate risk managers across various sectors, review crisis management in this new world (pp20-25).

On a final note, welcome to the new and improved A4 version of *StrategicRISK*. We've kept all the best sections and added some new ones, including The Knowledge (p26-31), a series of industry surveys that provide insight on some of today's most pressing risks.

Happy reading

Kin Ly

EMAIL › kin.ly@nqsm.com

THE LINES BETWEEN POLITICAL DOGMA AND HONEST ANALYSIS ARE BLURRED, MAKING IT DIFFICULT TO IDENTIFY WHAT THE RISKS FOR CORPORATES MIGHT BE

HELP TAKE CARE OF YOUR PEOPLE AND BUSINESS TOGETHER.

With Zurich, you can get a variety of tailored global solutions: employee benefits, liability and property insurance. And if you consolidate them into a single captive it could be financially beneficial – giving you greater control of your insurance portfolio.

FIND OUT MORE AT zurich.com/captives

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.

ZURICH®

Mars hangs on to its sweet reputation after recalling millions of chocolate bars

StrategicRISK readers say the confectioner's swift actions probably limited damage among consumers

In the wake of the TalkTalk hack and Volkswagen emissions scandal – which left both brands crippled by falling sales in 2015 – reputation damage and its causes crept higher up the risk register of many multinational corporations.

So when confectioner Mars recalled millions of chocolate bars, including Mars, Snickers and Milky Way, corporates were quick to ask whether it would suffer a similar fate.

Product recall is commonplace for the food and drinks business, but this was on a relatively large and potentially damaging scale.

Mars issued an international recall across 55 countries, among them the UK, France, Germany and the Netherlands, after a German customer found a piece of red plastic in his Snickers bar in January.

The plastic was traced back to a faulty machine in one of its factories in the Netherlands.

As the incident unfolded, signs pointed to a possible reputation crisis as news spread quickly across Twitter and Facebook of supermarket chains removing Mars products from their shelves.

But three months after the recall, risk managers say any brand damage is likely to be short-lived because of how Mars managed the contamination.

One, who works for a global company that provides catering and hospitality services, says: "The incident might have a slight impact on consumer confidence. But it is likely that the general public sees the recall as a good move and this will only strengthen brand appreciation by consumers."

The risk manager, who prefers not to be named, adds: "Mars still has the ability to get consumer mileage out of the recall, if marketed in the right way."

According to the Reputation Institute, a global research and advisory firm, it may even bounce back quickly from any shortfall in sales during the immediate aftermath of the recall.

Edward Coke, the company's UK director of consulting, says: "We have not conducted any recent research into consumer perceptions of Mars following the recall, but our normative data suggests that Mars's strong reputational capital will likely take a short-term hit, which would result in a degree of reduced sales.

"However, the investments the company has made in reputation before this time, supported by adept

NEWS IN BRIEF: Q1

A round-up of industry news that made our headlines: strategic-risk-global.com

The merger of Willis and Towers Watson was successfully completed. On the same day, Willis announced it had completed the acquisition of Gras Savoye. The French brokerage firm will keep its name and brand: **bit.ly/1RwQgsG**

Axa Matrix Risk Consultants appoints Laurent Barbagli as new chief executive. Barbagli was previously risk manager at building materials producer Lafarge Group.: bit.ly/1RzkGfR

Failure to address climate change is cited as the most impactful global risk, according to the World Economic Forum. Its *Global Risks Report 2016* also said global risks are imminent and more interconnected: **bit.ly/22Ccayj**

crisis management, are likely to help the company recover from this set-back relatively speedily."

In a poll asking *StrategicRISK* readers how the brand's reputation will fare, 67% said it would suffer no damage at all. Other potential outcomes – 'sales will drop slightly', 'sales will drop drastically', and 'general reputation damage' – scored 11% each.

The company's post-recall sales figures were not available at the time of writing, but if the poll is anything to go by, Mars did well to limit its reputation damage. So, what can global food and drinks firms learn from the brand?

SPEED MAKES ALL THE DIFFERENCE

As the confectioner has shown, speed is vital. The German customer made his complaint in January. After identifying the source of the problem, Mars issued its recall a short time later, in February.

Speed can make all the difference for companies who find themselves in a similar situation, says the Reputation Institute's Coke.

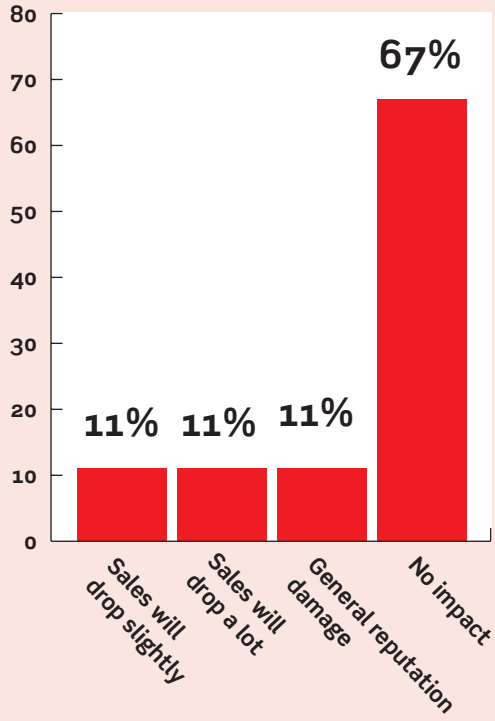
"If a company is regarded by the media as slow to act, or fails to proactively communicate the steps it is taking, the reputational risk broadens to include not only perceptions of the product in question, but also other important dimensions of reputation such as the leadership of the company."

The next consideration for any company managing food contamination is transparency.

"If companies are perceived as initially denying the need for a recall or hiding corporate misbehaviour, such as the 2008 melamine baby milk scandal in China, the reputational impact can be hugely damaging," Coke adds.

"If, however, the recall is viewed more as a preventative measure undertaken by a company to protect consumer interests, the reputational impact can be limited."

How will the recent Mars recall affect its brand?



As Mars publicly explained, its recall was voluntary and made as a safety measure.

Widespread recall does not mean that all products are contaminated, explains Christof Bentele, head of global crisis management at Allianz Global Corporate & Specialty: "Rather, a mass recall reflects a highly concentrated production source, with high output levels. As such, the most prudent approach for a manufacturer to take is to recall any product which could have potentially been affected during a production run, or that has been created by a faulty machine."

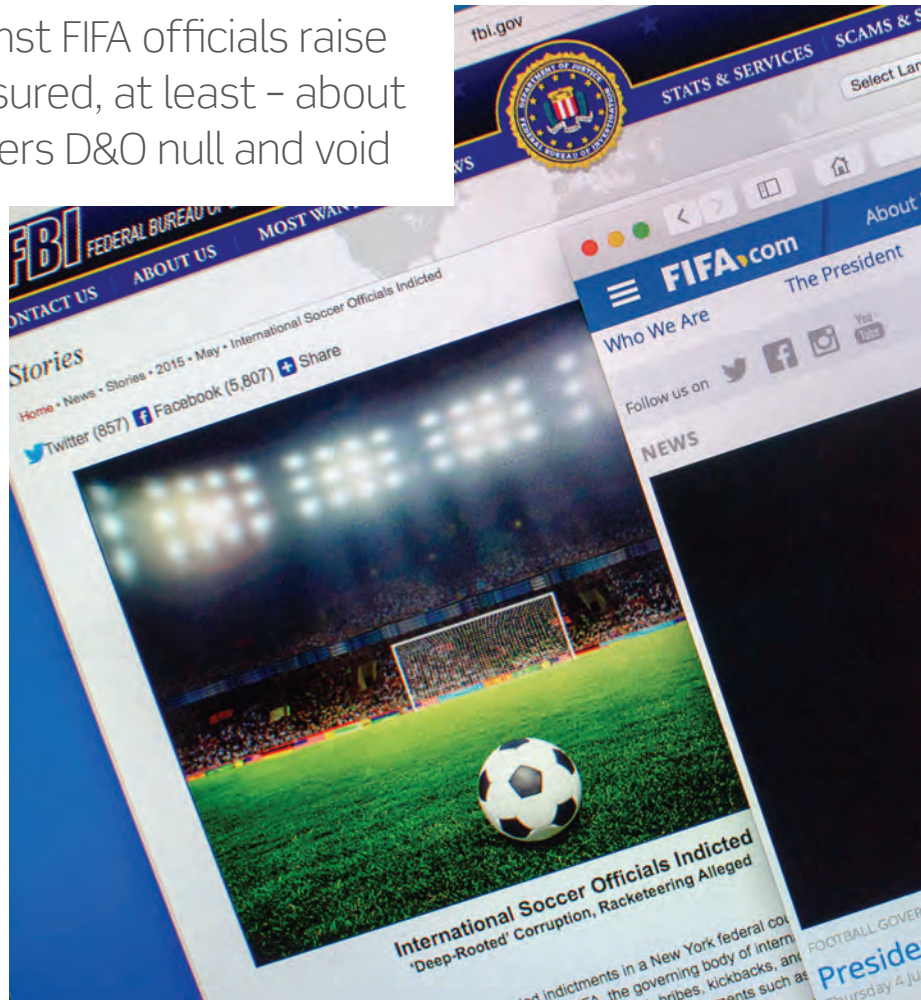
Mars may emerge unscathed from this intensely challenging situation. But as recent product recall headlines have shown, it may be one of few global companies to do so. **SR**

AXA Corporate Solutions names Rob Brown as its new chief executive. Brown joins from Aon, where he was most recently chief executive of Aon Risk Services across EMEA: **bit.ly/1Rdpq8P**

ACE completed its takeover of Chubb. The new combined company has adopted the Chubb name. In the weeks following the news, Chubb appointed its new senior management team for the UK and Ireland, and its Continental Europe business: **bit.ly/1VzD2NJ**

Good grounds for cancelling the cover?

The corruption charges against FIFA officials raise disturbing issues – for the insured, at least – about whether bad behaviour renders D&O null and void



The wholesale indictments of current and former officials of FIFA, not to mention the investigations into some of the top people at its athletics counterpart, the IAAF, raise disturbing issues about D&O cover in cases of bribery and corruption. Disturbing for the insured, that is.

The burning issue is when exactly – or if – D&O is invalidated by a director or officers' behaviour. For instance, while most policies cite acts of fraud and other criminal offences as a sufficient trigger to cancel the cover and leave the insured high and dry, the misdemeanours generally have to be proved first.

And then there's the "prior knowledge" exclusion. If the insured knew of corrupt practices that occurred before a D&O policy was written but did not tell the insurer, that may also give the carrier a let-out.

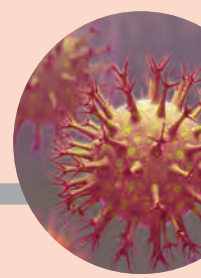
Nor does retirement close the book. Under some legal systems, as in Germany for instance, directors remain liable for prosecution for up to 10 years after they have retired.

And finally, the fraught matter of "allocation". If an organisation is sued, generally by a government agency, for bribery and corruption, how far down the line does the D&O cover go?

Perhaps, as law firms point out, executives or other officers may be left exposed for having, say, acceded to a director's request to pay kickbacks through

Zurich appoints Mario Greco as chief executive. Currently chief executive of Generali, he will be joining the Swiss insurance group on 1 May: **bit.ly/1XJQddm**

The World Health Organisation declares Zika virus a global public health emergency. Mostly present in the Americas, the mosquito-transmitted virus can cause brain damage in infants: **bit.ly/25mVWeQ**



The coming years will see more global megadeals in the insurance industry, following a record $143.5bn (€129m) worth of M&A transactions in 2015, says Willis Towers Watson in its insurance M&A report: **bit.ly/1KcP6RK**

secret bank accounts. In the meantime – as more and more countries, prompted by US investigators, adopt tougher anti-corruption regulations – directors' exposure to these kinds of regulations is growing on a daily basis, just about.

As Edward Smerdon, a D&O specialist in London-based law firm Sedgwick Detert Moran and Arnold pointed out in a report by ACE (now Chubb) on the subject released in December, jurisdictions everywhere are becoming less and less forgiving of ethical breaches.

"Europe, China and India, for example, are tightening their corruption laws. That's a theme we're seeing," he explains. "Key US laws such as the Foreign Corrupt Practices Act (FCPA) are being followed by other countries because they don't want US authorities poking their noses into their jurisdictions."

RAMPANT, SYSTEMIC, DEEP-ROOTED

But to get back to FIFA. The D&O issue within the football body is complicated because a hard core within the organisation has spilled the beans.

In mid-2015, US authorities indicted 14 current and former officials and associates on charges of "rampant, systemic and deep-rooted" corruption, as law firm Clyde & Co recalls in a report on the investigation in January.

And in December, a further 16 defendants were charged with racketeering, wire fraud and money laundering in relation to an "unconscionable" scheme of corruption that had been running for 24 years. That brings the number of indictments to 40, at the time of writing. In most cases of D&O cover, the duration of such a fraud would be sufficient to crack the policy wide open.

Now, while these allegations remain to be proved, some defendants have been singing. According to the US Department of Justice, eight defendants pleaded guilty under seal and agreed to repay $40m pocketed in kickbacks for media deals. Insurers are working out whether these admissions can be taken as proof of the liability of more senior officers such as former FIFA president Sepp Blatter.

In all this, Blatter's position is highly fluid. Banned in January from involvement in football for eight years because of "unethical behaviour", he has not been criminally indicted, but Swiss authorities are trying to prove criminal mismanagement among other examples of corruption.

Now, it would seem that the exposure of the FIFA hierarchy to lawsuits of various kinds is growing from within. This is because the organisation's own ethics committee has jumped into action, describing as "abusive execution" of their positions the matter of a $2m (€1.8m) payment that Blatter and former UEFA president Michel Platini made four years ago. Clearly, the conclusion of an internal investigation puts another big question mark over the validity of D&O cover for senior officers.

MONEY IN THE POT

But even if their cover survives all these confessions and findings, how far will it go?

As Clyde & Co points out, if the FIFA cases come to court, the defence and related costs will be considerable, given the size of the numbers involved and the extent of the alleged corruption. Most D&O policies provide cover for a defence up to a certain amount – the "aggregate limit of liability". When that's used up, there's no more money in the pot and the defendant is on his own.

