StrategicRISK

RISK AND CORPORATE GOVERNANCE INTELLIGENCE

Spring 2015 Issue 100

www.strategic-risk-global.com

ISSUES AND COUNTING...

Anniversary edition charts the changing face of risk and the profession

Cyber Sphere

Protecting businesses against Cyber risks

AXA CORPORATE SOLUTIONS

redefining / standards

StrategicRISK

Issue 100
Spring 2015
www.strategic-risk-global.com

Editor Mike Jones
Deputy editor Kin Ly
Managing and legal editor Hélène Préchac
Asia editor Sean Mooney
Senior reporter Asa Gibson
Commercial director, Asia-Pacific Adam Jordan
Senior production controller Alec Linley
Senior data analyst Fayez Shriwardhankar
Publisher Jack Grocott
Publishing manager Tom Byford
Executive publisher, Asia-Pacific William Sanders
Managing director Tim Whitehouse
Cover image Shutterstock
Email: firstname.surname@nqsm.com

ISSN 1470-8167
Published by
Newsquest Specialist Media Ltd
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)
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

INSIDE

Leader

EXCITING TIMES AHEAD

Much has taken place since *StrategicRISK*'s birth 15 years ago – and change continues

THE SHARP-EYED among you might have noticed that this is the 100th edition of *StrategicRISK*. We are marking the occasion in a number of ways, starting with a new look for the magazine and an enhanced presence online.

In this issue, we look back at the history not only of the publication but also at the changes to the risk landscape and the profession since *StrategicRISK* was first published in June 2000.

I wonder how many of you have been readers since that first edition. Just as the international risk community has grown, so too have the range and complexity of the risks faced and opportunities presented. Even the smallest businesses now effectively operate on a global basis, if not in terms of customers then certainly in respect of their supply chains.

The range of risks has multiplied and intensified, particularly around technology and so-called intangible risks. Where once property was the largest asset of a business and thereby its biggest physical risk, now intellectual property is becoming increasingly important.

How to protect against the loss or address the consequences of other non-physical risks such as reputation has been the subject of much debate and conjecture, particularly among the insurance profession. This discussion is likely to continue for some time yet. What is evident, however, is that more sophisticated risk management techniques and processes developed and instilled within the structure of large corporate business in the past 15 years leave businesses better prepared than ever to deal with the majority of challenges faced.

StrategicRISK has evolved considerably since its inception. Highlighting risks and potential strategies for dealing with threats and opportunities has always been at the heart of the magazine's activity, but the scope of what it covers has increased markedly.

Not only is this true for the span of risk covered by the publication but also in terms of our readership in respect of geographical reach through magazine distribution and our website and email newsletters.

Two years ago, *StrategicRISK* launched across Asia with a unique magazine and website and a continuing series of events held in countries across the Asia-Pacific region. In April, the second *StrategicRISK* Forum will be held in Singapore, aiming to build on the success of last year's inaugural event, which attracted almost 200 risk professionals from across the region.

The brand's success in the Asia-Pacific region was recognised in February, when *StrategicRISK* Asia won the Risk Management Journalism award at the Institute of Risk Management's Global Risks Awards. Although the publication goes from strength to strength in Asia, *StrategicRISK* continues to develop its international focus by, in April, launching in the Middle East and Africa region.

We have been working with MEA-based risk professionals and businesses for some time to help develop the brand and will host a series of events in the region in the coming months.

These are exciting times for *StrategicRISK* and your fellow risk professionals around the world. The risks might be getting bigger and more demanding, but at least the topic is now attracting far more attention at board level than ever before.

Transforming that interest into meaningful action through greater board understanding of some of the issues that comprise corporate risk is perhaps the next main challenge. This is starting to happen but the process is slow, albeit necessary.

What *StrategicRISK* will be covering in the next 100 editions depends on how the global risk landscape changes and predicting that, as most of you know only too well, can be difficult at best.

What can be stated with certainty, however, is that whatever the future holds, the risk community has never been better prepared or more able to take on those risks.

Mike Jones
Editor, *StrategicRISK*

> **"Risks might be growing but at least the topic is attracting attention at board level**


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®

Analysis

The changing face of risk management and insurance

The risk landscape has grown so complex that risk managers are compelled to take on new responsibilities. Insurers, meanwhile, face pressure to find solutions to 21st-century risks. With that in mind, how do leading risk managers, insurers and brokers see the industry's future?

> **"Nowadays, in a globalised world, risk managers have to take a more strategic approach**

In a landscape evolving constantly, risk managers have to change the way they operate, according to the vice-president of FERMA.

"Traditionally, risk managers focused on operational risks and threats arising from insured risks," said Michel Dennery at the annual conference of French risk management association AMRAE, which was held in Cannes. "However, nowadays, the responsibilities for risk managers have extended to include financial and strategic risks.

"The risk landscape has become so complex that risk managers have to change how they deal with risks. For instance, 10 or 20 years ago, when a risk arose, a risk manager's approach would be to treat the threat as an operational risk.

"Nowadays, in a globalised world, risk managers have to take a more strategic approach and not only consider how a given risk could interrupt business but how it could damage a company's reputation.

"There are two main tiers to a risk manager's role now – operational and strategic – and risk managers should practise both. It would be ineffective if risk managers focused solely on strategy or operations since this will not prevent or mitigate risks and could exacerbate a product recall, for instance."

Greater involvement

During February's conference, Dennery moderated a panel debate, 'The future of risk management', which discussed the role of the risk manager. One of the panellists – Sébastien Rimbert, a senior manager at EY – complained that risk managers are not involved in strategic decision making.

"There are a number of challenges for risk managers. The first is that they are not sufficiently involved in strategy," he said.

FERMA's 2014 *Benchmarking Survey* also identified this gap, suggesting risk managers must be involved in discussions about business strategy and areas such as investment and acquisitions.

"To be credible and recognised at strategic level, risk managers must be able to influence decision making and advise executive management on areas such as the cost of a risk, business strategy and risk financing. Supplying top management with a risk report is no longer sufficient," said Rimbert.

"The second challenge is that risk managers must develop strong relationships with all departments within the business. FERMA's survey highlighted several departments that risk managers do not have strong engagement with, including HR and IT.

"The last challenge is in providing regular quantitative analysis to executive management. Interestingly, the survey found that risk managers do not use IT or audit tools enough to support them, but if they did, they may be able to provide regular quantitative information to the board." **SR**

AMRAE

Old problems, new problems. What is the connection?

Emerging risks, such as cyber and terrorism, are set to become a prime focus for insurers and risk managers

Emerging threats are likely to become a sub-set of existing risks – meaning that risk managers must avoid working in silos and adopt a holistic approach.

That was the key message from a panel of insurer and broker executives at Airmic's inaugural fastTrack forum chaired by *StrategicRISK* editor Mike Jones.

The panel comprised Willis chairman and chief executive David Martin, ACE UK and Ireland regional president David Robinson, AXA Corporate Solutions UK chief executive Matthieu Caillat and Lockton chairman of international operations Mike Hammond.

Titled 'Future of the insurance market', the event reviewed the industry's approach to emerging risks such as cyber, terrorism and reputational damage.

The crucial message was that each party involved in the transfer of risk must consider how emerging risks connect with existing ones. Delegates were advised to avoid a silo approach to emerging risks.

Lockton's Hammond said: "As an industry, we need to understand not so much the emergence of new risks, but how existing risks could merge into new ones. It is easy to think we can compartmentalise risks into old and new. [Risk and insurance professionals] should view risks holistically."

Clarity and transparency

The discussion moved on when Willis's Martin asked whether insurers could quantify exposures and losses linked to emerging risks, particularly with regard to cyber.

He said: "The problem with most emerging risks is that there does not appear to be a general consensus about the type of cover required."

Clients lack clarity over which risks should be transferred to an insurer because the true probability of a loss is unclear, he added. "The market needs to know what premium is required… in order to create insurable propositions."

By way of example, Hammond cited issues related to cyber risk. He said the industry must be more transparent about the frequency and scale of cyber breaches. Being open with this information will provide insurers with more data to quantify loss and consequences.

The effect of globalisation

ACE's Robinson asked the panel to consider how globalisation had changed the insurance market. "Customer expectations have changed significantly in the past few years," he said. "Clients are more empowered than they have ever been; they are used to faster solutions and live in an instantaneous world.

"That means insurers must address emerging risks in a way that meets expectations in terms of speed but also regarding cover. We have to embrace technology and data for us to do that."

AXA's Caillat concluded the debate by touching on trends related to intangible threats. The consequences of intangible risks are likely to soar in the future, he said, adding that insurance was not designed for these risks.

"Insurance policies were not originally designed for these types of risks, meaning insurers have to evolve and adapt. They will need to be innovative and work with brokers and the insured to find the best solutions." **SR**

> **"Clients are more empowered than they have ever been – they are used to faster solutions**

Analysis

Businesses must adjust to an increasingly dangerous world

A gloomy report from the World Economic Forum suggests that corporate exposure to geopolitical risk is a key concern in 2015

Concerns about the global economy, such as deflation in the eurozone and slow growth in key emerging markets, are far from over. However, rising geopolitical tensions are starting to overshadow – perhaps even compound – these worries.

Given the financial crisis of recent years, the main focus has been on economic risks. This was evident in the World Economic Forum's (WEF) annual *Global Risks* report, which draws on the perceptions of experts in business, academia and the public sector worldwide. Each year, respondents are asked to rate a select number of risks in terms of their likelihood and impact over the course of the next decade.

For the first time in nine years, WEF's top global risk in terms of impact was not economic. In fact, economic risks were absent from the top five risks with the biggest consequences – a list that has included two or more of them since 2007.

> **"The terrorist attacks in Paris suggest the extremist militant threat is getting worse**

This year, interstate conflict with regional consequences was rated first in terms of likelihood and fourth in terms of impact. High-risk ratings for failure of national governance (third-most likely), state collapse or fall (fourth-most likely) and weapons of mass destruction (fourth-biggest impact) meant more geopolitical risks appeared towards the top of the table than ever.

Almost 900 experts rated 28 global risks between July and September 2014. Given the political environment at that time, it is perhaps unsurprising that interstate conflict with regional consequences was ranked so highly.

During that period, for example, Islamic State gained control of cities in Iraq and Syria, and the Israel-Gaza conflict escalated after the Jewish state blamed Hamas for the murders of three Israeli teenagers in June. In addition, tensions in Ukraine led to clashes between the new government and pro-Russian separatists on the country's eastern border and led to the annexation by Russia of Crimea. Political and societal unrest in Hong Kong, Thailand, Egypt and Libya were also significant to the risk landscape in 2014.

In the six months since the 2015 survey was conducted, the geopolitical risk landscape has been exacerbated, according to WEF report advisory board member Steve Wilson, who is Zurich's chief risk officer for general insurance.

"The situation with Russia seems to be increasingly tense, and leading military figures have made many comments warning about Putin's agenda [concerning Russia's influence in Eastern Europe]. In addition, the terrorist attacks in Paris suggest the extremist militant threat is getting worse," he says.

Growing fragmentation

The key risk for corporates arising from such political tensions concern business interruption (BI), according to WEF report steering board member John Drzik, Marsh's president of global risk and specialties.

"The potential sources of BI are diversifying as the world evolves and fragments in a geopolitical sense and develops in a technological sense. This [amplifies] the challenge for firms when assessing potential sources of BI and has created a more challenging risk landscape," Drzik says.

Corporate exposure to geopolitical tensions has become a global trend that Wilson says could be a catalyst for growth in the insurance market.

"Economies are connected, trade is connected and when geopolitical tensions arise that threaten trade and contracts between businesses across borders, there is a need for growth in political risk and credit risk insurance markets," he adds.

In terms of risk management, firms should account for geopolitical risk when evaluating investment plans and supply chain strategies, says Drzik.

"Geopolitical events are likely to be more frequent in the next few years and could cause disruption in different parts of the world. A good risk management strategy is to avoid undue concentrations of supply chain, investment portfolio or other risk exposures the firm may have," he says.

Globalisation and the financial crisis have encouraged businesses to invest in emerging markets. It means that firms are perhaps more exposed to conflict and political rivalry than ever before, at a time when the global geopolitical landscape is increasingly uncertain.

The situation in Europe is particularly hard to read: the economy is sluggish, Ukraine's future remains unclear, tensions between the EU and Russia are rising, religious extremism is spreading from the Middle East and the election of Syriza in Greece is raising questions about the eurozone's stability.

As with most risks, circumstances are subject to change and the geopolitical landscape is certainly one for risk managers to watch. **SR**

When it comes to economic trouble in Europe, currency and trade credit risks leave the current Greek drama in the shade

Never mind Grexit – the real worry is deflation


Shutterstock

The initial hysteria that shrouded talks between Greece and its eurozone creditors has perhaps deflected from the EU's wider issues.

The pound sterling reached a seven-year high against the euro at the start of March, a day after the European Central Bank (ECB) initiated its strategy to curb deflation through a process of quantitative easing (QE). It was the first time since December 2007 that sterling had reached €1.40 after rising 0.4%, according to Reuters. March also saw the euro hit a 12-year low against the US dollar, almost reaching parity before it regained some ground.

Economic growth in the EU is also hindered by high unemployment rates, particularly in Southern Europe. The World Economic Forum (WEF) expects joblessness to remain at current levels until 2018. This "reflects a growing problem of structural unemployment in advanced economies" and "will likely keep wages low, maintaining deflationary pressures", according to the WEF 2015 *Global Risks* report.

The likelihood of Greece exiting the EU or the eurozone (Grexit) may have been exaggerated by the media, but it remains a possibility nonetheless. Discussions with eurozone creditors and the European Commission have not been positive, but there are bigger issues in Europe, according to Lockton senior vice-president Nadine Moore.

"Although the Greek restructuring has driven many headlines, it is a much smaller issue than the economic headwinds, such as deflation, credit losses and currency risks," she says. "Southern Europe continues to have credit losses, although the losses have slowed. There is a consensus that most distressed companies have either closed or become insolvent, but that does not mean there will not be future losses. Overall, trade has declined in the region."

Moore says the Swiss National Bank's surprise decision to abandon the currency cap pegging the Swiss franc to the euro destabilised money flow, and that most firms were unprepared for the strengthening of the US dollar, which has amplified currency risks for firms trading in or with the eurozone.

Praise for QE

The ECB's decision to introduce QE was long overdue, according to a number of risk analysts. Mike Liu, quantitative analysis director at macroeconomic research firm Roubini Global Economics (RGE), says prolonged deflation would likely have dire consequences for EU firms and global corporates.

"There is justifiable concern about the risk of prolonged deflation in the eurozone given structural reasons, such as weak growth potential, high total indebtedness and excess capacity in certain industries," says Liu.

The severity of continued deflation in the eurozone should not be underestimated, according to Lockton's Moore, who says counterparties selling into the eurozone face increased pricing pressure and currency pressure owing to the euro's continued depreciation.

"The effect of deflation is much more severe than recession. If continued, the financially strong countries will likely weather the storm. Those on the periphery, such as Italy, may have a harder time raising capital and keeping credit flowing," adds Moore.

Multinational risk managers will be wise to monitor inflation rates in the next 18 months as the ECB proceeds with its plan to purchase EU government bonds and asset-backed securities for a combined €60bn each month until September 2016. The strategy will see the institute inject €1.1trn into the eurozone economy and Liu is confident that will have the desired effect for the corporates.

"ECB QE will reflate asset prices, generating positive wealth effects, partially contributing to cyclical growth improvement in the eurozone," he says.

Whether the ECB's QE programme successfully boosts inflation rates in the eurozone to the institute's desired level of just above 2% remains to be seen. For the time being, currency and trade credit risks are likely to be prominent factors on the corporate risk landscape in Europe. SR

> "Countries such as Italy may have a hard time raising capital and keeping credit flowing

Analysis

Why the IRM's new boss puts people before procedures

Incoming chief executive Ian Livsey urges the risk community to collaborate on professional standards and publicise ERM's benefits

As risk management evolves, more and more risk managers with an ERM focus are being employed to tackle the complex risks of the current business environment. ERM is a function that could be enhanced with risk management standards, says the IRM's new chief executive Ian Livsey (pictured).

In his first interview since succeeding interim chief executive Jeremy Harrison at the beginning of February, Livsey gave a frank assessment of the professional status of risk management and its role in the corporate arena.

Although Livsey is not a risk manager by background, he has extensive experience in working for and leading a number of professional bodies that provide standards and accreditation. It is this knowledge and experience that he will bring to the risk management community while at the helm of the IRM.

Livsey was previously chief executive at UK temporary labour licensing firm Gangmaster Licensing Authority and the Centre for Rail Skills, which sets national occupational standards for traction and stock maintenance.

He also chaired a number of organisations that provide professional trade standards and accreditation to practitioners, such as the UK government's TrustMark organisation, representing the repair, maintenance and improvement sector; and JTL, a non-profit charity that offers apprenticeships and training in building and engineering.

Central role

In his new role, Livsey is an advocate for ERM, an approach that has grown in popularity over the past 15 years. He says the IRM has a responsibility to use its global position to communicate the benefits of ERM to the wider economy.

"The IRM has a central role to communicate to businesses [the value of ERM] and that taking an enterprise-wide approach will be achieved through people and not procedures. Procedures underpin what people believe," he says.

Livsey says establishing standards for professional risk managers could help enhance ERM. The institute will launch a certification scheme in the coming months that will include standards of practice, behaviour and a code of ethics, using a framework that benchmarks risk competence and includes qualifications and continuing professional development.