As Willis points out in a 2004 series of FAQs on D&O (written long before it merged with Towers Watson), "this means the carrier has no further obligation in connection with defence costs that may continue to be incurred".

PRINCIPLES-BASED

Finally, the principles-based rather than prescriptive nature of the current round of anti-corruption regulations is also making directors nervous, especially those on the boards of international companies at a time when truly global coverage is unavailable. Regulators may determine after the fact that a director has behaved badly, leaving the accused to prove that he didn't.

As the head of claims and legal practice at Aon financial and professional services, David Nayler, pointed out in a report about D&O: "You have to guess your way through the legislation, really. When directors look for detail, there isn't much guidance."

And that's not a lot of comfort. **SR**

UK Prime Minister David Cameron announced the date for the EU referendum, which will take place on 23 June. Risk managers weigh up the effects of a possible Brexit: **bit.ly/1U7Ewh9**

Brussels suffers terror attacks. A bomb exploded at international airport Zaventem and another at Maelbeek metro station on 22 March. Islamic State claimed responsibility for the attacks: **bit.ly/1U7Ewh9**

XL Catlin appoints three managers for its Southern European operations: Bruno Laval, regional manager for Southern Europe and country manager, France; Simona Fumagalli, country manager Italy; and José Ramón Morales, country manager Iberia: **bit.ly/258zQN1**

Aon appoints Julie Page as its new UK managing director: bit.ly/1UGmQKX

Insurance buying budgets slashed as oil companies suffer price collapse

Insurance buying budgets have been hit by tough market conditions as global oil companies suffer losses in the billions. One of those companies is Maersk Oil, which clocked up a loss of $2.1bn. The Group's risk manager speaks out on how the company is managing the risk

Falling oil prices have had detrimental effects on the energy industry. Numerous large oil projects have been shelved and tens of thousands of people have lost their jobs since the oil price started its slide in June 2014.

One of the companies affected is Maersk Oil, part of the Danish oil and shipping conglomerate AP Møller-Maersk Group. The business suffered losses in the billions, reporting a $2.1bn loss over 2015. The news came after it wrote down the value of its oil assets by $2.6bn, citing low oil price expectations as the reason.

The risk did not go unnoticed by Maersk Oil. It projected falls in oil prices as a significant risk – just not to the extent the collapse eventually materialised. It has since taken steps to manage the fallout. Speaking exclusively to *StrategicRISK*, Lars Henneberg, head of risk management at AP Møller-Maersk Group, says: "The group is seeking to mitigate the risk by continuing to be a top-quartile performer through cost-reduction programmes, as well as by renegotiating terms with authorities, partners and contractors to make projects more attractive."

TUMBLING

Oil giants including BP, Royal Dutch Shell and Chevron have also taken to 'cost-reduction programmes', announcing payroll cuts to save on expenditure. In January 2016, BP said it will cut 7,000 jobs over a two-year period. Last July, Chevron announced job cuts of 1,500 jobs, and Royal Dutch Shell will make 6,500 people redundant. In total, the energy sector laid off more than 258,000 workers globally in 2015, according to industry consultant Graves & Co.

The oil industry's efforts to reduce costs have not bypassed insurance and risk management departments either.

"The oil price collapse is leading to reduced risk management budgets," says Nick Dussuyer, global head of natural resources at Willis Towers Watson.

"We have already seen several instances recently where, as a result of management directives, some of our major clients have significantly reduced their programme limits, with a corresponding dramatic reduction in premium spend."

He adds: "A few months ago, one of our clients, a major integrated oil company based in North America, elected to cut their insurance programme limits by 50%, while other clients have been forced to consider scaling back on their own insurance programme aspirations.

"This of course has had a knock-on effect on the insurance market."

Oil projects globally, such as deepwater offshore drilling, have also been postponed. Consulting firm Wood Mackenzie identified 68 large projects globally, with a combined value of $380bn, that have been put on hold because of the oil price collapse.

Angus Rodger, principal analyst, upstream research for Wood Mackenzie, explains: "For all 68 projects, there are multiple elements contributing to delay.

"Price is rarely the only factor slowing down final investment decisions – but it has exerted the strongest influence."

A GRIM PICTURE

It is likely these market conditions will persist for the foreseeable future, as oil prices are not expected to go up any time soon.

Indeed, the current picture is dire. Crude oil prices, for example, are at their lowest level since the 1990s, having fallen more than 70% since June 2014, to stand at $30.77 per barrel on 18 February 2016.

Overall, a combination of oversupply and soft demand are the cause of the price drop. Domestic production in the US has doubled over the past few years, reducing the need for oil imports and forcing oil producers in Saudi Arabia, Nigeria and Algeria to find new markets. They are all competing for market share

> **"ONLY A FEW MONTHS AGO, ONE OF OUR CLIENTS, A MAJOR INTEGRATED OIL COMPANY BASED IN NORTH AMERICA,ELECTED TO CUT THEIR INSURANCE PROGRAMME LIMITS BY 50%**
>
> Nick Dussuyer, Willis Towers Watson

in Asia, but to gain competitive edge they have had to drop their prices substantially. Meanwhile, oil production in Canada and Iraq is rising year after year and, following the lifting of sanctions, Iran is planning to start exporting oil too.

On top of all that, demand is lagging, since European and developing economies are struggling and vehicles are becoming more energy-efficient.

So, what is the answer for risk managers whose task is to manage this risk or at least limit the exposure?

Maersk Group's Henneberg says: "The oil price risk is inherent in the businesses we operate in, and the best thing you can do is to try to understand the underlying supply and demand dynamics driving the oil price and establish a risk appetite within which you manage your investments and portfolio."

The silver lining, if there is one, is cheap investments. As Henneberg put it, the current environment coupled with the Group's financial strength, could present opportunities to invest in oil assets at a low cost. **SR**

Photography: Kevin Miller

Still counting the losses

In 2014, Malaysia Airlines' Fuad Sharuji was thrust into a nightmare scenario – twice. Here, he speaks for the first time about what the twin crises taught him

On the morning of 8 March 2014, 227 passengers and 12 crew boarded a Malaysia Airlines flight in Kuala Lumpur. MH370 was bound for Beijing, China, and scheduled to land at 6.30am. Two years on, the aircraft and its passengers are still unaccounted for.

Disaster struck again on 17 July 2014, when 280 passengers and 15 crew boarded a Malaysia Airlines plane in Amsterdam. En route to Kuala Lumpur, flight MH17 was shot down by a missile in eastern Ukraine.

Two planes, and 534 lives, lost in four short months.

Speaking exclusively to *StrategicRISK* just days after the second anniversary of MH370's disappearance, the crisis director for MH370 and MH17 and head of the Malaysia Airlines post-accident office, Fuad Sharuji, explains what the past two years have been like for him and what he has learned.

FIRST RESPONDER

As the first point of call for operational issues such as flight delays and groundings, Sharuji was used to getting calls from his operations manager at all hours of the day and night.

But the significance of the phone call he received at 2.30am on 8 March 2014 was unlike any other. Even now, he describes those first few moments with disbelief – but also with clarity.

"Immediately I opened my laptop, accessed the flight systems, and saw there were four other aircraft that were in the vicinity of where MH370 was supposed to be, but 370 was not in the picture at all," he says.

After several attempts to contact the plane through satellite communications, air traffic control centres and nearby aircraft, the severity of the situation became quickly apparent. Just before 3am, 30 minutes after that first call, Sharuji declared a code red emergency.

"You really need three people to agree to declare code red because that is the most serious crisis for us. But because my CEO was not available and the director of operations was not immediately contactable, I had to make the big decision by myself," he explains.

Within an hour, most members of the airline's emergency operations committee had assembled at the airport, followed soon after by an emergency response working group, 'go teams', and a special assistance team.

At 7am, half an hour after the plane was scheduled to land, Sharuji received a phone call from CNN, asking where MH370 was. After that, news spread almost instantly that the aircraft was missing.

"We told them (CNN) that we couldn't confirm what had happened to the aircraft because we just did not know where it [was], but we confirmed that we had lost contact with the aircraft," Sharuji says.

This is where one of the key challenges for responding to the crisis stems: in Malaysia, the Department of Civil Aviation, not the airline, is responsible for any search, rescue and repatriation efforts for a crisis of this kind.

"The airline has no control over these functions except to communicate with [the government] and to provide any assistance that they want from us," Sharuji says. "Our concentration at that time was to search for the aircraft that might have gone down. It was like groping in the dark."

On the information Malaysia Airlines had to hand, the team members' best guess was the South China Sea. They later found out this was wrong, but only after the government had moved its search efforts, owing to new flight signals that indicated the plane had made a U-turn.

"By morning we were told that the search mission had been launched, but we didn't know exactly how many ships or planes [had been] deployed," he says.

All the while, Sharuji's team was receiving tips on possible sightings of the plane. From oil riggers in Vietnam who said they saw a ball of fire falling from the sky to beachgoers around South East Asia who reported hearing a loud explosion, the reports were many and varied.

"We tried to respond to every single thing that we heard and every time, we relayed that to the RCC – the rescue command centre – run by the government."

But it seems the communication was not two-way.

"From the public's perspective, they thought that there was a lot of cover-up and we were withholding information, which is actually not true because we also didn't know," Sharuji says.

FAMILY TRAGEDIES

As the hours turned into days, and days into weeks and months, the team's priority was looking after the next of kin. There were more than 1,000 in Beijing alone.

For almost two months, the airline paid for accommodation, meals, counselling and other basic living expenses of those who claimed next-of-kin status for the 153 Chinese nationals onboard MH370.

‹ ALERT Sharuji called code red for flights MH370 and MH17

"WE ALSO LOST OUR FRIENDS AND RELATIVES, WE LOST THE AIRCRAFT, WE LOST OUR BUSINESS, WE LOST OUR REPUTATION. WE LOST A LOT

"We didn't expect it to be that many because China had a one-child policy, so it was quite overwhelming for us," Sharuji says.

By way of comparison, there were 192 Dutch passengers onboard flight MH17. So when that plane went down, Sharuji briefed his team to expect about 600-700 next of kin at Amsterdam Schiphol Airport. Instead, only 50 required assistance and all of those returned home within a week.

As the search for MH370 continued and new information was received, experts eventually agreed that the most likely place that the plane went down was in the South Indian Ocean off western Australia.

"I know it's a bitter pill to swallow, but this is the truth and we've just got to accept the fact that we have lost the aircraft and there's no possibility at all, under the harsh condition of the ocean, that there is any possibility of any survivors," Sharuji says.

While many have accepted this explanation, there are still those who, without concrete evidence, refuse to believe it. "We still receive letters from [Chinese] next of kin to ask me to ask the government to return their loved ones back to them alive," he adds.

"We also lost our friends and relatives onboard the flight, we lost the aircraft, we lost our business, we lost our reputation; we lost a lot. So we also want to know where the aircraft is, we want to know why it happened. We want to know what went wrong, we want to know who is behind all of this; we are just like them."

The certainty of what happened to MH17 made the second crisis "much easier" for Sharuji and his »

‹ COMMITMENT Sharuji's whole career has been with the airline

team to handle from a crisis management perspective. That, and the efficiencies of the Dutch government's response plans, Sharuji says.

"I want to put on record my appreciation to all of the governments involved in MH17, in particular to the Dutch Safety Board," he says. "I also want to thank the Chinese government and the Australian government who helped us on the search for MH370. And, of course, the Malaysian government as well, who helped us in the search-and-rescue effort."

Sharuji, now 60, has been with Malaysian Airlines for his entire career.

He joined the country's national carrier straight after high school and was sent to England in 1976 to complete an engineering degree.

For more than two decades, the Kuala Lumpur native worked in the aircraft's engineering team, before moving to the operations department in 2005. In 2009, he became the group's vice-president of operations.

Last year, when the airline went into administration, Sharuji decided to stay with the old company, rather than move to the new airline, to continue focusing on the two crisis events.

RESPONDING TO CRITICISM

In the aftermath of both crises, several media reports suggested that the airline did not have tried-and-tested crisis plans in place. But this is incorrect.

In fact, just three weeks prior to MH370's disappearance, Sharuji had conducted a full emergency response exercise; and the similarities between the 'practice' event and MH370 are not lost on him.

"The [practice] scenario was a 737, departing Kuala Lumpur, which then had an engine failure and crashed in the Strait of Malacca and we lost contact with the aircraft," he says.

The Malaysia Airlines emergency response team conduct one major crisis scenario event every year. Every second year, they also involve the airport authorities.

"Even though our [emergency operations centre] is not sophisticated … our emergency response plans are very comprehensive and very detailed," he says.

Overall, Sharuji says he was "very happy" with how his emergency response teams reacted to both crises.

"We made a few mistakes here and there and we corrected those mistakes almost immediately. But on the whole, we handled the two crises extremely well," he says.

That's not to say that Malaysia Airlines' response was perfect, however.

8 March 2014

Malaysia Airlines flight MH370 departs from Kuala Lumpur International Airport, en route to Beijing. On board are 227 passengers and 12 crew. An hour after the flight is scheduled to land, Malaysia Airlines releases its first statement confirming that the flight had lost contact with air traffic control.

9 March

A full-scale international search-and-rescue operation begins to find the aircraft, with attention focusing on waters between southern Vietnam and Malaysia.

10 March

An investigation is launched regarding two passengers who boarded the plane with stolen passports and are linked to a stolen passport syndicate.

16 March

Malaysia calls for help from 25 countries as the search for missing flight MH370 expands across a vast area of land and ocean covering 11 countries.

6 April

Multiple signals are detected that could have been emitted from the black box of the missing flight. Australian prime pinister Tony Abbott says searchers are confident they are picking up the right signals, and have narrowed down the search area to "within some kilometres".

30 April

The intensive aerial search for surface wreckage of MH370 officially ends, with ships also moving out of the remote Indian Ocean area where the plane is believed to have gone down.

1 May

Preliminary report released. It took authorities four hours to activate a search-and-rescue operation after they lost contact with flight MH370, according to the report, made public by the Malaysian government.