The IRM's plans pit it against FERMA, which is also aiming to launch a certification programme this year. FERMA's European certification programme of competence for risk managers will offer risk managers the opportunity to earn a European Certified Risk Manager certificate.

Collaborative approach

Livsey says the similarities between the programmes reflect a need to enhance the professional recognition of risk management and raise standards of practice and training. Moreover, he says there should be a collaborative approach between organisations in the risk management community.

"There will be offers from us to collaborate with organisations doing similar things," he says.

"There is a need for the risk management community to work together. We are all going in the same direction and collaboration will avoid any confusion, augment what we are doing and help us all reach our goals faster."

Whether Livsey's appointment ushers in a more united approach, his enthusiasm for ERM and enhancing professional recognition for risk managers is likely to add verve to discussions among the risk management community. SR

> "We are all going in the same direction and collaboration will help us reach our goals

Everybody benefits when board members shadow risk professionals

Lionel d'Harcourt, a French risk consultant and ERM expert, sets out his practical guide to winning around executive management

Top management must be involved in creating risk maps if they are to fully understand the value of ERM, says Lionel d'Harcourt, partner at risk consultancy firm Arengi.

"The best way to involve top management in risk and ERM is to get them involved in risk-mapping and to shadow an experienced risk manager," he says. "Only by involving senior management and showing them how risk is managed through an ERM programme will they truly understand the value of the function."

D'Harcourt's advice, outlined in an interview with *StrategicRISK*, sets out how risk professionals can sell ERM's benefits across a business, involve leaders and managers in the ERM process and measure the added value of ERM.

On involving management, he says: "Aligning the views of senior management and the risk team will help identify the risk priorities for the company.

"Once that has been established, there will be a clear view as to what the risk portfolio is and this can be communicated to all departments across the business. All departments can then work together to improve business resilience."

He adds: "In some large organisations, the risk team comprises several professionals – risk managers, insurance buyers, internal control and audit, for example – and these departments often work in silos, so there is a lack of cohesion. Getting management involved in risk will create better cohesion because [managers] can begin to understand where the expertise is and how to build the right team to handle a particular risk."

A good first step

When it comes to showcasing the value of ERM, d'Harcourt says a good first step is integrating risk management into operations. "Embedding risk management concepts and principles into operational decision making will help to promote the benefits of the function.

"Top management is always grappling with several projects – the problem is, they do not always know with which projects to proceed and which ones to stop.

"Risk managers can help here because they will be able to assess and quantify the risks of each project and compare the threat level of each, as well as assess revenue expectations and advice on which ones to invest in and which ones to stop immediately. In essence, risk management can be closely aligned to operations. However, to get close to top management, risk managers need to be proactive." **SR**

Time to rethink business interruption

Marsh's Caroline Woolley warns of a mismatch between how risk managers and insurers approach business interruption risk

Insurers need to "take the blinkers off" and "start treating business interruption (BI) risk with the focus and attention it deserves", says Caroline Woolley, global leader of Marsh's business interruption centre of excellence.

A mismatch between how risk managers view BI and how the insurance industry deals with the risk often leads to gaps in cover, says Woolley.

To a risk manager, BI risk is anything that may interrupt business activity, but insurers have historically focused on BI's property damage element.

Woolley says: "BI does not fit neatly into insurance categories. There are BI elements to many different policies, such as cyber, environmental, terrorism, property damage and supply chain."

Historically, risk managers did not record non-physical BI losses because the risks were usually uninsured – therefore data that would assist insurers when quantifying such losses is scarce.

Woolley adds: "Risk managers are not making informed decisions on risk transfer because they do not have [sufficient] historic information that insurers would like them to have, and that is part of the problem.

"The industry must look at the 'golden triangle' of the insured, insurer and broker. The insurer needs to take the blinkers off and start to look more broadly at BI risks facing [companies] and be willing to collaborate with underwriting teams. Brokers should assist the insured in gathering the right information so they can make informed decisions about risk transfer." **SR**

Viewpoints

V

John Scott,
chief risk officer,
Zurich Global Corporate at
Zurich Insurance Group

AN EYE ON THE WEATHER

Geologist and chief risk officer John Scott flies the flag for mitigation, adaptation and behavioural change in the battle against climate change

DEBATE AROUND CLIMATE CHANGE OFTEN polarises opinion. There are two schools of thought: those who acknowledge that change is taking place and those who deny this is the case despite what appears to be significant evidence to the contrary. Judgements on both sides are often poorly informed through a lack of understanding, deliberate or otherwise.

For those who seek to determine the truth, acknowledging that climate change cannot be considered in simplistic terms one way or another is perhaps the best starting point. Gaining true insight requires consideration of myriad factors, historic and future, and a deep knowledge of the science behind theoretical perspectives and empirical measurement.

Few are better qualified to do this – or to articulate the risks – than John Scott, chief risk officer at Zurich Global Corporate. Scott's role necessitates taking a view on the broader risk landscape for Zurich. He is widely respected among his peers and across the industry for his depth of expertise on some of the key challenges facing businesses around the world. Scott was the only individual from any insurance company to be singled out by several respondents for risk management expertise and knowledge in the recent *StrategicRISK UK Corporate Insurance Buyers' Survey*.

Demand for his services from Zurich and its clients, as well as his involvement with the World Economic Forum and other associations, mean that although Scott is based in London he is only a transient visitor to his own office.

The suitcase next to a coat stand indicates another imminent international departure – to Zurich's Swiss headquarters – on the same day as this interview. Before that, however, he is focused on the issue of climate change.

Scott's academic background – a geology degree from Oxford – and his business experience as a geologist in the oil and gas industry and as a chief risk officer in the insurance industry make him well placed to understand some of the often contradictory factors around climate change and weather, and the potential implications of these from a risk and insurance perspective.

> 'The connection with climate change is a very complicated story. It happens almost outside human observation to what we notice on a day to day basis, which is the weather'

"When you read what's written about climate change in the insurance industry, it generally falls into a couple of categories," Scott says. "It is either broad and high-level, with papers written about the potential future impacts of climate change, or it is focused on adaptation, typically taking an underwriting view around minimising the impact of flooding on property risks."

He has little doubt that human influence "in terms of carbon dioxide emissions" has affected climate change, particularly since the Intergovernmental Panel on Climate Change (IPCC) made that explicit link with the backing of the scientific community.

"Who are we to deny 1,000 scientists agreeing on something when it is hard enough sometimes to get two scientists to agree on anything?" he asks. "We should take it, as a lay community, that the scientific community agrees that there is anthropogenic change [human influence] on the climate."

The bigger question, he says, surrounds the link between changing climate and extreme weather patterns. There is an increasing body of scientific work on this, known as 'attribution'. Intuitively, it would seem reasonable that a warming planet would in some way affect weather patterns. The reality is that is it difficult to say whether any one extreme weather event and its consequences are the result of climate change.

In any one flooding event, many factors influence the level of damage – from management of flood defences through to increased concentration of insured assets in coastal cities – and these have a direct correlation with economic growth.

"Since the 1950s, there has been a dramatic increase in urban dwelling, especially in coastal cities," Scott says. "So when you see a chart over time showing increasing value of assets destroyed by weather-related natural catastrophes, it is difficult to discern whether this secular trend is related to the increasing frequency and intensity of weather-related natural catastrophes.

"If tracking weather intensity – the strength of winds in a hurricane – and the frequency of hurricanes, then it is a little more difficult to see a discernible pattern over time."

Short-term climatic influences

Climate change operates over a long period of time and the earth has many mechanisms that influence weather over the short term. The impact of El Niño and La Niña, ocean current circulation and the movement of the jet stream all influence the weather and it is difficult to discern the effect of climate change on weather models.

The sophisticated computing power of modern meteorologists is showing analysis that a climate signal is affecting the increasing effect of severe weather, but the science is not yet conclusive regarding frequency. As a result, the commercially available natural catastrophe models used by the insurance industry for pricing have only weak climate signals in them. To quote one science journalist on the topic of attribution, "the boffins are still baffled".

"It is clear that the geographic pattern of tropical cyclones is changing," says Scott. "There has been a period of relatively benign Gulf coast hurricane seasons, but hurricane activity and intensity have increased in the Pacific basin. Some have linked this to movements of the jet stream – which in turn relates to the melting of Arctic ice and has an effect on the upper atmosphere – and the occurrence of hurricanes and other severe weather, such as the recent frosts in North America and last year's intense depressions across the UK and the western European coastline."

He acknowledges, however, that the connection with climate change is less straightforward. "It is a very complicated story and it is difficult to make this link, which happens over a very long period, almost outside human observation – over decades if not centuries, if not millennia – to what we notice on a day-to-day, week-to-week basis, which is the weather."