FORUM TALK

Fuad Sharuji, head of the Malaysia Airlines post-accident office and crisis director for MH370 and MH17, will be the one of the key speakers at this year's *StrategicRISK* Forum in Singapore. Held on 17 May at the InterContinental Hotel, this third annual event is free for risk and insurance managers to attend by pre-registration. For more information about the event, or to apply to attend, visit http://riskforum.strategic-risk-global.com

Sharuji says the events highlighted some "loopholes" in its response plans.

"There were quite a number of assumptions that we made and we realised that the assumptions were wrong," he says. "For example, we thought that the way we would handle the Malaysian Chinese next of kin [in Kuala Lumpur] would be the same as the Chinese Chinese [in Beijing], but we were wrong because the culture and the behaviour is extremely different."

The importance of choosing the right crisis team leader – known as a 'go team' leader at Malaysia Airlines – also became apparent in the crises.

"You can have a person who walks like John Wayne and talks like Tom Cruise during peacetime, but during war he can become like Mr Bean," Sharuji says. "That person must be very strong and very level-headed, and very composed and calm even under extremely stressful conditions, and it's not easy to find."

HANDICAPPED

A few days into the MH370 crisis, Sharuji's 'go team' leader in Beijing had to be replaced as he was unable to cope with the stress.

"One of the things that we have done is put in what we called management advisers – this is in addition to the go team leader, who actually manages the crisis teams, the handling of the next of kin, the family assistance centres, support and so on," he says.

The role of the management advisers is to act as a liaison between the airline and the government during a time of crisis. "We made quite a lot of changes in our corporate emergency operations manual after MH370 and MH17," Sharuji says.

"The structure of the go team is also slightly changed: we changed some templates, and we changed some of the training programmes to include diversity and cultural handling.

"We also changed our process in dealing with the government, or government relations."

> **WE STILL RECEIVE LETTERS FROM THE CHINESE NEXT OF KIN TO ASK ME TO ASK THE GOVERNMENT TO RETURN THEIR LOVED ONES BACK TO THEM ALIVE**

One of the main challenges in terms of responding to the 370 crisis was its unprecedented nature.

"In modern aviation history, we haven't [had] any other airlines that have lost an aircraft for as long as MH370 and because of this, we were handicapped," Sharuji explains. "We were also handicapped by government intervention and government bureaucracy."

The key lesson he has learned is that airlines must always be prepared. "We cannot be prepared for every single conceivable scenario, but you have to be prepared to react to any given situation," he says.

The importance of good government relations is another key lesson.

"My next step is actually trying to work very closely with the government in helping them bridge the gaps that we had before," he says.

"That is to me the most important thing in my wish list right now – to bridge a gap that we have in the crisis management programme between us and the authorities."

17 July

Disaster strikes Malaysia Airlines for the second time in a year when flight MH17, flying from Amsterdam to Kuala Lumpur, crashes near the village of Grabove in eastern Ukraine. The plane is carrying 280 passengers and 15 crew. The suspicion is it was shot down by a Russian-made Buk missile.

18 July

The blame game for MH17 begins. Ukrainian president Petro Poroshenko calls it a "terrorist act". Pro-Russian rebels claim the airliner was shot down by a Ukrainian military jet. Russian president Vladimir Putin says Ukraine "bears responsibility" for the crash.

31 October

A Malaysian family sues the government and Malaysia Airlines for negligence in the disappearance of flight MH370, in what is believed to be the first lawsuit filed over the disaster.

29 January 2015

The Malaysian government announces all 239 passengers and crew onboard missing flight MH370 are presumed dead.

13 October

Dutch newspaper *Volkskrant*, quoting sources close to the investigation, says the inquiry of MH17 has concluded that a Russian-made Buk missile fired from rebel-held eastern Ukraine shot down the plane.

3 March 2016

Debris washes up in Mozambique and is tentatively identified as a part from the same type of aircraft as MH370, the only known missing Boeing 777.

Moves towards a Brexit are making a lot of people nervous

While the UK's politicians squabble and public opinion seems to teeter on a knife edge, the insurance industry is anxiously preparing for a possible split with the EU

On 23 June, the British public will vote on whether the UK should remain in the EU – and campaigns for and against a British exit (or 'Brexit') are in full swing.

The UK joined the EU – back when it was the European Economic Community, or EEC – in 1973, and its relationship with its neighbours has long been ambivalent. During the last referendum on membership, in 1975, 67% voted to stay in.

Since then, anti-EU sentiments have been growing, prompting a promise from the Conservative government that it would hold a referendum on the topic before the end of 2017. Now that a date has been set, both camps are trying to convince voters about the net costs, or net benefits, of membership.

Prime minister David Cameron and 16 members of his cabinet are campaigning for the UK to remain in the EU. They have the support of the Labour Party, the Scottish National Party, the Liberal Democrats and Welsh nationalists Plaid Cymru. Additionally, many British businesses have indicated they would prefer Britain to stay in the EU, as have French president François Hollande and European Commission president Jean-Claude Juncker.

The Conservative Party has pledged to remain neutral, but nearly half its MPs, including six ministers, have backed the 'Leave' campaign (some have yet to declare). So too have London mayor Boris Johnson and the party's leader in the European Parliament, Syed Kamall. The UK Independence Party, several Labour MPs and Northern Ireland's Democratic Unionist Party also want out.

The two camps disagree on the benefits the EU brings to the country and what the consequences will be if it decides to withdraw.

Leave campaigners say the EU imposes too many rules on business and costs too much in membership fees, with little reward. Moreover, they want Britain to regain full control of its borders and regulations.

Those in favour of EU membership believe it gives a significant boost to British business and the UK economy. They also argue the country is more secure in the European Union than on its own.

THE INSURANCE SECTOR

While politicians are heavily divided on the issue, many British businesses have spoken out against a Brexit, including Lloyd's of London.

In a recent speech to the Insurance Institute of London, Lloyd's chief risk officer Sean McGovern said Brexit does not offer a route to "insurance regulatory

> **THE UK WOULD BE A 'THIRD COUNTRY', AND WHILST IT MAY BE FOUND TO HAVE A REGULATORY REGIME THAT IS EQUIVALENT TO SOLVENCY II, THAT DOES NOT CONFER A RIGHT TO ACCESS**
>
> Sean McGovern, Lloyd's of London

nirvana", as the UK regulatory system has been largely driven by domestic political and regulatory concerns and cannot be blamed on Brussels.

An equivalence finding under Solvency II does not provide a solution either, he added. "The UK would, under EU parlance, be a 'third country', and while it may be found to have a regulatory regime that is equivalent to Solvency II, that does not confer a right to access the EU market, either on a cross-border or on a branch basis."

McGovern made it very clear that the UK's membership of the EU is key to Lloyd's future growth and its competitive position as part of the global insurance market.

While he stressed that the best scenario would be for the UK to remain in the EU, McGovern said Lloyd's has been working on contingency plans to deal with a range of possible scenarios.

"In the event of a vote to leave, we would work with the UK government and EU institutions during any negotiations to retain market access for Lloyd's and the London market and create as much regulatory certainty as possible," he said.

McGovern added that Lloyd's has examined all alternatives to the UK's existing relationship with the EU if Britain votes to leave. "There is real uncertainty about what those alternatives might be and what will be politically and practically achievable after a vote to leave. What we do know with certainty, however, is that none of the alternatives will be as beneficial for the London market as the current relationship."

A recent report by AXA Investment Managers supports this view. It estimates the UK will suffer a 2% to 7% drop in GDP over the next 15 years if the public votes to pull out. The investment firm said a Brexit is unlikely, but that the chances of a 'leave' vote will increase significantly if the EU migration crisis worsens.

HOW LIKELY IS A BREXIT?

Presenting the report's findings at an event held at Lloyd's of London, its author David Page, UK and US economist at AXA IM, said three reasons counted against a Brexit.

First, the UK government is campaigning aggressively to stay in the EU, which will have "some resonance with some of the British people", he said.

British businesses have started to speak in favour of remaining: "Those that are somewhat distrustful of politicians may look to the business community [because they] believe that [businesses] give a more objective assessment of what would happen to the country post-Brexit."

Last, status quo bias may influence how people vote on 23 June. "Looking at referenda outcomes across the EU over the last 30 years, we can see that there has always been a preference for the status quo. It is a natural human emotion to fear change."

Voting decisions that side with the status quo tend to be expressed closer to the voting date, "which we saw in the recent Scottish referendum". »

FORUM TALK

StrategicRISK is hosting a half-day event specifically dedicated to exploring Brexit risks. Sponsored by QBE, this free to attend event will be held on 12 April at the City of London Club EC2N 1DS, starting at 08.30. Our Brexit event will focus specifically on the implications for business, particularly multinational companies, of the UK's possible withdrawal from the European Union. This non-political forum will focus on practical steps for risk managers.

For more details go to http://events.nqsm.com/e/preparing-for-brexit

» But the hot-button issues of migration and security could cause a change in sentiment.

"The EU migration crisis is weighing on people's mind," said Page. "A lot of people see a Brexit as a way to give [the UK] greater control over migrant flows. The more the EU migration crisis [worsens], the more we see trouble at the borders, the more the migration crisis will weigh on people's mind."

POST-BREXIT FREE-TRADE AGREEMENTS

In its report, AXA IM also investigated the impact a 'leave' vote would have on trade and financial services. At the moment, the EU accounts for 44% of the UK's export. Post-Brexit, the UK would likely arrange a bespoke bilateral free-trade arrangement (FTA) with the EU, but there are likely to be difficulties in securing the best tailor-made agreement.

AXA IM predicts an FTA agreement will maintain the UK's access to EU markets for goods (of which it is a large importer). But the UK is a service-dominated economy and obtaining a favourable services agreement will be harder, according to the report.

As a member of the EU, the UK is part of a network of preferential trade agreements with non-EU countries, to which 10% of its exports go.

Additionally, of all UK exports, more than 25% are to countries that are currently negotiating trade agreements with the EU or whose agreements are yet to be implemented. If the UK were to leave the EU, it would have to renegotiate new agreements with these countries, but it is unclear whether it would be able to do so.

CONSEQUENCES FOR EUROPE

For Europe, however, a Brexit is unlikely to cause adverse problems. The EU will see only a small net negative impact, said AXA IM.

Nonetheless, some countries could suffer more than others, namely Ireland and the Netherlands, both of which have large trade links with the UK.

Inadvertently, a Brexit may encourage other countries to think about leaving the EU, but Page thinks this is unlikely, certainly in the short term.

"A country like Sweden, which is part of the EU but not the Eurozone, might look at what [happens to the UK in the event of a Brexit] and follow suit.

"If our report has underestimated the benefits and the UK is performing much more strongly [after a Brexit], then there will be some increased pressure for an additional exit," said Page.

"But in terms of what a Brexit will mean for the EU over the next two to three years – other than giving a few more stories to [anti-EU] movements within the Eurozone – I'm not sure it's going to have that much of an impact."

Estimating the consequences of a Brexit is difficult. If Eurosceptics win the day, the UK will still have two years' membership before it secedes. But the consequences of a vote to leave will only become clear if, on 24 June, it finds itself in the exit lounge. **SR**

> **THE MORE THE EU MIGRATION CRISIS [WORSENS], THE MORE WE SEE TROUBLE AT THE BORDERS, THE MORE THE MIGRATION CRISIS WILL WEIGH ON PEOPLE'S MIND**
> David Page, AXA IM

IMPLICATIONS OF A BREXIT

Business: More so than manufacturers, exporters of services could find it harder to access the EU market

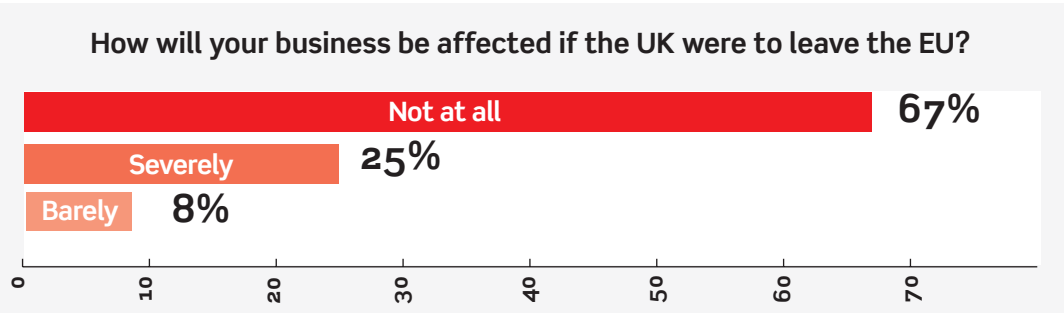
Economy: The UK's GDP is likely to drop between 2% to 7%, according to AXA IM

Trade: Agreements with EU and non-EU states will need to be renegotiated

Europe: Other governments may have to hold similar referenda

Will a Brexit make a difference to your firm?

A *StrategicRISK* poll of UK risk managers reveals what difference – if any – a Brexit will make to their companies' operations



The British public has been fairly evenly split on whether the UK should remain in the EU, but, at the time of writing, opinion polls show the scales tipping slightly towards a Brexit.

In a poll by ORB, published in the *Daily Telegraph* on 15 March, 47% of respondents said they wanted Britain to remain in the EU; 49% said they supported a Brexit.

But when likelihood to vote was taken into account, those backing Brexit were in a stronger position, polling 52% against the 'remain' camp's 45%. Furthermore, 31% of undecided voters said their "biggest hesitation" in backing the pro-EU campaign is the "potential for uncontrolled or increased immigration" in the EU.

With two months until the EU referendum, *StrategicRISK* conducted a poll of its own, asking readers how they think their company will be affected in the event of the UK seceding from the EU.

Two-thirds of risk managers responding to the poll say they do not believe their companies would be affected at all by a Brexit. Only 25% think they'd be severely affected by such a move and 8% say they'd be barely affected.

Gilbert Canaméras, secretary general of FERMA and consultant at Eramet, the French multinational mining and metallurgical group, sees Brexit as the main political risk in Europe.

"At macroeconomic level, it is an important issue because it would create new regulations between the UK and the rest of Europe," he said. "London could lose its status of financial capital and suffer new taxes for products imported from European countries."

For European businesses, a Brexit would create uncertainties around doing business with the UK because of the change in regulations, currency volatility and import controls, he added.