Scott lends some geological context to the picture. "Considering all the science that enables the understanding of paleoclimates [climates in the past], clearly, the earth has gone through periods where there have been greater concentrations of greenhouse gases, carbon dioxide and water vapour in the atmosphere. This is related to increased periods of volcanicity, which is in turn related to the rate of continental drift and the impacts on ocean current circulation, depending on how continental plates and land masses have been arranged around the earth. Over geological time, these factors have had a major effect on climate and sea level.

"Other factors also affect climate, such as the Milankovitch cycles, which relate to the way the Earth oscillates around on its axis as it goes around the Sun," adds Scott. "Over a 30,000-year period, that axis wobbles and this can be seen in the geological record as cycles of sea-level change related to changing climate.

"All these factors influence changing climate on Earth and changing weather patterns and that is way before humans ever evolved. Now humans are here and in the past 150 years they have burned a lot of fossil fuel and emitted a lot of carbon [trapped fossil fuels]. That means carbon from coal, oil and gas buried in the deep subsurface has now been released as carbon dioxide into the atmosphere."

Given that climate change is here for a number of reasons, the challenge for humankind is tackling the problem. The solutions fall into three areas: mitigation, adaptation and behaviour.

Mitigation "has not achieved what was expected or quickly enough", says Scott. "It is now more than 20 years since the Kyoto Protocol and there has been no globally binding greenhouse gas [GHG] emissions agreement."

Some countries have developed policies to introduce low carbon power generation and the transportation industries are slowly beginning to address the challenges of GHG emissions. Overall, these two sectors contribute more than two-thirds of GHG emissions globally.

The International Energy Agency and other agencies have encouraged the power generation industry to introduce renewable power (wave, wind, tidal and solar), nuclear power, hydroelectric power and carbon capture and storage of fossil fuel power plants. There are technical challenges in all these technologies related to base load and intermittency, but new technologies such as smart grids and grid-scale storage are being developed to address this.

Transport developments

In the transport industry, gradual changes in engine technology have led to the development of hybrid vehicles, plug-in hybrids, fully electric vehicles and hydrogen fuel cell vehicles. Technical challenges arise with battery technology and developing a low-carbon hydrogen supply chain, not to mention novel risks to manage and mitigate.

The challenge for the insurance industry is to encourage these developments by providing appropriate risk management insights and, in some cases, niche insurance products.

Insurers have a role to play in providing policies to protect emerging risks around low-carbon energy – "especially the property ones", says Scott.

"There have been some good examples in the wind and the solar energy world, where novel insurance policies have been created in the past 10 years to support those technologies," he says.

Adaptation is where most people's focus lies, says Scott. Protecting large urban areas through more secure flood defences and better management of water as a resource, are two examples among many.

However, management of water – be it too much through flooding or too little through drought – is complex. It involves many stakeholders, ranging from landowners and farmers to planners, water companies, government regulators, industrial users and private consumers. This is also an area in which the insurance industry has abundant risk management insight.

CV

- Graduated in geology at Oxford University; also has a PhD in sedimentology from Aberystwyth University
- Gained commercial experience in the chemicals industry with BOC
- 2001: senior vice-president of Zurich Strategic Risk
- 2007: became Zurich's head of risk insight
- 2009: promoted to chief risk officer, Zurich Global Corporate, leading global and local implementation of the enterprise risk management strategy
- 2010: joined the CCS Development Forum, an industry and government group working to maximise business opportunities to deploy carbon capture and storage in the UK
- Chairs the Carbon Capture and Storage Association group on risk and is on the stakeholder dialogue board of the ECO2, an EC project to investigate the effect on marine ecosystems of sub-seabed CO_2 storage

Insurance experts can provide sound advice to customers and governments on the best approaches to manage flood risk.

If climate change progresses to the point where nations feel they are being economically or environmentally damaged, they may be encouraged unilaterally to use geoengineering to protect their populations, potentially leading to the risk of rogue geoengineering. This is already happening as some nations use techniques such as cloud seeding to encourage and divert rainfall away from flood-prone areas. The consequences can be dramatic for neighbouring nations, which might suffer drought when seasonal rainfall fails or unexpected flooding.

> 'If it is against the law to do something – build a house on a floodplain, say – that is a powerful signal'

More serious attempts to adapt to climate change may include creating geostationary sunshades in low-orbit space above nations to reduce temperature or injecting microparticles into the atmosphere to create clouds and shade. All of which have unpredictable and potential harmful effects on the climate and environment.

Behavioural change is another important area to manage. Climate change is a global risk to which everyone has contributed over many generations, emitting GHGs as nations since the industrial revolution. "Every time a person gets into a car, every time an electric device is used that requires fossil fuel to be burnt to generate that power, people rarely think about the consequences of their actions."

The failure of global governance mechanisms to create controls on GHG emissions has encouraged some people to take political or legal approaches to enforce change. In some jurisdictions, attempts have even been made to assign legal liability for climate change to industrial organisations, in particular in the power generation, oil and gas and mining industries. However, despite several court cases, legal action has not been successful and is probably neither an effective nor long-lasting solution to behavioural change.

"Pricing as a mechanism to influence behaviour is important," says Scott. "It is something that the insurance industry can use to show to the outside world the level of risk associated with an activity by the way that risk is priced."

Scott concedes that sometimes pricing alone is not sufficient and that regulation or legislation are the only effective way to drive meaningful change.

"If it is against the law to do something – to build a house on a floodplain, for example – then that is a powerful signal," he says. "People just won't do that if they face jail or a huge fine."

Mitigation, adaptation and behavioural change are all important approaches that need to be developed together, not individually, to bring about change.

"It sounds simple to boil it down to three approaches, but of course there are so many different pressures on all the actors that it is very complex," he says. "If it were that simple, this problem would have been fixed a long time ago." **Mike Jones**

REACHING TIPPING POINT

The effect of greenhouse gases (GHGs) on climate change is influenced by many factors over time, but one important aspect is the many different ways in which the earth manages the carbon cycle.

There are multiple sinks and stores for carbon, most of which act in a slow, gradual way to exchange GHGs in and out of the atmosphere. However, some carbon stores can release GHGs in a much more sudden way. Scott identifies methane hydrates as one potential trigger for rapid GHG emission and acceleration of climate change.

Methane hydrates form in the sediment of the deep ocean floors when plankton and other marine biomass settle on the sea floor. The decaying process of organic matter produces methane, which becomes trapped in top layers of sediment in a frozen crystalline form of methane – methane hydrate – because of the cold temperatures on the deep ocean floors. Temperatures at this depth were once considered to be universally constant but are now known to be rising.

"It would not take much for the ocean floor to warm up sufficiently for methane hydrates to be released as methane and that is a very different trigger," Scott says. "The release of methane hydrates would dramatically increase the GHG effect because methane is a much more powerful greenhouse gas agent than carbon dioxide.

"The fear with climate change is not that it is gradual and steady, but that it will trigger one of these mechanisms to release a lot of additional GHGs from some previously unreleased carbon stores. That would have a dramatic effect on climate. This is similar to the disaster movie scenario where a very rapid change in climate would take place, but it is also something that is real. The implications of this would be to make life very difficult for human beings on the planet – not only in certain regions but perhaps everywhere." It is this scenario of runaway climate change that most concerns climate scientists, not merely the gradual effects of a slowly warming world.

SURVEY RESULTS

Insurers and brokers often provide exceptional service but can be inconsistent. Furthermore, the insurance industry is failing to evolve as quickly as large corporations and faces becoming irrelevant

How corporate insurance buyers rate insurers and brokers

MAJOR INSURERS AND BROKERS are failing to keep up with the rapidly changing demands and expectations of the UK's largest corporate businesses.

That is the key finding of *The UK Corporate Insurance Buyers' Survey* 2015, produced by *StrategicRISK* and aimed at leading risk professionals.

Research was undertaken in the fourth quarter of 2014 among a cross-section of *StrategicRISK*'s UK readership of corporate risk managers and insurance buyers representing FTSE 250 companies or those of a similar size in the private sector.

Although they remain solid on traditional industry basics, insurance and broking firms need to evolve significantly to maintain relevance for corporate clients.

From a perceived lack of innovation to concerns around understanding fully the constantly shifting nature of globalised commercial requirements, the service provided often falls short of what is or will soon be needed by insurance buyers and risk managers.

Failing to keep pace

Many insurers and brokers provide exceptional service to clients, but it is often patchy or sector-specific.

One respondent said: "Some insurers are delivering what we need with some products, but if [the question was whether] insurers delivered across the board, then the answer is 'no'... Insurers are failing to keep pace with the complexities of large multinational organisations in terms of understanding our needs and, for some, their ability to deliver anything that is of value aligned to those needs."

Survey respondents were able to talk freely and frankly in exchange for anonymity – and they did. Claims was one area that elicited some particularly strong responses.

"Certainty of payment is absolute when it comes to claims," said one respondent. Another, citing a previous bad experience, said their company judged insurance partners "in terms of claims settlement, attention to detail and flexibility".

Claims battleground

Problems with claims were potentially fatal for the insurance partnership. For example, one insurer was lambasted for turning claims into a "battleground" because they "lost the plot" in terms of who was dealing with the claims. Ultimately, this insurance buyer terminated the relationship.

On brokers, many respondents were critical of the changing nature of the market, with one suggesting that the broking industry had "cannibalised itself", limiting choice for customers in the process.

Clearly, although the needs of every individual business are unique and depend on a range of often different factors, some overall conclusions can still be drawn in respect of the state of the UK insurance and broking industry in relation to large corporate clients.

It's not all bad...

With risk managers and insurance buyers able to speak anonymously, many took a tough line on what they thought was needed in the changing market, particularly during the longer supplementary interviews conducted with respondents.

As a result, although criticism is extensive, broadly speaking the results still indicate most insurers continue to provide a viable and valued service for corporate clients.

Seven of the largest insurance companies featured in the survey scored more than 4.00 out of 5.00 in terms of overall general service, which indicates an appreciation of insurer performance among risk managers and insurance buyers.

Bespoke solutions

Look beyond the top line, however, and there are inconsistencies across the board, with no single insurer getting close to service perfection, with the exception of FM Global for its specialist offering.

Many respondents cited irritation at being offered "products" rather than "bespoke solutions" to their unique business situations.

Not all insurers are culpable, but the entire industry has some way to go to rectify this, particularly around more complicated and technological issues such as cyber.

Meanwhile, the broker space has undergone substantial change in the past decade on several levels, with a greater emphasis on risk consulting and other services.

Yet, corporate clients tend to dismiss many such service offerings. Innovation and tools for better understanding risk was the only area of broker operations that respondents consistently rated below 4.00, scoring 3.92.

This indicates that appetite is limited for some broker services, with several respondents calling them "irrelevant".

One respondent said that being proactive should not mean "the broker trying to upsell things... They do too much of that".

Another said: "Brokers are generally very good at doing what you ask them to and not necessarily what you need."

Indeed, overemphasis on non-specific sales is also criticised, with one interviewee

'Brokers are generally very good at doing what you ask them to and not necessarily what you need'

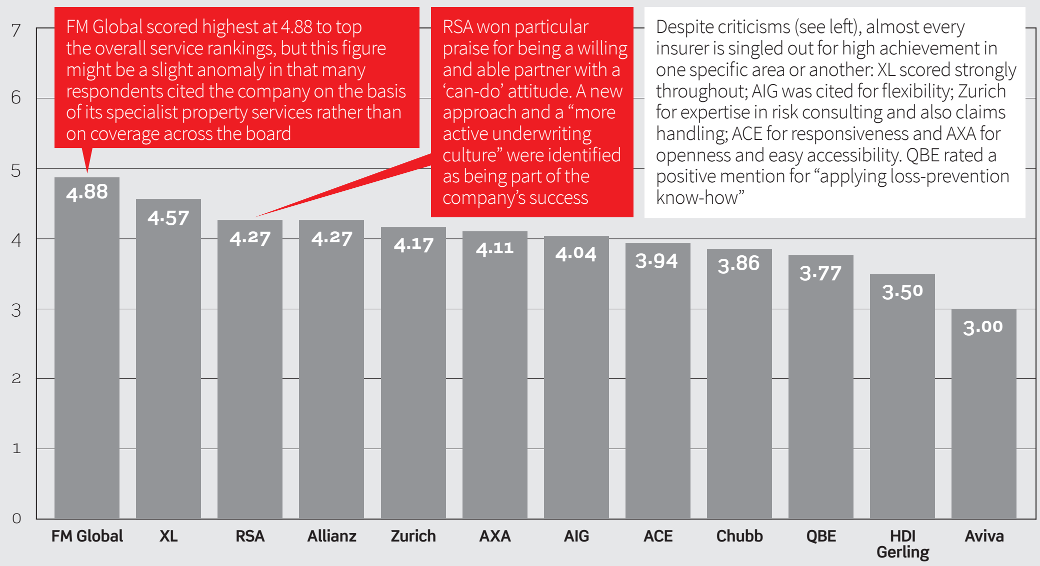
Survey respondent

HOW INSURERS AND BROKERS RATED

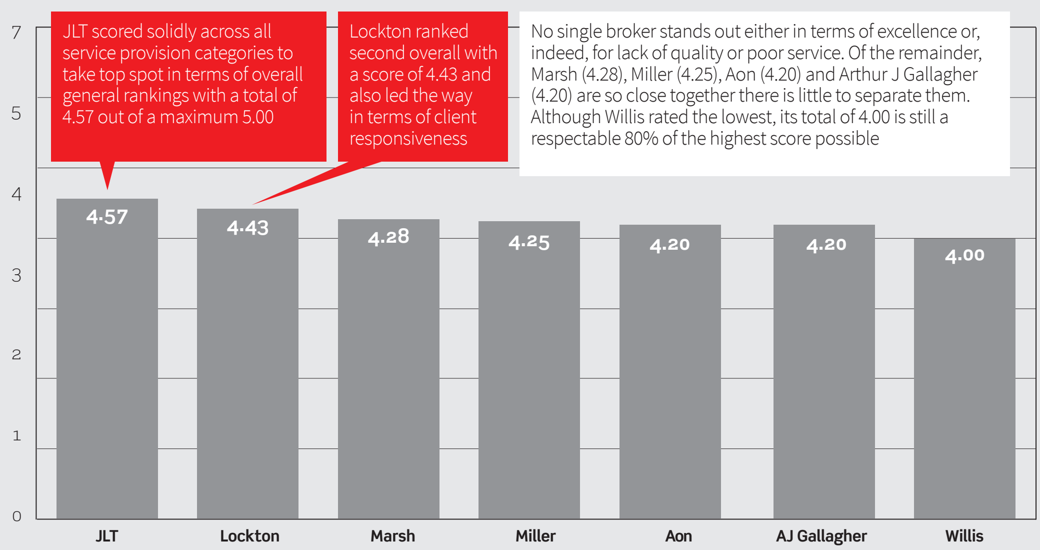
OVERALL SERVICE SCORES FOR INSURERS AND BROKERS IN THE *UK CORPORATE INSURANCE BUYERS' SURVEY* 2015

Source: *StrategicRISK UK Corporate Insurance Buyers' Survey* 2015

INSURERS



BROKERS



imploring brokers to ensure "service does not come a poor second to selling products".

Less choice

Against this background of diversification in terms of providing new services, the broker dynamic has also shifted, with two major players, Aon and Arthur J Gallagher, growing rapidly through acquisition.

Although this has boosted the big firms' market share, it leaves large corporates with "less choice" and "less recourse to alternatives and innovation", one insurance buyer said.

Others argue many brokers have become detached from customers because of their size and bemoan that by trying to be "all things to everyone" they end up providing little of genuine or meaningful value.

Yet, although large brokers continue to grow, it is the people working within them that matter most to those surveyed.

One insurance buyer said of their broker: "There are some very credible individuals working there, so much so that these people are now engaged in dealing with our senior management, who are far higher up in the organisation than I am, and this is excellent." **SR**

To purchase copies of The UK Corporate Insurance Buyers' Survey 2015, contact Tom Byford: tom.byford@nqsm.com or 020 7618 3081

WHAT CORPORATE INSURANCE BUYERS WANT FROM INSURERS

- **Long-term partnership** but, as one commented: "We have to constantly remind [insurers] that our relationship is not something that should be taken for granted"
- **Recognition of good risk management and corporate governance** "reflected in the pricing of my risks"
- **Not invoking or 'hiding behind' reservation of rights** "I am not interested in an insurer that will invoke an automatic reservation of rights"
- **Continuity** "We changed a key insurer, primarily because of changes in personnel"
- **Flexibility** "Too many insurers still operate in silos such as cyber"
- **Time to be creative** "We are not looking for off-the-shelf products but bespoke solutions and that does not happen overnight"

WHAT CORPORATE INSURANCE BUYERS WANT FROM BROKERS

- **More choice** "Unless you want to be particularly adventurous, you are left with a choice of three or even two brokers and that is not a healthy situation"
- **More expertise** "[There has been] a reduction in the technical approach among larger brokers"
- **Openness** "It must be an open relationship and very much a tripartite one. We need to be one team"
- **Fee transparency** "It would concern me more that I did not know, rather than the actual details of who receives what"

SR AT 100

In 15 extraordinary years, *StrategicRISK* has captured the zeitgeist and reinvented itself as an award-winning global brand, but the best is yet to come…

OVER LUNCH AT A LONDON SUSHI BAR IN 2000, David Gable, who was then the chief executive of Airmic, and insurance writer Lee Coppack conceived a plan for a new publication and website for risk managers.

This idea emerged after the publication of several governance guidelines in the late 1990s. These aimed to tackle significant flaws in internal corporate governance following scandals such as the one surrounding Robert Maxwell, the notorious media tycoon who plundered more than £400m (€542m) from his Mirror Group employees' pension funds to shore up his companies.