Given the potentially far-reaching consequences, Canaméras believes companies are not really prepared for a Brexit. "The possibility of a Brexit is estimated at 33% in the financial markets. In that case, we can just wait and see. But if the percentage increases, it may for instance be necessary to do some currency hedging and to strengthen credit risk policies."

Short to medium-term instability and uncertainty on the currency and stock markets is also a concern for Colin Campbell, head of risk and compliance at retailers Arcadia Group. He said a Brexit could bring all sorts of downsides for the UK, from financial institutions and manufacturing businesses relocating their head offices or major operations, to labour shortages and calls for a new referendum on Scottish independence (if Scotland seeks to stay in the EU and secede from the UK).

Added to that, the removal of EU subsidies may have adverse effects on some regions in the UK, possibly making Britain even more London/south east-centric.

Some industries would be affected as well. "Farming subsidies from the EU will no longer be available to UK farmers, which may mean many will have to give up the profession. It would certainly require a reworking of their business models," Campbell said.

UK farmers would suffer less from cheap imports from the rest of the EU, which sometimes lead to oversupply. The worry is that if supply from the EU declined, food prices in the UK could increase.

However, Campbell believes that generally, most UK firms would welcome a reduction in new regulations. **SR**

This isn't the time to vote with your gut

People need an impartial body to lay out the EU's pros and cons. They can't rely on those shooting from the hip and pushing their own agenda

Elaine Heyworth, interim head of risk and insurance at the Royal British Legion

Whether they're for or against membership of the European Union, politicians, economists and other interested parties are providing UK headline-writers with big, ballsy statements about the negative consequences of one referendum result or the other.

Both sides of the debate have taken to the media with scaremongering rhetoric in a bid to influence the UK electorate – and I question the validity of what can be read as crisis statements. Pro-EU campaigners in particular have been publicly criticised for using scare tactics, certainly where economic growth and trade are concerned.

Economists who back the 'remain' campaign, for instance, have suggested a drastic decline in GDP – figures that appear similar to that of the 2008 financial downturn. Yes, there will undoubtedly be economic consequences and currency fluctuations if we exit, but this is likely to be a short-term problem while Britain settles into a new world.

Those most passionately opposed to a Brexit claim that a withdrawal will harm the country's access to EU markets or that the UK will need to set up new agreements with every single EU country.

The most likely outcome, however, is new trade agreements with the European Union.

The fact of the matter is that if the British public votes to withdraw, it does not mean that the UK will be closed for business. Reports will have you believe that Britain will retreat into a box and hide. But it will remain a trading entity – it has always been and always will be a trading entity.

A Brexit just means that the country will enter a new dynamic. And yes, there will be hiccups along the way, but 'remain' campaigners are preying on a fear of change.

Funnily enough, I'm a Europhile and I do not want Britain to leave Europe. But my point is that people should not be afraid of what might happen.

The biggest risk of the EU referendum is that the vote has been handed to the British public without clear, honest and unbiased information about either outcome. So lots and lots of people will vote with their gut and their emotions –and this is not the best way to make one of the biggest decisions of our generation.

The for-and-against debate needs clarity. The British public need an independent body to present the ins and the outs, the pros and cons.

This information cannot come from the Boris Johnsons and David Camerons of this world who are shooting from the hip and pushing their own political agenda.

Turning to risk management, businesses do need to prepare now for a Brexit. What I will be doing on behalf of the Royal British Legion is hosting a workshop to reach out to my directorates.

The question we will address is, how will a Brexit affect us?

I will be using a pestle agronomic to create a grid that details the external and internal risks under six categories: political, economic, societal, technological, legal and environmental.

For instance, what will be the internal and external effects of the political situation? What will be the internal and external effects of the economic situation? This will help us build a grid of issues that might arise under those headings.

Now is the time for risk managers to step up, and we cannot do that if we are afraid of change. **SR**

I'M A EUROPHILE AND I DO NOT WANT BRITAIN TO LEAVE EUROPE. BUT MY POINT IS THAT PEOPLE SHOULD NOT BE AFRAID OF WHAT MIGHT HAPPEN

The stakes are highest for financial services

A Brexit could have good and bad effects on Malta, but the UK losing its passporting rights in the EU is likely to be particularly disruptive

Ian Stafrace, president, the Malta Association of Risk Management

There is still much speculation on what a Brexit could really mean if the UK votes to leave the EU, and I have summarised the key points below.

NOTICE PERIOD

It is reported that a two-year notice period would be given for negotiations. Comparisons have also been drawn to Norway and Switzerland. Such special arrangements for the UK would reasonably take much longer than two years to negotiate.

Britain would face having to negotiate access to the EU's single market in exchange for continued adherence to its rules, or losing access in return for more regulatory sovereignty. EU member states may wish to discourage other countries from following suit and the UK would be in a weak negotiating position, having shown its hand through the referendum

However, a Brexit would leave a weaker EU and some countries like Germany that have trading surpluses towards the UK could try to seek a win-win and reduce the pain of the break-up.

INVESTMENT

Britain is home to a larger stock of EU foreign direct investment (FDI) than any other EU economy and is the preferred location for investment from other leading markets. Some of this could be threatened by a UK exit from the EU. Markets are already volatile. This is likely to increase as the referendum approaches, especially if the polls suggest that a Brexit is more likely than not. European investment managers are stress-testing their funds for what could happen in the run-up to the referendum and in the event of a vote to leave. Scenarios could include a decline in UK equities or sterling-denominated bonds or depreciation in sterling.

PASSPORTING RIGHTS

In theory, financial services passporting into the EU would no longer be possible following a Brexit, unless the UK remained part of the European Economic Area (EEA) or another special arrangement could be negotiated. The same applies to other free trade. That uncertainty may encourage businesses to move to or set up subsidiary fronting operations in other EU countries from where they can have direct access to 30 member states of the EEA.

SOLVENCY II

Considering the importance of the London reinsurance market, it is reasonable to assume that the UK would apply for Solvency II equivalence like Bermuda and Switzerland. UK insurers and reinsurers would then have to apply Solvency II rules or similar without much say in their drafting while also having a degree of local gold-plating.

MALTA

There could be positive and negative impacts for Malta in the event of a Brexit, but ultimately it would be better for Malta if the UK stayed in the EU, not least as the UK is an important trading partner. Businesses trading with the UK would need to reconsider their strategies. Due to the current uncertainty, businesses will already be giving preference to continental European ventures, rather than UK ones.

The sector most affected by Brexit would be financial services. If the UK loses its passporting rights, businesses in Malta providing financial services to the UK could be required to use UK fronting partners or set up fronting subsidiaries in the UK. On the other hand, Malta may attract business from the UK and Gibraltar in the same way it does from Switzerland, as it could offer passporting within the EU. In insurance, the only other current domicile in the EU with Protected Cell Legislation is Gibraltar. In a Brexit, this would be relegated to offshore status and cells with direct EU exposures would likely redomicile to Malta.

In periods of high uncertainty, risk managers can show their worth by helping their organisations identify, assess and manage the fulfilment of new opportunities. Every cloud has a silver lining. **SR**

When bad news breaks, be prepared and act fast

With social media and the 24-hour news cycle in their sights, crisis management teams need to take charge of a situation before it spirals out of their control

Crisis management is rapidly evolving from a discipline deployed in physical emergencies – fires and explosions, say – into one that's commonly used to fight intangible threats. Industries such as oil and gas, and airlines, traditionally called on crisis management methods the most, but now banking, telecoms, media and food production are all strengthening their crisis teams. International standards in crisis management are emerging, and regulators are eyeing the discipline as part of a wider focus on corporate resilience.

"The world is changing and, because crisis management responds to business in context, it is changing as a discipline," says Airmic's technical director, and an expert in business continuity, Julia Graham. "The top risks for many organisations today are damage to systems, damage to reputation or breach of regulations.

"It's a very different risk profile than 20 years ago, and people have to plan for many more intangible events than they used to," adds Graham, who is drafting guidance, to be published by Airmic this year, on how to run a crisis scenario exercise.

DANGEROUS ESCALATION

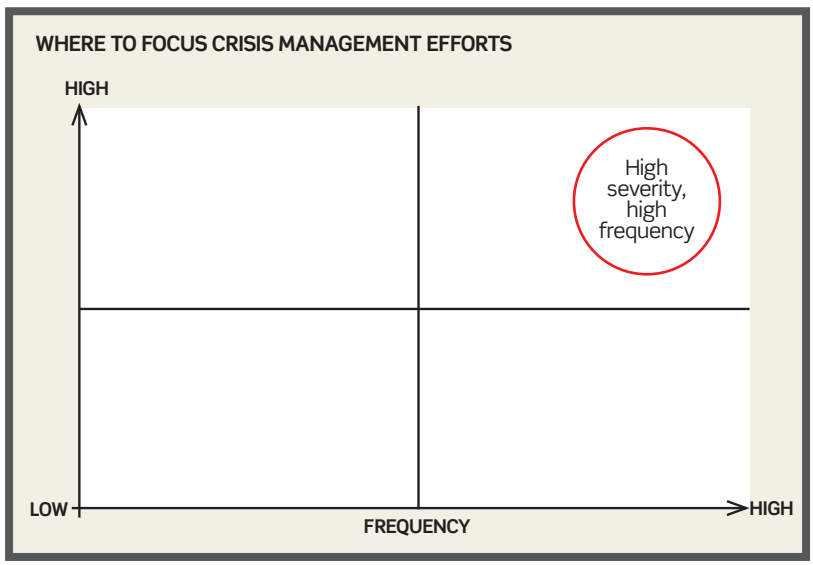
The rise of 24-hour news media, and the power of public sentiment on social media, means a relatively minor event can escalate into a crisis capable of destroying an organisation's value fast. The crisis management community is abuzz with examples of communications gone wrong, from former BP boss Tony Hayward's trial by social media after the Deepwater Horizon spill, to Volkswagen chief executive Martin Winterkorn's departure as the emissions scandal broke. Then there was TalkTalk chief executive Dido Harding, who was sharply criticised in the UK last year for lacking the full facts about a cyber breach.

"The biggest change I've seen is the need for faster responses," explains the director of crisis communications for a well-known global pharmaceuticals corporation. "If you have a site incident like a fire or explosion, there's always been a need to react very quickly, but for more complicated, slow-burning issues, for example around a product or a person, you used to have time to search for facts, and to put together a plan and a statement. Now, it's an instant response."

The upshot is that now corporate leaders must be trained in crisis communications, or kept out of the media glare. "You saw with BP and VW the boss saying, 'I don't know what's happening,' and that is something you cannot have," says Adrian Clements, general manager, operational risk management, at multinational mining corporation ArcelorMittal.

"We cannot have it that Mr Mittal says, 'I know nothing about it.'"

To judge when it's appropriate to enter crisis mode and to call the chief executive, most organisations differentiate major incidents from full-blown crises. One way to quantify events is to use a version of the Boston Grid, a chart developed by Boston Consulting Group in 1970, with frequency along one axis and severity along the other (see box). "That top right corner should cause the crisis management team to step up," says Tim Cracknell, partner, head of consulting risk practice at JLT Specialty. "Organisations also have their own criteria. Casualties, for example, automatically trigger a crisis response, and in the food sector, allegations about product go to the top of the pile." Another way is to size up the potential threat to the company's stated objectives, to its stock market value, and to its ability to continue operating.



Crisis managers looking for an effective operational blueprint for categorising and managing incidents and crises often borrow the gold, silver, bronze command structure used by UK emergency services. This might then trigger use of the appropriate crisis management plan and process, which often exist within or alongside business continuity frameworks, or operational risk activity. Many corporations develop their own frameworks, which are typically also three-tiered: plant, country, and global corporate is used by ArcelorMittal; while a country, regional and global crisis structure is preferred by one high-profile bank. In crisis management consultancy circles, the advice is to create a tiered structure by crisis function: leaders, communicators, operations.

TEAM EFFORT

An effective crisis plan should firstly ensure that the right people are available to form a team at short notice, whether bringing them together in the same room or in a digital workspace. Crisis teams are usually formed of representatives from senior management, communications, human resources, IT, legal, finance, and security, with any combination of these available at all times.

"You need delegated authority to deal with issues and to move fast, that's the key, and has to be properly understood," explains Alex Martin, director, crisis and security consulting at Control Risks. "You want to bring the resources of the organisation together to manage the crisis, and ideally they understand that it's a team effort. Authority must be clearly established, as well as lines of communication; a plan; and actions, with the authority to effect those actions, agreed and recorded; and the crisis plan being continuously reviewed as the situation develops."

Martin adds that resourcing a 24-hour global crisis management capability can be made easier by technology. "In the past, a crisis management plan might've been a dusty tome that sat on a shelf; now, it's a living, breathing, online dynamic – it's evolving. Previously, if you wanted to activate a crisis management team, you might have phoned up the members, updated them on the situation, dusted off their plans. Now, they receive a voicemail, are automatically bridged to a conference call, log into an online collaboration workspace and instantly see a synopsis of the situation."

A more command-and-control style of management is usually appropriate during a crisis, and lines of reporting may be shorter; while experts agree that crisis management frameworks are most effective when they complement the existing risk management process within an organisation, says Graham: "Crisis management is when something hits the fan, it's one of the tools in your risk management toolbox. You don't develop it in isolation. A crisis management framework ought to be part of the business continuity framework, which in turn is part of the overall risk management framework."

The opportunity for risk managers now is to step up to the plate on crisis management. As board-level executives contemplate horror stories like BP and VW, they are increasingly willing to accept that major events are a question of when, not if. **SR**

> **"THAT TOP RIGHT CORNER SHOULD CAUSE THE CRISIS MANAGEMENT TEAM TO STEP UP"**
> Tim Cracknell, partner, head of consulting risk practice, JLT Specialty

How 'war gaming' puts corporates through their paces

To prepare for a worst-case scenario, the armed forces need to train constantly. Faced with an uncertain world, company executives must do likewise

Crisis scenario exercises range from desktop walk-throughs to fully simulated live rehearsals with actors, but can staging a fictitious terrorist attack or concocting a corporate scandal really help corporations to prepare for a crisis? ArcelorMittal thinks so. For its crisis management in response to the Ebola virus, which began in a village close to its plant in Liberia, the global steel and mining company is shortlisted for an Institute of Risk Management Award for Excellence in the Face of Adversity this year.