During the lead up to *SR*'s inception, a harsh spotlight was shone on UK corporate governance and internal controls. Governance guides such as *Cadbury* (1992), *Greenbury* (1995) and *Hampel* (1998) set out to address corporate governance failures. Then, in 1999, the Turnbull report was published, detailing recommendations on best practice in internal control for UK-listed companies. Although recognising the importance of risk management, the guidance placed a greater obligation on risk professionals to improve audit controls and risk prevention – a factor that prompted Gable and Coppack's idea to create a publication that would inform on and analyse such developments.

With the backing of publisher Southern Magazines (now Newsquest Specialist Media), *SR* was launched in June 2000 at the Airmic conference in Birmingham.

Early days

Sue Copeman was the first editor. With more than 20 years of experience in insurance writing, including at the *Financial Times*, first as an in-house editor of *World Insurance Report*, then as a freelance consultant editor on the *FT*'s insurance newsletters and author of several *FT* management reports, she was the perfect choice. Despite her insurance writing background, Copeman was "determined that *SR* take a broader view of risk".

As she wrote in a 2010 edition of the magazine: "I like to think that *SR* has always looked holistically at risk, covering insurance where appropriate but relating it to the far wider concerns of many risk managers, who view insurance as just one of the instruments in their toolbox.

"With the huge focus on risks that has occurred in the past 10 years [since the launch of *SR*], I believe that we launched at a very opportune time."

SR TIMELINE

2000

June: *StrategicRISK* is launched as a quarterly publication for UK risk managers at the Airmic conference in Birmingham

The first *SR* roundtable discussions are held to promote sharing of best practice among risk managers

2001

2002

January: *SR* goes bi-monthly
December: *SR* publishes its first special report – on directors' liability

2003

June: *SR* produces daily newsletters for the Airmic conference – and has been the conference's official daily ever since
August: following the spread of SARS, *SR*'s special report deals with 'Epidemic – the impact of disease'
October: *SR* goes truly European – exhibiting at the FERMA forum in Rome and producing a daily forum newsletter

Starting out as an information brand for UK corporate risk managers and insurance buyers, it soon became clear that the magazine and website would play a useful role in interpreting the effect that European regulations would have on businesses.

In October 2003, *SR* took on a wider remit, expanding its reach from the UK to other European countries. For the first time, it appeared at a non-UK conference, the FERMA forum in Rome. It also published a daily conference newsletter, covering all the news and comments from the event.

Nowadays, *SR* has grown its European presence, reporting on key markets such as France, Germany, Spain and Belgium. More recently, it turned its attention to Central and Eastern Europe as risk management practices develop there.

Growth has not only been geographical. Since 2000, *SR* has expanded its range of events, special reports and supplements. In 2001, the brand hosted its first roundtable discussion, bringing together senior risk managers to London to promote and share best practice. Others followed – risk-specific roundtables, country-focused roundtables and the presidents' roundtable, where leaders of risk management associations came together to discuss latest trends and developments – all of which spawned several reports and guides.

In time, larger half- and full-day conferences were organised.

Going global

More recently, *SR* has taken its business model further afield, launching in Asia-Pacific in 2013. Starting as an online news service, *SR* in Asia is now a multiplatform information brand with a quarterly magazine and a series of events that reach risk managers from China through to Thailand, Singapore, Indonesia and Australia. Only two years after its launch, *SR Asia* was recognised by the Institute of Risk Management, which awarded the brand the Risk Management Journalism Award – an accolade that, as one reader remarked, not only recognises *SR*'s "comprehensive coverage of risk management-related issues", but also its achievement in helping "to connect the risk managers in this region like never before".

Looking to the future

After 15 years and 100 magazines, the *SR* team has no intention of stopping. Indeed, following its success in Asia-Pacific, in April *SR* is launching in the Middle East with events, including an inaugural Middle East and Africa Risk and Insurance Awards, held in conjunction with sister title *GR*.

Plans for an online news service, aimed at insurance and risk managers, will be announced at a risk and (re)insurance event at the Four Seasons, Jumeirah beach, Dubai, on 20 April.

Not bad for a magazine thought up in a sushi bar. **SR**

2004

SR launches its European risk management awards event
April: *SR* holds its first European presidents' roundtable for leaders of the European risk management associations

2005

January: *SR* produces a daily newsletter in French for the **AMRAE conference** – and has continued to do so every year

2006

PPA, the UK association of magazines and business media, names *SR* International Business and Professional Magazine of the Year

2007

SR holds its first conference on 'Risk and opportunity – tomorrow's boardroom challenges'

2008

For the first time, *SR*'s European Risk Management Awards are held in Paris. The following year, they are held in Berlin

2009

March: *SR* launches the first of its ongoing series of standalone guides and reports on major risk topics

A profession in progression

In the past 15 years, risk management has undergone a period of significant adaptation, but the profession is still striving for more board engagement

SINCE *STRATEGICRISK* LAUNCHED in 2000, the corporate risk landscape has transformed and expanded considerably, especially thanks to the advent of digital technology and globalisation.

The rapid and unrelenting pace of change during this time has subsequently raised the profile of risk as firms have become more global in their operations and, therefore, more exposed to risks.

The nature of risk has also diversified, with intangible risks, such as cyber and reputational damage, emerging as major threats to businesses. This period of change has had a significant effect on the risk management profession in terms of its shape and position within corporate strategy.

Moreover, a number of global events in the past 15 years have had major consequences for risk professionals, including: the Enron and WorldCom corporate accounting scandals in 2001-02, the 9/11 terrorist attacks, the 2008 financial crash and an unusually high number of high-impact natural disasters, including Hurricane Katrina in 2005 and the 2011 Tohoku earthquake and tsunami in Japan.

Heightened awareness

These events, among many others, and the advent of digital technology have led to a general heightened awareness of risk, according to International Federation of Risk and Insurance Management Associations (IFRIMA) chair and chief risk officer at Katoen Natie Carl Leeman. However, Leeman says the risk management community can do much more to improve its perceived value to corporate strategy.

"At most firms, an increased awareness of risk has not led to a sufficient improvement in the profile of risk management," he says.

Leeman is concerned the profession lacks the appeal needed to attract young talent and believes the risk management community has missed opportunities to promote its value at board level. Perhaps part of the difficulty that risk professionals have encountered in communicating with the board is the lack of a universally accepted definition of risk management.

Airmic chief executive John Hurrell says that, 20 years ago, the profession was amorphous and it was therefore difficult to promote its strategic value. Moreover, he believes the risk management function has undergone a significant transition at many firms in recent years.

SR TIMELINE

2010

SR produces French and German language reports focused on key risks for corporates

2011

SR launches SR100 – a forum for senior risk managers at FTSE-listed or multinational programmes – at its inaugural Risk Retreat event in the UK

2012

SR sets up operations in Asia-Pacific

2013

SR launches in Asia-Pacific as an online news service and magazine and begins hosting a series of roundtables around the region

"One of the biggest trends in the past 15 years has been to move from a centralised risk team to an integrated model," he says, before adding that the most dynamic firms maintain a central risk team to scan the risk landscape for emerging threats in a consultancy-like operation.

Such central risk teams comprise a "tapestry of professions" under the risk management umbrella, says Airmic board member and InterContinental Hotels Group (IHG) senior vice-president risk management John Ludlow.

Ludlow says his team at IHG exemplify the diversity of skills and specialist roles in a modern risk management team, such as ERM, risk financing, business continuity, safety, security and project risk.

"My team finds working together incredibly valuable. Together, [it is easier to] have one voice and being a coherent force within the company gives more power," Ludlow says.

Leaders required

Ludlow, Hurrell and Leeman agree that for the profession to increase its influence at board level and inform corporate strategy, future risk managers must have the leadership qualities needed to manage larger teams and handle the corporate politics that inevitably comes with seniority.

FERMA president Julia Graham is confident that risk management will adapt to the volatile global risk landscape and prove its value to business strategy.

"Managing risk will increasingly be embedded in the development and execution of strategy. As the world in which risk management is practised evolves, so too will the risk management profession and risk managers will become risk leaders, an integral part of organisational governance," she says.

The professional development of risk management is building momentum. FERMA and the IRM are each expected to launch a certification programme for risk professionals this year; meanwhile IFRIMA is leading an initiative to align global standards for training and education in risk management.

Establishing standards of practice through certification is widely considered a move in the right direction for risk management. Although there have been similar initiatives before, Leeman says that they were not approached on such a co-ordinated level as the current ones.