ArcelorMittal regularly trains staff to respond to crises, whether at plant, country or global corporate level. Every week it has on call a crisis team of 10, who must stay within four hours' commute of its headquarters in Luxembourg. A live simulation of a crisis at global corporate level is rehearsed yearly. The most recent one, involving the fictitious failure of a nuclear power reactor in France, led to a radioactive cloud drifting towards three of the company's French plants before a change in the wind direction diverted it towards Luxembourg.

"We were evacuating thousands of people. We had to find tents, food, water and decontamination equipment. We ran a 24-hour scenario. It highlighted holes in our system and holes in government systems," says ArcelorMittal's Adrian Clements, general manager, operational risk management. In such situations, the global crisis team is trained to gather in a crisis room in Luxembourg, with pens, paper, computers, telephones, observers – whether that's note-takers or video recorders – and plenty of coffee.

In a separate exercise, ArcelorMittal trained the local crisis team at its plant in Dunkirk, France, in a simulation of a contaminated gas leak, discovering in the process that mobile phone networks failed because of the noxious gas. This led to a real-life decision to invest in walkie-talkies. "It's a cost saving to use mobile phones, but we decided to use walkie-talkies," says Clements. "Some of our plants are five kilometres by five kilometres, and if you want to tell the guy over there to turn off the gas valve, you use a walkie-talkie."

TERRORIST ATTACKS

In the wake of the Paris attacks, a relevant topic for many firms is terrorism, particularly siege and marauding shooter-type situations. At one multinational bank, the global operations manager, crisis management, says: "It's unlikely that we'd be directly targeted by IS, for example, therefore what we're rehearsing is an external event which has an indirect impact on our operations or staff. In the City of London, we scenario-planned through a 7/7-type attack. What would we do in terms of counting staff, would we continue operations, what do we think the markets would do, what could that mean for our global operations – that's the kind of thing we would step through."

Such 'war gaming' can be hugely beneficial in building crisis capability within an organisation. "The military don't fight a war every day, but in order to be ready at any time, they practise and train regularly. It's a technique that's used to build operational capability and readiness to respond to a crisis," says Rick Cudworth, resilience and crisis management leader, Deloitte UK, who designs and runs simulated crisis scenarios. "The type of exercise you run depends on what you're trying to test. A tabletop walk-through could be about building awareness around decision-making, whereas full simulations are designed to stress-test processes and teamwork."

"WE RAN A 24-HOUR SCENARIO. IT HIGHLIGHTED HOLES IN OUR SYSTEM AND HOLES IN GOVERNMENT SYSTEMS"
Adrian Clements, general manager, operational risk management, ArcelorMittal

WHAT MAKES A GOOD SCENARIO PLAN?

1 Begin with a risk assessment and an interrogation of crisis plans. Through this, build a picture of what skills or processes are strong or lacking within the organisation, and what it may be beneficial to test.

2 Be clear which competencies you're training for. These may include decision-making under pressure, situational awareness, information management, internal and external communications.

3 Identify which processes are being rehearsed. A scenario could test the communication flow within a single function across geographies, or communication between different tiers of a crisis response.

4 Pick a relevant topic and design a realistic scenario. People learn best from situations that relate to their everyday roles. Some scenario operators confidentially gain information about organisations in order to test genuine weaknesses that may not have been addressed.

5 Assign a record-keeper. A full set of notes, or a video, of what decisions were made by whom, why and on what basis, is invaluable for a post-exercise report and recommendations.

6 Stop every five to 10 minutes to check in. The frequency depends on the scenario, but stopping every so often to share information can be beneficial in a crisis.

7 Limit to the number of skills or processes to be tested. A maximum of four or five aspects of crisis response may be tested within a single scenario.

8 Produce a post-exercise report. Analyse decisions and actions, celebrate what worked, and consider what didn't. Actions to improve crisis readiness should be assigned and given a deadline.

Crisis training should ideally fit within a wider, ongoing process of continuous improvement in risk and crisis resilience, with each exercise clearly testing specific skills or processes. The best approach is to rehearse success, to build people's confidence in their own skills and those of team-mates, and to develop muscle memory of what a good response looks like.

COOL HEADS

Often, crisis leadership and communications emerge as the skills most requiring development. "People, not processes, manage a crisis, therefore you have to focus in preparedness as much on the people skills – leadership, teamworking – as on the hard structures," says Andrew Griffin, chief executive of RegesterLarkin, a global crisis and reputation management consultancy. "Not everybody is suited to leading in a crisis: it's hugely stressful, your job is on the line, the spotlight is on you and the scrutiny from politicians and the media can be extraordinary. The need for leadership training often comes out of exercises."

Another important element to rehearse is how to organise during a crisis, which may require clearer command-and-control structures than everyday operations, and shorter reporting lines.

Cudworth says: "Good practice is a three-tier structure – those trying to fix or resolve issues, those trying to co-ordinate and communicate operationally across the organisation and with the outside world, and leadership, who are looking at it strategically, setting overall direction, tone of communication, liaising with senior stakeholders and looking to the future.

"What you don't want is management trying to fix the problem, because they'll miss what's going on around them. Ultimately, in a crisis, nothing you will do or say will instantly make things better, and that's something which leaders often learn early on.

"People look for a silver bullet, whereas in reality, you've got to accept the situation and to steer the best path that you can." **SR**

> **"FULL SIMULATIONS ARE DESIGNED TO STRESS-TEST PROCESSES AND TEAMWORK"**
> Rick Cudworth, resilience and crisis management leader, Deloitte UK

As organisations come under greater scrutiny from regulators, evidencing exactly what happened during a crisis is increasingly expected. Add to this the valuable lessons that post-crisis reviews can provide, and crisis reporting is emerging as an indispensable way to build and demonstrate corporate resilience.

"In big crises, corporates may come under regulator scrutiny or even legal or government enquiries, and you need to provide evidence of what decisions were taken, when and why," says Rick Cudworth, resilience and crisis management leader at Deloitte UK.

Last year, Deloitte produced a post-event review of the Bank of England's response to the October 2014 outage of its real-time gross settlement system. The report, which prompted the Bank to make a series of improvements, identified the root cause of the incident – a vital piece of information for organisations that aim to improve resilience over time.

"Fixing a symptom isn't enough, it's going to happen again. You have to get right down to the root of why that went wrong in the first place," says Elaine Heyworth, head of risk and insurance at the Royal British Legion. Heyworth recalls a finance system failure while she was working at Barclays Capital Wealth (BCW). "I asked, 'What happened to the system?' and was told, 'It was in a building where all the power went off.' I asked, 'How the hell did all the power go off?' and I heard, 'BT were digging outside and put a spade through our power pipe.' So I asked, 'Hang on, why didn't the landlord tell us so that we could activate our back-up systems?'"

You're out of trouble. This is where the difficult questions start

Preparing a post-crisis report means asking who, what, why and when – but organisations can learn valuable lessons from the answers

Finding the problem's root cause enabled Barclays Capital Wealth to claim on the landlord's insurance and to reiterate the contractual obligation. "For me, you can't have the same excuse twice. It's about learning, and coming up with solutions to the root of the problem," says Heyworth, adding that while she "may have given the landlord a hard time, post-event reviews are about learning, not blaming".

KEEP A RECORD

Heyworth's root cause analysis, covering all major incidents over the course of a year at BCW, resulted in an 80% reduction in events. "My chief operating officer asked me, 'What's happening?' and I said, 'I'm looking for a new job.' We had no crises to manage. Our insurers were delighted, premiums came down. When you fix things at root cause, you reduce business disruption," she says.

A post-crisis report should detail decisions and actions taken, with a timeline making up its backbone. Julia Graham, technical director at Airmic, says: "One of the first actions in a crisis is to assign a record-keeper, and the company should have a pre-agreed method for reporting. In chronological order: what did we agree, who has the authority to do it, when did they do it. It's a record of actions and authorities. There's no ambiguity about who said what, who had authority, and the outcome. As long as it's pre-agreed and chronological, it's a common sense approach."

The company can use the details of who did what, when and why to understand more about how good decisions are made, and what leads to bad ones. Heyworth says: "I always start with a timeline. I want to know how quickly people reacted, what their reactions were and if they were appropriate or not. I had one incident where we waited half an hour to escalate it, but it was very clearly going to be a major incident. It's about saying, 'Look, when it's water and electricity, let's make that call straight away."

HINDSIGHT

A report should enable an organisation to check how closely the crisis team followed the crisis management plan and whether it needs updating. Alex Martin, director, crisis and security consulting, Control Risks, says: "Decisions can prove to be wrong, but that doesn't make them bad. With hindsight, maybe it was wrong, but as long as it is defensible, and was the right decision at the time, that makes sense. You're looking to see that you followed your crisis management plan and due process. The plan is a guide, you don't have to follow it rigorously, but you should have a good reason to deviate from it.

"In some cases, a record of the crisis management process becomes the subject of an after-action review, in others it may be a court case or board of enquiry. Out of a review should come an action plan, with deadlines and rigour applied, to ensure that the process is improved. Additional training takes place, additional resources and tools are put in place; the crisis management plan is changed, if necessary. The important point is that institutions should benefit from the good or bad decisions that were made during previous crises." **SR**

"OUT OF A REVIEW SHOULD COME AN ACTION PLAN, WITH DEADLINES AND RIGOUR APPLIED, TO ENSURE THAT THE PROCESS IS IMPROVED"

Alex Martin, director, crisis and security consulting, Control Risks

Europe versus the world

A *StrategicRISK* survey shows European risk managers have a different outlook to their Asian, and global, counterparts

Increased competition is the biggest risk facing European businesses in the coming year, with a combined risk score of 3.53 out of a possible five. That's the headline finding of a straw poll conducted by *StrategicRISK*.

A close second on the top 10 risk list for Europe is economic conditions (combined score: 3.51), followed by failure to innovate (3.27) and damage to company reputation or brand (3.22). The risk of a targeted cyber attack (3.19) rounds off the top five.

Nearly 50 European risk managers responded to the exclusive survey, ranking the risks of both likelihood of occurrence and financial impact.

Of these, 25 said increased competition was likely or highly likely to occur. Meanwhile, 24 said economic conditions were likely or highly likely to have an adverse effect on their business in the coming 12 months.

"IT IS NOT NECESSARY FOR MOST BUSINESSES TO ANALYSE THE RELATIVE PROBABILITIES OF VARIOUS EXTERNALLY TRIGGERED RISKS, PROVIDED THAT THEY KNOW HOW TO REACT SHOULD THEY OCCUR"

John Hurrell, Airmic

GLOBAL DIFFERENCES

Damage to company reputation or brand topped the list when it came to financial impact, with failure to innovate in second place.

By and large, economic risks keep European risk managers up at night (see page 28). The risk landscape looks different, however, from a global perspective.

Research from the World Economic Forum (WEF), *The Global Risks Report 2016*, found that large-scale involuntary migration and extreme weather events were the most likely to occur, while failure of climate change mitigation and adaptation was deemed to be the top risk in terms of impact.

Margareta Drzeniek-Hanouz, lead author of the WEF report, told *StrategicRISK* that economic risks were still a concern on the global scale, but that other societal considerations were pushing risks such as migration and climate change further up the risk agenda.

"Economic risks generally remain high on the agenda, albeit not as the top risk," she says. "But they should not be underestimated as they remain very important and impactful. There is definitely an underlying long-term concern about economic risk.

"This has been the case over the last few years since the global financial crisis. There is a sense that we are not really addressing those the way we should and they are therefore persisting in one way or another."

She adds: "Asset bubbles have shot up considerably compared to two or three years ago, and that is clearly another concern."

Airmic chief executive John Hurrell says risks fall into one of two categories: internal risks resulting from the failure of company processes and external risks that are the result of unforeseen occurrences.

"The first category will be managed to the best of the ability of the board and management of the company in the light of their (hopefully well-informed) market intelligence and the deployment of their own resources," he says.

"However, the second category requires analysis and intelligence (a good risk radar) but, most of all, the ability to respond effectively and rapidly. It is not necessary for most businesses to analyse the relative probabilities of various externally triggered risks, provided that they know how to react should they occur. Crisis planning will be more effective in practice than risk analysis."

To help ensure internal processes are suitable for the business's needs, and to ensure it is prepared for any unforeseen circumstances, FERMA president Jo Willaert says companies must ensure risk managers are properly embedded within the organisation.

"It is really important that the internal structure of an organisation defines who the risk manager is working for," he told *StrategicRISK*.

"A risk manager should be high-level enough to be part of, or at least support, the decision-making process of the company. He should be there when the strategic options are set out and to give his technical opinion like other disciplines such as financially responsible senior executives.

"It is obvious that these senior executives are close to the decision-making process and that when they say something, it is taken into account. It is often not so obvious for the risk manager."

THE VIEW FROM ASIA

In 2015, *StrategicRISK* conducted a survey of more than 145 of Asia's top risk professionals to get a view of the biggest risks facing organisations in Asia-Pacific.

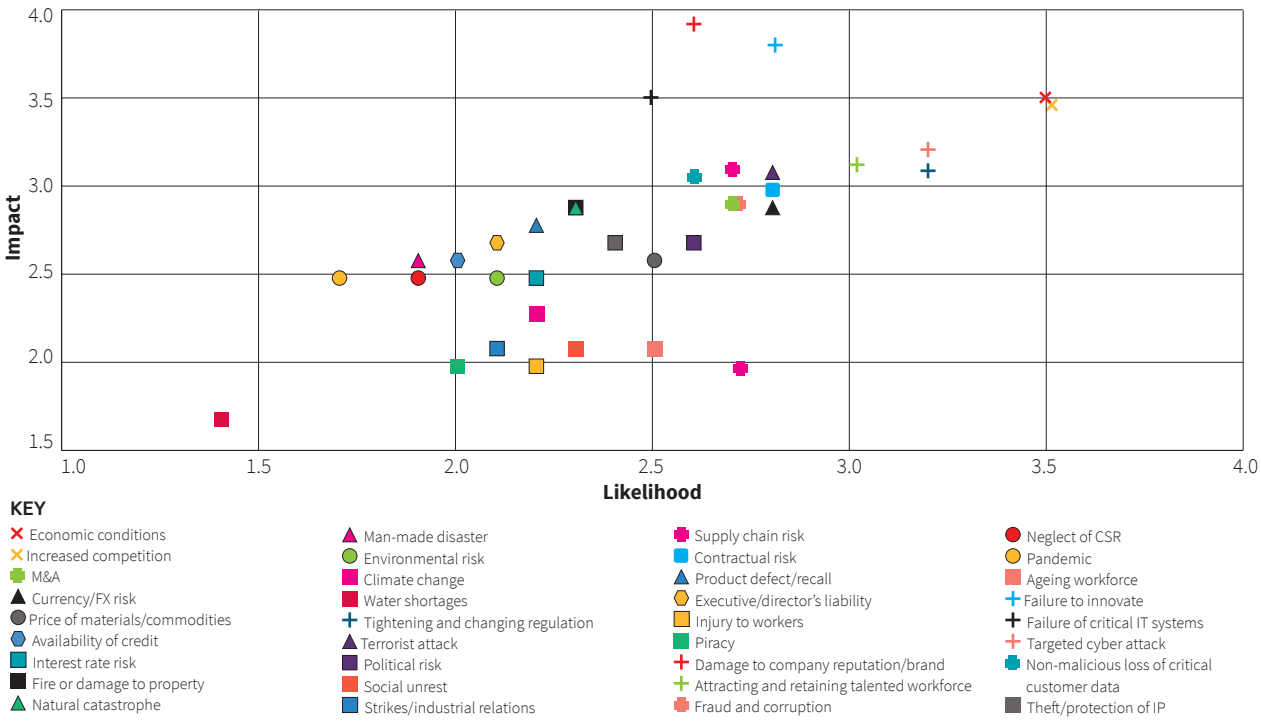
Top of the Asia-Pacific risk agenda was the economic landscape, with a combined risk score of 3.45. While this is lower than the 3.51 score for European economic conditions, it is still enough for it to take the top spot in the Asia-Pacific survey, with

TOP 10 RISKS – FINANCIAL IMPACT

Damage to company reputation/brand	3.9
Failure to innovate	3.8
Economic conditions	3.5
Increased competition	3.5
Failure of critical IT systems	3.5
Targeted cyber attack	3.2
Tightening and changing regulation	3.1
Attracting and retaining talented workforce	3.1
Terrorist attack	3.1
Supply chain risk	3.1

ECONOMIC AND COMPETITION RISKS TOP THE EUROPEAN RISK AGENDA

This chart correlates the financial impact and likelihood of 35 risks



the second and third spots going to, respectively, attracting and retaining a talented workforce (3.09) and increased competition (3.06).

A targeted cyber attack, which was the fifth-biggest risk in the European survey, was of increasing concern for Asian risk managers, climbing from ninth spot in 2014 to fifth in 2015 with a combined risk score of 2.84, compared to 3.19 in the European survey.

Another threat climbing the risk ladder in Asia-Pacific was a company's failure to innovate, breaking into the top 10 for the first time with a combined risk score of 2.84.

Daniel Tan Kuan Wei, second vice-president of the Risk and Insurance Management Association of Singapore and convenor of Singapore's National Risk Management Working Group, says he was surprised that the risk manager community had taken so long to appreciate this risk.

It should have already been in the list, he says. "This is absolutely critical for organisations to constantly produce new products or services that meet customers' needs or innovate internal processes to be more efficient and agile."

Interestingly, European risk managers ranked failure to innovate much higher on the risk spectrum, with a combined risk score of 3.27 taking it to third spot on the list of Europe's biggest risks for 2016.

The risks that least concern Asian risk managers coincided with the European view of the risk landscape. Water shortages and piracy made up the bottom two of both *StrategicRISK* surveys, with likelihood risk scores of 2.0 or less. **SR**

TOP 10 RISKS – LIKELIHOOD

Increased competition	3.5
Economic conditions	3.5
Tightening and changing regulation	3.2
Targeted cyber attack	3.2
Attracting and retaining talented workforce	3.0
Contractual risk	2.8
Terrorist attack	2.8
Currency/FX risk	2.8
Failure to innovate	2.8
M&A	2.7

TOP 10 RISKS – COMBINED

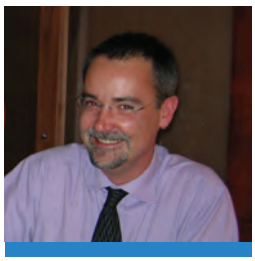
Increased competition	3.5
Economic conditions	3.5
Failure to innovate	3.3
Damage to company reputation/brand	3.2
Targeted cyber attack	3.2
Tightening and changing regulation	3.2
Attracting and retaining talented workforce	3.1
Failure of critical IT systems	3.0
Contractual risk	2.9
Terrorist attack	2.9

"IT IS REALLY IMPORTANT THAT THE INTERNAL STRUCTURE OF AN ORGANISATION DEFINES WHO THE RISK MANAGER IS WORKING FOR"

Jo Willaert, FERMA

It's more than just the economy, stupid

For Europe's risk professionals, the 10 most likely threats include four related to economic factors – but technology and geopolitics are big concerns too



"THE PERCEPTION IS THAT WE ARE FACING MORE AND MORE NEW RISKS BUT OFTEN IT IS THE SAME RISKS, WEARING A DIFFERENT HAT"

David Howells, Tetra Laval International

Economic risks rank among the biggest concerns for European risk managers over the next 12 months, according to a 2016 survey conducted by *StrategicRISK*.

The survey of almost 50 leading risk managers found that four of the top 10 most likely risks were related to economic factors: increased competition, economic conditions, currency and foreign exchange risk, and mergers and acquisitions.

Other categories in the top 10 risk list for Europe include technological risks (targeted cyber attacks and failure to innovate), geopolitical risks (tightening and changing regulation and terrorist attacks), societal risks (attracting and retaining a talented workforce) and contractual risk.

Overall, economic risks had a likelihood risk score of 2.8, compared to 2.7 for technological risks and 2.6 for geopolitical.

Tetra Laval International's director of group risk management and insurance, David Howells, says the globalisation of the marketplace means that businesses now face an increased exposure to economic risks as they enter into new and emerging markets.

"The core risks like damage to assets and supply chain disruption remain, but the economic landscape often changes their location," he says. "As organisations seek growth, their sales become focused on their emerging markets and their manufacturing base moves to contain or reduce costs.

"Doing business in new markets brings new exposures, be it credit risk, country risk, security risk or economic risk. The perception is that we are facing more and more new risks but often it is the same risks, wearing a different hat."

TECHNOLOGICAL CHALLENGES

While economic threats topped the list of most likely risks to affect businesses over 2016, respondents said technological developments were likely to have the biggest financial impact, should they occur.

The results of the survey gave technological risks a financial impact risk score of 3.3 out of a possible five, with economic risks (2.9) and societal risks (2.8) rounding off the top three.

Speaking to *StrategicRISK*, the World Economic Forum's (WEF) director of the Centre for Global Competitiveness and Performance, Margareta Drzeniek-Hanouz, said companies are often ill-equipped to cope with technological risks, despite improvements being made in the private sector.

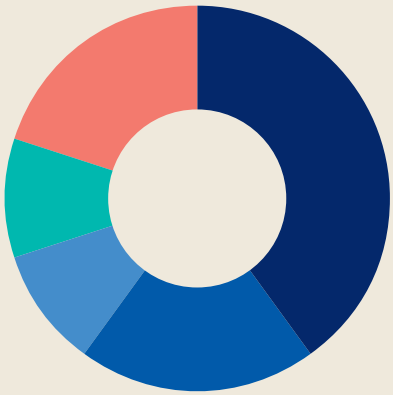
"We do not have mechanisms in place to deal with many of those [technological] risks," she says," but the private sector is advancing very quickly in terms of adjusting to those risks.

"[The problem is that technological] risks also spill over into security and societal questions. Technology empowers people at the same time as governance structures look to disempower them – so new tensions are being facilitated by technology.

"As a result we will see, through those interconnections and the application of technology in different areas of risk, an amplification of risks [across the spectrum]."

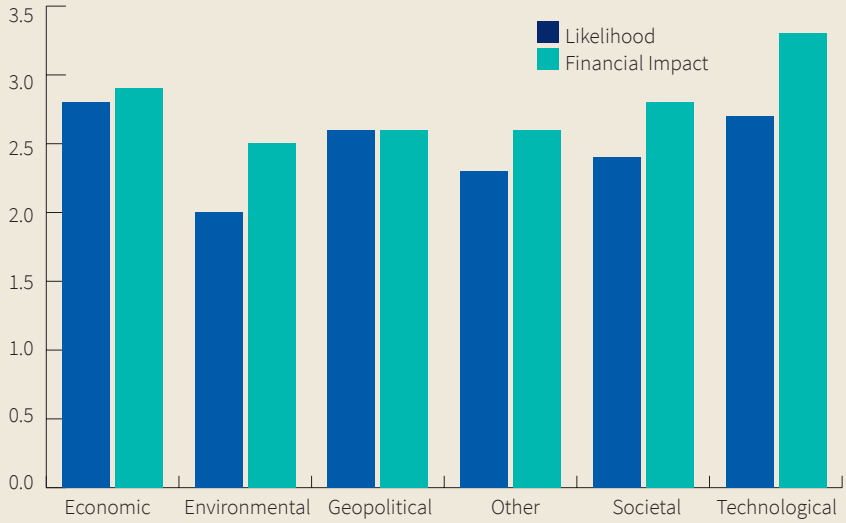
THE EUROPEAN RISK LANDSCAPE

TOP 10 RISKS BY CATEGORY



- Economic – 40% of risks fall in this category
- Geopolitical – 20% of risks fall in this category
- Other – 10% are other risks
- Societal – 10% of risks fall in this category
- Technological – 20% of risks fall in this category

TECHNOLOGICAL RISKS DEEMED COSTLIEST THREAT



To combat this, Howells says it is vital for risk professionals to carry out thorough risk analyses and ensure business practices are kept up to date in the face of constantly evolving technological threats.

"Changing and developing threats are the reason we regularly review our risk assessments and mitigation plans," he says.

"We assess technological and cyber risks by considering information confidentiality, privacy, information integrity and availability.

"So while the threats are constantly changing, so are the strategies used to address them. By reviewing the threats against each of these categories, we can better ensure we remain focused, ahead of the threat, and that our mitigation strategies are effective."

The latest research from the WEF, however, shows that classification of risks by categories can have its limitations.

Drzeniek-Hanouz, who is also lead author of the WEF *Global Risks Report 2016*, says risk managers are now seeing a range of different risks rise to the top of their agenda, rather than have a concentration of particular types of risk as their main concern.

"Until 2008, we saw a clear dominance of economic risk, then we had the emergence of environmental risk between 2008 and 2014, and then over the last two years we've seen other risks move up [the risk agenda]," she says.

"This year was the first year we had four out of the five risk categories represented in the top-five risks. Previously it's been more dominated by one category, so it is visible that risks are increasingly coming together – we cannot think of it in terms of categories any more.

"The risks for today are becoming more about how they are connected and how they play into each other."

What is more, this interconnection of risks requires risk managers to react differently to the risks their organisations are facing, as more risks are introduced that businesses may not have otherwise been exposed to.

"These interconnections can give rise to cascading risk factors," Drzeniek-Hanouz says.

"Risk managers should think about those cascading effects more seriously, rather than thinking of risks as individual events, because it's not about individual events any more.

"It's really about the trends that drive long-term risks and the cascading effects between interconnected risks." **SR**

LIKELIHOOD VS IMPACT

Economic risks such as increased competition, currency and foreign exchange risk, and mergers and acquisitions account for

40%

of the top 10 risks in Europe

Technological risks such as targeted cyber attacks, failure of critical IT systems and non-malicious loss of critical data accounts for

20%

of the top 10 risks in Europe but it is deemed the most costliest risk

"RISKS ARE INCREASINGLY COMING TOGETHER – WE CANNOT THINK IN TERMS OF CATEGORIES ANY MORE"

Margareta Drzeniek-Hanouz, World Economic Forum

Don't rule out an unforeseen calamity

Unlikely they may be, but hidden risks and 'black swan' events can be extremely damaging. So, how do you prepare for the unexpected?

The economic downturn and increased competition may be topping the risk agendas of Europe's risk managers, but a failure to address the unexpected risks lying beneath the surface could be just as calamitous. This was one of the key findings of a European risk management survey conducted by *StrategicRISK*.

The failure of critical IT systems, failure to innovate and damage to company reputation or brand are risks with a low likelihood of occurrence but a high financial impact, should they take place.

Speaking to *StrategicRISK*, FERMA president Jo Willaert said businesses must conduct a proper assessment of the risk landscape they are operating in before they make any strategic decisions.

"It is crucial that when you set up the strategy of the company, you are aware what all the risks are and that people are taking care of those risks," he says.

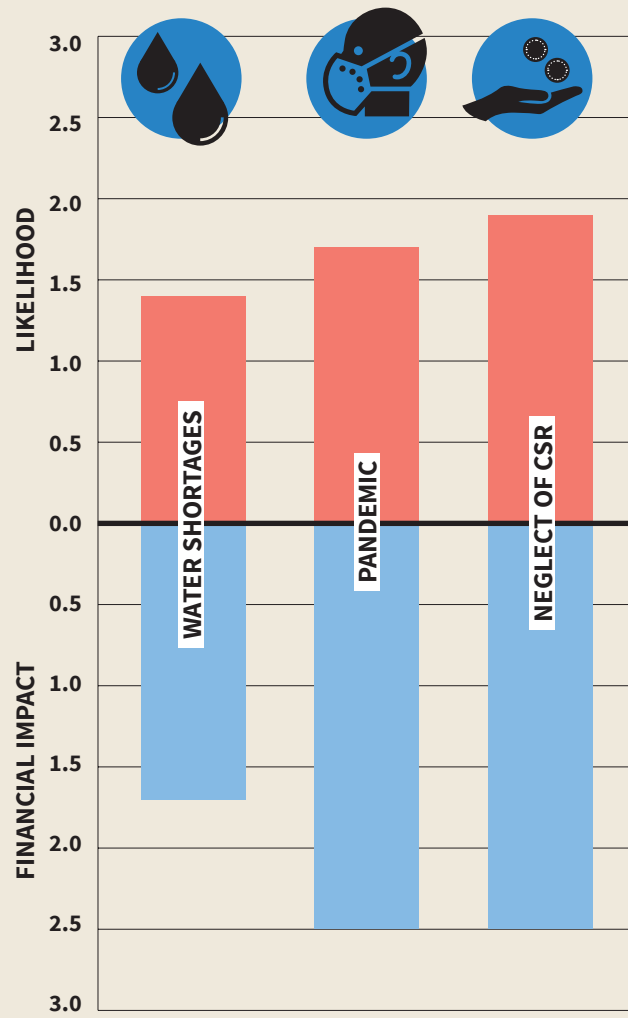
John Windsor, head of insurance at Marks and Spencer, says organisations can prepare for these unexpected events through the use of traditional risk management techniques, to assess the risks, and through careful crisis management planning.