Maybe the community has been spurred by the global consequences of several unexpected events in the past 15 years, which have increasingly put the profession under the spotlight. Perhaps when *StrategicRISK* celebrates its 30-year anniversary the initiatives of FERMA, IFRIMA and IRM will be viewed as the springboard that helped establish risk management as a key component of corporate strategy. **Asa Gibson**

> 'Managing risk will increasingly be embedded in the development and execution of strategy'
>
> **Julia Graham,** FERMA

2014

SR launches sector-specific events for senior risk managers working in the financial institutions and construction industries

SR Asia hosts its first one-day conference in Singapore, bringing together 150 risk professionals and specialist brokers to share best practice

2015

February: *SR* Asia wins the Institute of Risk Management's Risk Management Journalism Award

SR starts an online news service in the Middle East and North Africa and launches its inaugural risk and insurance awards, held in conjunction with sister title *GR*

Focus

MIDDLE EAST

READY AND ABLE

Security concerns and tumbling oil prices are setting the agenda across the region

BUSINESS IS BOOMING ACROSS THE MENA region, driven by major growth in the United Arab Emirates (UAE) and Saudi Arabia. Oil and gas exports built the economies of the Gulf States, but it seems they will also underpin their post-hydrocarbon future.

To date, the region has been an exemplar of how to diversify. A total of 71% of the UAE's GDP now comes from non-oil sectors, with growth averaging 4.66% from 2000 to 2013. However, oil and gas exports still remain critical and a risk arises that when prices fall, as they are doing now, growth and GDP could follow.

"Although a short-term reduction is unlikely to have a significant effect on economic growth, the possibility of a sustained reduction in pricing levels could affect confidence. Some of the planned infrastructure and development spending could be postponed or curtailed, which could slow economic growth," says Paul Holmes, managing director, Middle East, Al-Futtaim Willis.

The 2015 Aon *Political Risk Map* singles out Iran, Iraq and Libya as being at heightened political risk as a result of tumbling prices and an over-reliance on exports.

So far, the large financial reserves of the Gulf States are providing an effective buffer. According to research by KCS Strategic Intelligence and Corporate Security, Saudi Arabia has currency reserves of $750bn (€707bn), allowing it to ride out the current falling oil prices without markedly cutting spending. Its economy is set to boom in the short to medium term. Riyadh is creating new economic zones and planning to open its domestic stock exchange to outside institutional investors for the first time later this spring.

Despite this national resilience, evidence shows that falling prices may still be acting as a spur to the development of better risk management, at least at the corporate level.

Speaking anonymously, one chief risk officer told *StrategicRISK*: "The oil price is certainly making organisations more fiscally prudent. They are realising that there is no bottomless money pit and that they need to demonstrate to their stakeholders how they are spending their income."

Correcting this vulnerability to price shocks has been a key focus of strategic planning for some time across the region. However, developing local economies beyond their dependence on oil exports requires more reciprocal links with the West, which brings with it a new level of scrutiny and risk.

As the UK and US extend their legal reach in an attempt to clamp down on corruption, companies in the MENA region face new issues relating to corporate governance and compliance.

"This can prove to be challenging, particularly in terms of the application of extra-territorial legislation, such as the US's FATCA [Foreign Account Tax Compliance Act] and FCPA [Foreign Corrupt Practices Act]," says law firm K&L Gates partner Natalie R Boyd.

As a result, reputational risk is increasing proportionately as countries in the region reposition themselves on the world stage. "The responses are new regulations and controls, which demonstrate the appetite for risk reduction," says Boyd.

"In addition, people and companies in the Gulf Co-operation Council are much more connected than in other markets. This presents challenges and risks associated with doing business with related entities. Due diligence builds on existing trust. Deal structures unfamiliar to insurers need detail and assurances to overcome their reluctance to provide cover."

Pace and scale of change

The regional boom is also bringing with it other challenges as the sheer scale and pace of development become a catalyst for risk. Increasing globalisation exposes the lack of a skilled indigenous work force, limited corporate governance, low awareness of cyber security and poor investor protection.

"In particular, I worry about the leadership pipeline," a senior risk manager told *SR*. "I'm not convinced organisations are bringing the future leaders through. I don't believe organisations [here] are good at succession planning and developing their employees. From a long-term perspective, this will work against them.

"For many people working in the region, they are sitting in the best job they will ever have, and so they don't want to do anything to change that. They become 'yes men'; they accept things the way they are, and thus there is a real risk firms cannot change and adapt."

Philip Wood, insurance senior manager at the Qatari Diar Real Estate Investment Company, says: "Obtaining the right people and materials at the right time is becoming increasingly difficult. Similarly, there are significant integration risks involved in managing multiple complex developments."

Beyond the boardroom, some other significant strategic risks cannot be ignored. Conflict and terrorism are serious concerns in some markets, and the heightened volatility and unpredictability in evidence since the Arab Spring began in 2010 means companies need to be much more aware of political risk.

> 'The oil price is making organisations prudent. They are realising that there is no bottomless money pit'

"Businesses need to know who they are dealing with and who is pulling the levers of power," says Paddy Lord, managing director at Control Risks. "There have been some dramatic reversals of policy in recent years, particularly in the major engineering sectors, such as oil and gas, where the government of the day tends to make its presence felt quickly."

Businesses are aware that understanding how the political tides are moving is essential if they are to avoid seeing their hard-earned reputation disintegrate.

"Businesses should know who they are dealing with and how this could affect their reputation," says Lord. "We don't necessarily need to be talking about war zones here. Even in places such as Saudi Arabia and other Gulf States, firms need to understand who their partners are and what exposure they have to business and politics as a whole."

It is also crucial to remember that a fast-changing political situation can make a location dangerous. Two major evacuations of foreign expatriates have already taken place in Libya since 2011 and a third is under way. Businesses need to be able to get their people out fast if necessary. "Places such as Iraq, Libya and Yemen are experiencing serious security situations," says Lord.

From the battlefields of Syria and Iraq to the everyday challenges of operating in an increasingly globalised world of low oil prices, the MENA region faces significant risks. For those able to take on these challenges, the opportunity is there to be part of the growth in one of the world's most dynamic regions. **SR**

TUNISIA: A BEACON OF HOPE NOW FACING TROUBLE

Tunisia was named 'Country of the Year' by *The Economist* in 2014 as it adopted a more enlightened constitution and celebrated successful parliamentary and presidential polls. However, the recent attack at the Bardo museum in Tunis, which killed 21 people and injured another 50, brutally demonstrated that a peaceful future is far from secure.

Many believe the Arab Spring began in 2010 when a Tunisian street vendor called Mohamed Bouazizi set himself on fire in protest at the confiscation of his wares and his humiliation by a municipal official. His suicide would send ripples across the region and cause the Tunisian government to fall. However, real incomes have remained stagnant since then and attracting foreign investors is a major challenge.

"The most significant risk to business stems from the threat of growing extremism," says Philip Stack, principal MENA analyst at Verisk Maplecroft. "The elections confirmed that there are really two Tunisias: the relatively affluent urban coastal region, which supported secular parties, and the rural interior, which predominantly voted for the Islamist Ennahda party. The spillover of extremism, especially from Libya but also from Algeria, could take root... [That] would affect Tunisia's economic development and could lead to a more authoritarian form of government.

"Although the country is taking well-judged measures to prevent this risk developing, many of the drivers of extremism are outside the government's immediate control."

RISK MANAGEMENT, THE NEW DISCIPLINE

The financial crisis has made MENA businesses aware of the need for serious governance and risk management strategies

RISK MANAGEMENT IS DEVELOPING RAPIDLY as a serious discipline and businesses in the MENA region are moving fast to embrace global standards.

Neal R Brendel, partner at law firm K&L Gates says: "Until recently, there was a sense that firms here were aware that it was important to pay lip service to the ideals of corporate governance but that there was very little actual infrastructure, such as codes of governance or even dedicated risk managers, to implement these aspirations.

"In the years since the financial crash, this area has been receiving much more serious attention. This was particularly obvious when the situation was difficult, and the big cash flows that had obscured some elements of bad practice were drying up."

Speaking anonymously, one chief risk officer said: "Eight years ago, risk management was in its infancy. However, organisations have developed this a lot in the intervening period, even if problems still remain with board charters and board training and few organisations have proper business continuity. They may have a crisis management strategy, but in terms of how they recover afterwards they have little to go on."

One of the main factors driving an increased awareness of risk management is that much of the region's economic diversification has involved partnerships with US or European brands. When western companies come into the region, they require a certain level of risk management from the companies with which they deal.

"There is a building pressure on companies that want to partner with western brands that they will have to develop their approach to risk management," says Paddy Lord, managing director at Control Risks.

As a result, regional businesses are becoming more and more sophisticated. However, this is a process that takes time, as well as serious investment in people and training. "Companies need to invest in more sophisticated staff and give them the mandate necessary to make their presence felt," says Brendel.

"Businesses need to be talking to the kind of sophisticated brokers and risk advisers who can identify risks and suggest customised ways of addressing them."

One of the biggest obstacles to change is the widespread lack of transparency. It can be hard for firms to determine who they are dealing with – and crucially whether they would be deemed a 'government official' according to the US's Foreign Corrupt Practices Act (FCPA). "The US has expanded its jurisdiction in a lot of ways and this lack of transparency presents a real risk," says Brendel.