"The most important thing is to know what your risk is – quantify and identify the risk and make sure you understand it," he says. "Your business continuity plan must involve the physical part of your business, but the IT guys and insurers must also be included from day one, as should the press office to ensure you all speak with one voice. You don't want to have people going off and saying things they don't have enough knowledge of to discuss."

10 HIDDEN RISKS (LOW LIKELIHOOD, HIGH IMPACT)

- Damage to company reputation/brand
- Failure to innovate
- Failure of critical IT systems
- Terrorist attack
- Supply chain risk
- Contractual risk
- Non-malicious loss of critical/customer data
- M&A
- Fraud and corruption
- Currency/FX risk

HIDDEN RISKS



COMMUNICATION IS KEY

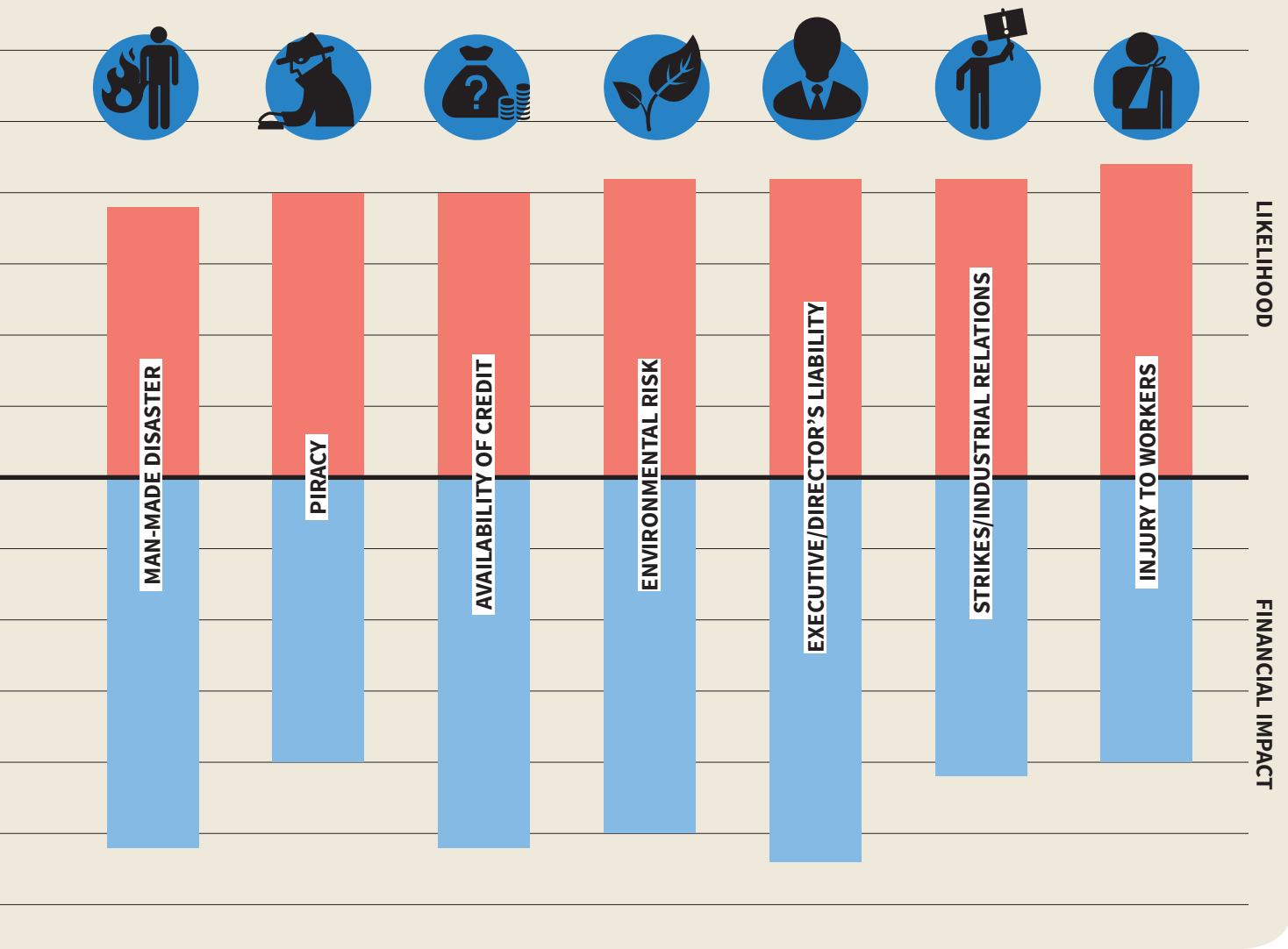
He adds: "Reputational risk in any event, whether it be cyber or fire, is hugely important. You have to maintain the support, loyalty and confidence of your customers. The most important thing when something does happen is to make sure you've got a tried and tested response to these things.

"Communication is key – it has to be confident communication to make sure your customers realise you do know what you are talking about and you are trying to address the situation."

Margareta Drzeniek-Hanouz, director of the Centre for Global Competitiveness and Performance at the World Economic Forum, notes that companies must also be aware of the costs of risk mitigation and make sure any measures are proportionate to the risk faced.

She adds: "It's really about a cost-benefit assessment and each will be very different depending on the

Some risks may have a low likelihood but if they occur, they could cost companies dearly



operations [of the business] and economic exposure of those risks [to the organisation].

"Proper assessment of that exposure and the potential impact is needed; there's no silver bullet or miracle solution."

As well as the risks highlighted by the survey, Tetra Laval International group risk management and insurance director David Howells says risk professionals also need to be aware of the threat of black swan events. "These 'hidden risks' or 'black swan' events, are considered to be so unpredictable that they cannot be measured or modelled," he adds. "But that doesn't mean they should be ignored.

"While they may seem to come as a complete surprise, it is generally accepted that they can be rationalised afterwards. Risk managers can prepare; using previous events we can develop scenarios to test our resilience.

"It is a challenge to motivate an organisation to consider events that are, by definition, so unlikely to occur that they cannot be modelled, but the use of examples helps. The organisation's strategy will have considered these scenarios and without even identifying the event, it will have considered how diversified it is, it will monitor performance across a multitude of areas and use key indicators to determine when it is necessary to rebalance and realign operations."

"YOUR PLAN MUST INVOLVE THE PHYSICAL PART OF YOUR BUSINESS, BUT THE IT GUYS AND INSURERS MUST BE INCLUDED FROM DAY ONE, AS SHOULD THE PRESS OFFICE"

John Windsor,
Marks and Spencer

BOTTOM 10 RISKS – COMBINED

Water shortages	1.6
Piracy	2.0
Pandemic	2.1
Injury to workers	2.1
Strikes/industrial relations	2.1
Social unrest	2.2
Neglect of CSR	2.2
Climate change	2.2
Man-made disaster	2.3
Environmental risk	2.3

But Windsor says it is important for risk managers not to overlook the more old-fashioned threats. "Yes, you do have to look at the emerging risks, but you can't forget about the traditional risks that have been around for many years," he says. "For me, the three main threats would be the traditional perils, fire and flood, because of the effect they can have depending on where and when they hit, as well as terrorism and cyber risks." SR

Getting to grips with the General Data Protection Regulation

Significant penalties for non-compliance will force firms to report breaches, writes Varonis senior content producer Andy Green

It's been a long time coming, but the new EU data security and privacy law, known as the General Data Protection Regulation (GDPR), was finalised at the end of 2015. With the rules now set in stone, companies will be given two years to become compliant and the GDPR will likely go into effect some time in 2018.

The GDPR can be seen as an evolution of the EU's existing data rules, the Data Protection Directive (DPD). If your company is new to the EU market, then the GDPR might be a challenge. However, any company that follows IT best practices or industry standards should not find it too burdensome.

One way to describe the GDPR is that it simply legislates a lot of common sense data security ideas, especially from the 'privacy by design' school of thought: minimise collection of personal data, delete personal data that's no longer necessary, restrict access, and secure data through its entire life-cycle.

DPD 2.0

The Data Protection Directive has been around since 1995, but as technology marched on, some of its shortcomings became more apparent. The internet, the cloud and Big Data were just a few of the factors that forced the EU to reconsider its approach to its data security law. One of the main problems with the directive is that it allowed member countries to write their own legislations, using it as a template, and then enforce the rules separately. With the aforementioned technology disruptions, member countries had different interpretations as to what constitutes personal identifiers (MAC addresses? biometric?) or who's responsible when data is on the cloud (the company or the service provider?).

Realising the old data security law had to be revamped, the EU Commission in 2012 started the process of creating legislation. Its primary goal was a single law covering all EU countries and a 'one-stop shop' approach to enforcement through a single data authority. The GDPR is not a complete rewrite of the DPD. Instead, it enhances the DPD. Interestingly, back in the 1990s, the DPD also had as its goal a single law to replace individual national laws.

The GDPR looks like it will realise that dream – or come a lot closer. So it's probably better to view the law as DPD 2.0. However, it adds a few important changes. Most significantly, there's a breach notification requirement that would force companies to notify the data authorities and consumers when there's been a data exposure. There's really nothing like that in the US (yet).

Another change is that the penalties for non-compliance will be significant. The GDPR will have a tiered fine structure. For less significant lapses, a company can be fined 2% of global revenue, and more serious infringements will merit up to 4% of global revenue. One could argue that the GPDR is really focusing on multinationals, particularly US ones, which earn most of their revenue outside of the EU.

> **ARTICLE 17 STRENGTHENS RULES ON DELETION AND ADDS THE RIGHT TO BE FORGOTTEN**

VOCABULARY

The GDPR is a huge document – more than 100 pages of legal language. However, for IT and security folks who will have to implement some of the rules, the key parts are in just a few of the regulation's articles.

But before we dive in, let's get some basic vocabulary out of the way.

In the GDPR, personal data means any information "relating to data subject". A data subject is "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used" by someone.

This somewhat convoluted definition is actually the language of the original DPD. As with the old rule, the GDPR encompasses obvious identifiers such as phone numbers, addresses and account numbers, as well as internet-era identifiers such as email, biometric – just about anything that relates to the person.

The GPDR also accounts for what's known as quasi-identifiers. These are multiple data fields – typical geo and date – that through a little bit of processing and external reference sources one can use to zero in on the individual indirectly. In any case, personal data is what you are supposed to protect! Data that has been anonymised is not covered by the GPDR or, for that matter, the current DPD.

The GDPR also continues with the DPD's terminology of data controller and data processor, which are used throughout the law. A data controller is anyone who determines the "purposes and means of processing of the personal data". It's another way of saying the controller is the company or organisation that makes all the decisions

about initially accepting data from the data subject. A data processor is then anyone who processes data for the controller. The GDPR specifically includes storage as a processing function, so that takes, say, cloud-based virtual storage into account.

Putting all this together, the GDPR places rules on protecting personal data as it's collected by data controllers and passed to data processors. One shortcoming of the DPD was that it left some loopholes for data processors – i.e. cloud providers – that the GDPR now effectively closes off.

THE ARTICLES

Now let's get into some of GDPR's legalese. The new law puts in place more specific obligations on data processors and therefore the cloud. This is described in articles 26 (processor) and 30 (security of processing) – for wonks, this parallels the DPD's article 17 – and effectively says that the cloud provider must protect the security of data given to it by the data controller.

The GDPR makes it possible to directly sue a processor for damages – in the DPD, only the data controller could be held liable. Article 5 (principles related to personal data processing) essentially echoes the DPD's minimisation requirements: personal data must be "adequate, relevant, and not excessive in relation to the purposes for which they are processed". But it also says the data controller is ultimately responsible for the security and processing of the data.

Article 23 (data protection by design and default) further enshrines privacy by design ideas. The article is more explicit about data retention limits and minimisation in that you have to set limits on data (duration, access) by default, and it gives the EU Commission the power to lay down more specific technical regulations at a later time.

THE NEW STUFF

There are a few new requirements that directly impact IT. Again if you're following common sense best practices, none of the following should be too much of a burden. The bureaucracy involved in DPIAs (see below) will likely cause some head-scratching (and cursing), but the details will probably have to be worked out by the regulators.

Article 28 (documentation) adds new requirements for data controllers and processors to document their operations. There are now a number of rules for categorising the types of data collected by controllers, recording the recipients for whom the data is disclosed, and specifying an indication of the time limits before the personal data is erased.

Article 33 calls for data protection impact assessments (DPIAs) before the controller initiates new services or products involving the data subject's health, economic situation, location and personal preferences—and more specifically, data related to race, sex life and infectious diseases. The DPIAs are meant to protect the data subject's privacy by forcing the controller to describe what sort of security measures will be put in place.

The new breach notification rule has probably received the most attention in the media. Prior to the GDPR, only telecom and ISP service providers had to report breaches within 24 hours under the e-Privacy Directive.

Modelled on this earlier directive, article 31 of the GDPR says controllers must tell the supervisory authority the nature of the breach, categories of data and number of data subjects affected, and measures taken to mitigate the breach.

Article 32 adds that data subjects must also be told about the breach, but only after the supervising authority is informed.

Article 17 (the right to erasure and to be forgotten) has strengthened the DPD's existing rules on deletion and adds the controversial right to be forgotten. There's now language that would force the controller to take reasonable steps to inform third-parties of a request to have information deleted.

This means that in the case of a social media service that publishes personal data of a subscriber to the web, they would have to remove not only the initial information, but also contact other websites that may have copied the information. This would not be an easy process!

Finally, a requirement that has received less attention but has important implications is the new principle of extraterritoriality described in article 3. It says that if a company doesn't have a physical presence in the EU but collects data about EU data subjects – for example, through a website – then all the requirements of GDPR are in effect. This is a very controversial idea, especially in terms of how it would be enforced.

COMPLIANCE

Before the GDPR was finalised, there were two competing versions from the EU Council and the Parliament. Compromises were made in a few well publicised areas, especially breach notification and fines.

For example, the GDPR has fallen a little short of its initial goal of a one-stop shop: a single supervising authority that would handle complaints and enforce the law.

Instead, in the council's version, companies will deal with a lead DPA in the country where the controller is based. This gets complicated when personal data is transferred to another EU country, and so DPAs in those countries would get involved as well. However, if there's no agreement among all the DPAs, then the case goes to a super-DPA, the European Data Protection Board, whose decisions would be final.

> **FOR COMPANIES CAUGHT IN THE EXTRATERRITORIALITY NET, THE GDPR WILL COME AS A SHOCK**

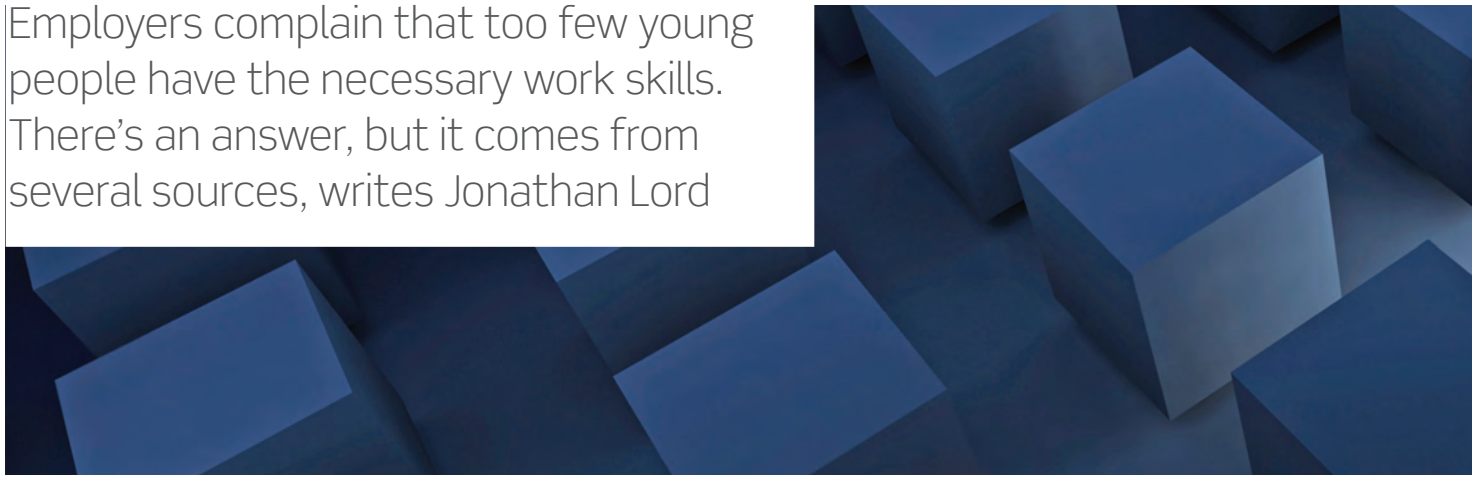
Bottom line: companies will likely have to deal with several DPAs.

For companies new to the EU market and any company, particularly US ones, caught in the extraterritoriality net, the GDPR will still come as something of a shock. This is especially true for web-based services that are not regulated under existing US financial or medical data security laws.

As you work out your own strategy for the GDPR, here are four areas where you should be focusing your attention and resources:

- **Data classification** – Know where personal data is stored on your system, especially in unstructured formats in documents, presentations and spreadsheets. This is critical for both protecting the data and also following through on requests to correct and erase personal data.
- **Metadata** – With its requirements for limiting data retention, you'll need basic information on when the data was collected, why it was collected, and its purpose. Personal data residing in IT systems should be periodically reviewed to see whether it needs to be saved for the future.
- **Governance** – With data security by design and default the law, companies should focus on data governance basics. For unstructured data, this should include understanding who is accessing personal data in the corporate file system, who should be authorised to access, and limiting file permission based on employees' actual roles – i.e. role-based access controls.
- **Monitoring** – The breach notification requirement places a new burden on data controllers. Under the GDPR, the IT security mantra should "always be monitoring". You'll need to spot unusual access patterns against files containing personal data, and promptly report an exposure to the local data authority. Failure to do so can lead to enormous fines, particularly for multinationals who have large global revenues. **SR**

Employers complain that too few young people have the necessary work skills. There's an answer, but it comes from several sources, writes Jonathan Lord



The skills gap damaging Europe and the UK

The graduate and school leavers' skills gap has come under the spotlight recently, with the UK generally seen as faring poorly.

Research by the Chartered Institute of Management Accountants in 2015 identified UK school leavers as the worst in Europe for essential skills, and the Confederation of British Industry believes a lack of high-quality apprenticeships has created an unskilled workforce through the exacerbation of numeracy and literacy problems.

The government has been pushing for a major increase in the number of apprenticeships, but there are still questions over whether enough is being done to make sure young people view such options as worthy alternatives to university.

Some companies, such as Rolls-Royce, have more than 1,000 science, technology, engineering and mathematics (STEM) ambassadors worldwide. Employees of the company spend at least 60,000 hours a year delivering STEM programmes to local communities.

Despite such initiatives, a recent YouGov study found that nearly six in 10 employers of STEM graduates think there is a skills gap in the UK.

The *STEM Skills Gap Report* found that 59% of businesses and 79% of universities surveyed believe there aren't enough skilled candidates leaving the education system to meet the employment requirements of industry.

The survey also demonstrates a need for greater collaboration between academics and businesses, as the study reveals that universities' approach to teaching STEM subjects does not always tally with the needs of employers.

One of the most important debates is whether companies, the government or individuals should 'fund' education to ensure they are provided with the skills they require.

In reality, the responsibility should be levelled at employers, to train staff to meet the needs of their specific business, and at the government, to create a valued education system better able to prepare young people for life beyond the classroom.

A report by the Institute of Directors reveals that its members consider STEM knowledge to be important, but the following skills even more so:

- honesty and integrity
- basic literacy skills
- basic oral communication skills (e.g. telephone skills)
- reliability
- being hardworking and having a good work ethic
- numeracy skills
- a positive, 'can do' attitude
- punctuality
- the ability to meet deadlines
- team working and co-operation skills.

Universities and other educational partners have a responsibility to acclimatise young people to the world of work at a much earlier stage through employability programmes and greater work experience opportunities. The promotion of more paid placements, internships and apprenticeships is also important.

Businesses need to acknowledge that skills shortages are not just a problem for graduates trying to find their way into the world of work; they can create serious difficulties for businesses trying to recruit the employees they need.

In 2016, the UK government recognised that the digital economy requires workers to have specific skills. It has adopted the five basic digital skills as defined by the charity Go.On:

- managing information
- communicating
- making payments
- solving problems
- being able to create things online.

Go.On believes more than 12 million people, and a million small businesses in the UK, do not have the appropriate skills to prosper in the digital era. But the UK is not the only country suffering.

According to a report by management consultants McKinsey – *Education to Employment: Getting Europe's Youth into Work* – more than a quarter of European employers are struggling to fill vacancies at a time when young people are facing high levels of unemployment. The report, drawn from a study of eight major European economies, states that youth unemployment has hit crisis levels. In the European Union, 5.6 million young people are out of work, with southern Europe suffering the most.

The study calls for better alignment between the worlds of education and employment, warning that education providers have too much confidence in the relevance of what they are teaching. Tellingly, 74% of the education providers surveyed believed that young people were being equipped with skills for work; only 35% of employers agreed that this was the case.

The skills shortage in the UK is one of the most severe, resulting in a 'war for talent', according to the Global Skills Index from recruitment group Hays and consultancy Oxford Economics.

Industries such as engineering and technology have suffered the most from the skills gap and the remedy can be found in better training, attracting highly skilled workers from overseas and better investment in technology.

Last July, the UK government unveiled an ambitious plan to boost productivity. It wants to train up 3 million apprentices by 2020 to fill the skills gap in areas such as engineering.

This has been welcomed by business leaders. However, many are critical of the government's policy on immigration, which they say deters highly skilled workers from outside the EU, aggravating the shortage of skills. The government has also launched an inquiry into the Tier 2 Skilled Workers system, where the most pressing questions to consider will be:

- What impact has the cap of 20,700 employer-sponsored skilled migration (Tier 2 general) visas had upon employers?
- Which sectors have been particularly affected?
- If a cap on Tier 2 skilled workers remains, what is the best way to meet the needs of the UK economy while maintaining control of the number of skilled workers coming to the UK from outside the European Economic Area (EEA)?
- If the cap on Tier 2 were to be removed, what would replace it?

The government hopes to gain an insight into whether the current system is the best way to achieve its aim of a controlled immigration system that can maintain essential levels of skilled workers.

The introduction of apprenticeships and the review of work visas could address some of the longer-term issues. In the short term, companies can quickly identify their own skills shortage by analysing recruitment and retention rates, and targeting jobs that have not been filled or have a high attrition rate due to employees not being sufficiently skilled.

Companies can establish their own graduate or apprenticeship schemes based around their own needs. They can also improve links with schools and universities to outline what kind of workers they need, so that educational institutions can introduce measures into the curriculum to improve the overall employability of students.

One of these initiatives is the 'Degree Apprenticeship', in which 40 companies have hired IT apprentices in partnership with universities such as Manchester Metropolitan University, Queen Mary University and Northumbria University. The premise is that businesses are able to integrate the individual into the culture of a company while they are studying, rather than waiting until the person graduates and taking a risk on whether or not they are 'work ready'.

As has already been noted, the responsibility of shorting the skills gap should be the triumvirate responsibility of employers, the government and educational institutions, working in partnership to strategically target specific areas of concern, in the short and long term.

It is also the responsibility of the individual to ensure they have the correct skills for their chosen career. They should gain practical working knowledge of the sector by applying for part-time work, placements or internships, seek advice as to what employers are looking for in their employees and work towards these skills and attributes. ■

ACCORDING TO MCKINSEY, MORE THAN A QUARTER OF EUROPEAN EMPLOYERS ARE STRUGGLING TO FILL VACANCIES AT A TIME WHEN YOUNG PEOPLE ARE FACING HIGH LEVELS OF UNEMPLOYMENT

Dr Jonathan Lord is a lecturer in human resource management and employment law at Salford Business School

Diamond Geezer

We spoke to Matt Frost, vice-president risk finance at BHP Billiton, about learning the bass guitar at 50, his love for Ipswich Town Football Club and why moving from England to Australia has been one of the best decisions of his career

What are you thinking about right now?
The company is in a challenging commodity price environment. Like many, I am facing the 'business as usual' workload in addition to challenges and responsibilities from a major loss. So right now I am thinking about the challenges of two weeks away from home engaging with brokers, insurers and stakeholders in Singapore, London and Brazil and ensuring all the moving parts are moving smoothly and efficiently.

What's your greatest fear?
The health and welfare of my children. They have not been without health challenges and I have been very proud of what they have become and what they have achieved, but we live in troubled times and like most parents, you constantly worry about them.

What's your most embarrassing moment?
Probably crying at my wedding after seeing Melanie come down the aisle. 'Fortunately' one of my 'friends' recorded the wedding and so has never let me or my friends in the industry forget!

What makes you happy?
Playing the bass guitar. I took it up for my 50th birthday after receiving a 1962 Fender Precision Bass and have loved learning and playing ever since. My inner [Black Sabbath bassist] Geezer Butler can shine. It takes me to a different place where I can forget work and life's stresses.

What makes you unhappy?
Playing the bass guitar – I'm hopeless after three years of lessons. Closely followed by when our new cavoodle puppy does his business on the carpet when the back door is open.

What's the biggest risk you've ever taken?
Moving to Australia from England. This was a massive risk for me personally and for the family. We had no idea what to expect, Melanie was pregnant and we had a two-year-old. Making new friends, a new life and a new career after leaving Blighty after 43 years was a real toughie.

What's the worst job you've ever done?
Breakfast waiter at a hotel in Windsor, England, over Christmas and the New Year. I had to cycle to work every morning at 5am in the cold, pouring rain to serve bacon and eggs to the tourists. Worst of all was working New Year's Day: most of the staff never showed up and I was enlisted as the breakfast chef for the morning.

What is your greatest achievement?
Personally, marrying Melanie: somehow she figured I was quite a catch, being 10 years older with three children! Business-wise, taking BHP Billiton into a position of full self-insurance. It took a year of analysis, management reporting and a major captive recapitalisation.

What's the most important lesson you've learned?
If you have the opportunity to work overseas, do it. The exposure to different cultures, ethics, standards and languages is an amazing, enriching experience.

Who do you look up to and why?
My boss, Alistair – he told me to say that or he wouldn't approve the article! Seriously though, a former Willis broker called Bob Martin. His work ethic and happy personality proved nice people with good humour can still succeed in business.

Tell us a secret
I'm a Tractor Boy. That sounds weird. If you don't know what it means, check out the best football teams of the 1970s.

WHATEVER YOUR BUSINESS, WE ARE HERE TO PROTECT IT

Customized solutions for risk transfer, management, prevention and claims handling

Our 1,500 employees are committed to protecting your business over the long term. We can offer you support in 150 countries via our international network.

axa-corporatesolutions.com

AXA CORPORATE SOLUTIONS

redefining / standards

Property insurance solutions on a new global scale.

Our commitment to clients is now even larger with market-leading property insurance capacity of up to $2.5 billion. Our expanded limits reduce the need for multiple co-insurance markets and negotiations, and minimize gaps between layers of coverage. When coupled with expert loss prevention engineering, claims excellence, multinational and local expertise, and consistent, seamless service, you can count on AIG's total commitment to support your risk management goals at your facilities around the world. AIG is a full service partner that can respond to all of your Property Casualty insurance needs. To learn more, visit www.AIG.com/globalproperty

AIG®

Bring on tomorrow®