Lord agrees. "Awareness is growing about the UK Bribery Act 2010 and FCPA, but there is still some way to go," he says. "The level of litigation in the region is still low and companies usually prefer to reach a settlement before getting to court."

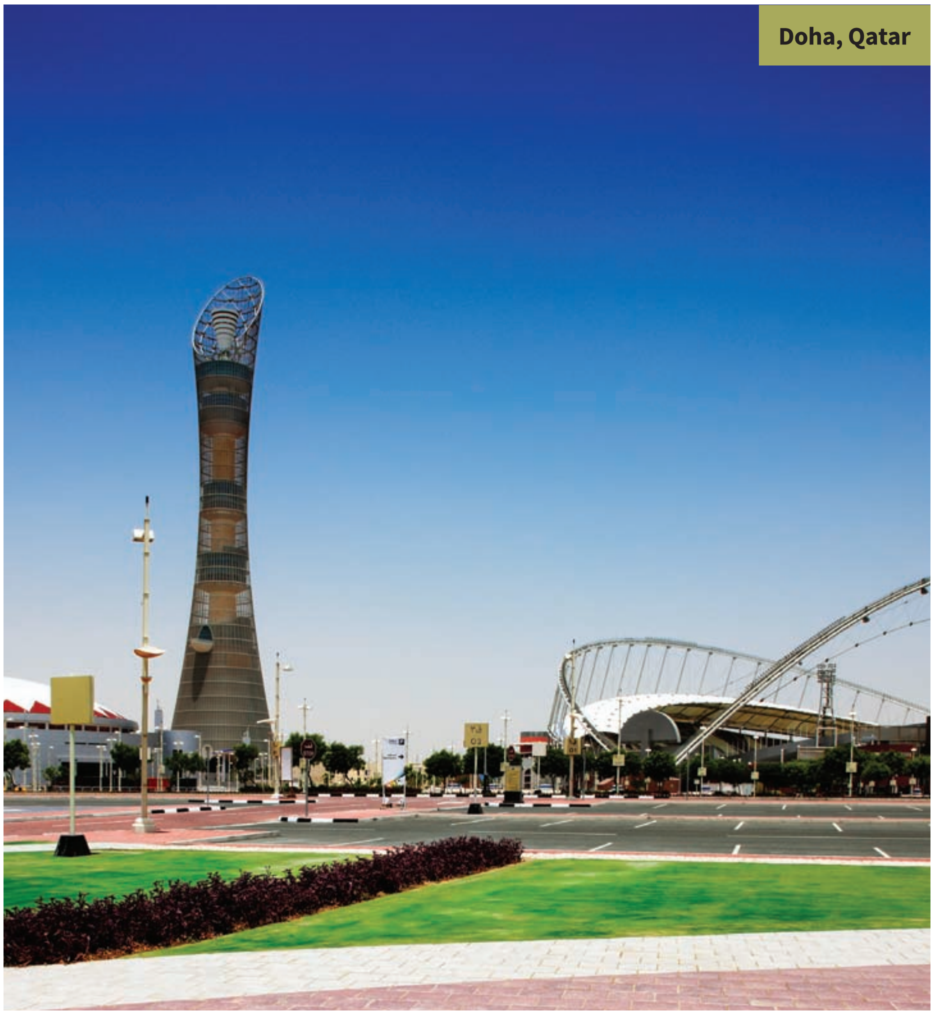
Low insurance penetration

Another major barrier to modern risk management standards is the relatively low penetration of insurance. Although the insurance market grew overall from \$20.4bn to \$44.1bn (€19bn-€41.5bn) between 2006 and 2012, penetration has remained flat at 1.5%. Most of the growth took place within the United Arab Emirates (UAE), Saudi Arabia and Qatar as a result of major infrastructure projects such as the Qatar World Cup and new universities in Saudi Arabia.

"Although the Middle East does have a much lower insurance penetration compared to most western countries, this continues to increase year on year and provides the insurance fraternity with a continued focus on expansion," says Paul Holmes, managing director, Middle East, for Al-Futtaim Willis.

"Low insurance penetration is partly explained owing to the measure against GDP, whereby a large proportion

Focus



Sophie James / Shutterstock

of GDP often relates to the petrochemical influence. Economic growth is not materially affected by a low insurance penetration."

There is at least one significant barrier to insurance penetration that is specific to the region: sharia law frowns on many aspects of profit-making financial services. There are signs that products complying with sharia law – known as takaful – which are structured so that risks and rewards are shared in a similar way to a co-operative or mutual, could deliver a breakthrough.

Growth has already been strong across life, non-life and medical cover. "In the UAE, Bahrain and Qatar, takaful companies that were start-ups a few years ago are becoming better established, and the challenge for them is to find ways of differentiating their products and finding new distribution channels," says Tony Saada, chief executive of UAE-based Lockton (MENA).

Takaful is a powerful reminder that risk management is not a one-way street and newcomers and investors could learn some lessons from regional firms.

"One of the ways that local family groups manage their exposure is by placing family members in different divisions of the company or even different territories to make sure that they retain an appropriate level of influence," says Lord. "In this region, much comes down to relationships and businesses have to work hard to maintain those relationships."

Some remarkable changes have taken place in the past few years and the direction of travel seems clear. The economic crisis has exposed shortcomings in risk management and provided a powerful incentive to handle things better.

Now that the business climate is improving, the challenge is to maintain that focus. **SR**

> 'In this region a lot comes down to relationships and businesses have to work hard to maintain those'
>
> Paddy Lord, Control Risks

COMPLIANCE CULTURE

The culture of corporate governance and risk management in the MENA region is very different to that of the US and Europe. "It is not unusual for companies not to have in-house compliance and risk management personnel or for the head of legal to assume the compliance role. This is a significant responsibility for the person allocated with such a dual role, particularly given the diversity of risk across the region," says Natalie R Boyd, partner at law firm K&L Gates.

"It can be difficult to explain to managers why and how their businesses are affected by extra-territorial legislation."

This is starting to change, she says. "Legislators and regulators recognise the need to provide for international best practice. Companies are beginning to acknowledge that they cannot ignore the risks, particularly in terms of breaching anti-money laundering laws and extra-territorial laws and sanctions, which represent significant risk for the business and the individuals involved," says Boyd.

For example, recently there has been a significant push in the United Arab Emirates to apply international best practice, such as corporate governance codes and binding and non-binding guidelines for regulated banks.

"Application of laws and regulations to government sector companies and individuals, however, is not always clear," says Boyd. "Confusion may arise as to who would fall within that sector and this can cause problems for firms operating within the territory."

There is no room for mistakes, however, and regulators in the region are becoming much more aggressive.

"A number of prominent financial institutions have been the subject of regulatory sanctions for failure to comply with corporate governance and compliance regulations," says Boyd.

"This is reflected in the growth of specialist risk management companies setting up in the region. It is often easier for local companies to outsource to experts than to build up their own internal capacity.

"The region is reacting to changes that are evolving in other parts of the world and laws and regulations relating to risk management issues, and they are developing accordingly."

LAYING THE FOUNDATIONS

In the booming Gulf states, risk managers are rare, but the problems of turbo-charged growth may offer the profession a way in

DEVELOPING MIDDLE EAST AND NORTH Africa (MENA) has made respectable economic progress, experiencing an average annual real growth rate of about 5% since the start of the millennium (lower than developing Asia's rate, but higher than Latin America's). This marks it out as an emerging market with attractive opportunities for business investment.

The Gulf Co-operation Council (GCC) (namely Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE)) in particular, has benefited enormously from oil and gas reserves and assets that have generated significant financial liquidity. In addition to being resource-rich, the region's population growth, forecast to increase by 30% in the next decade to 53 million people by 2020, has kick-started numerous construction projects, including new cities, transport links and healthcare facilities. More than 100 major projects are due to be completed by 2030, costing in excess of $1trn (€746bn).

The GCC is also entering an important phase of diversification. As oil and gas reserves are expected to diminish in years to come, its countries aim to reduce their dependence on the hydrocarbon sector and create employment opportunities by integrating economies with the global knowledge economy, encouraging entrepreneurship, attracting foreign investment, fostering innovation and ensuring access to finance for SMEs.

All these developments spell opportunities and challenges for risk managers. Although risk management as a practice lags behind the region's growth, it is gradually gaining momentum, according to three senior risk managers based in Qatar.

During a corporate risk management panel debate held at the ninth Multaqa Qatar reinsurance conference at the St Regis hotel in Doha, Qatar, the panellists – Gregory Irgin, director and group risk, legal and reinsurance at UrbaCon Trading and contracting; Philip Wood, insurance senior manager at Qatari Diar Real Estate Development Company; and Frédéric Desitter, director of enterprise risk management at Sidra Medical & Research Center – gave an overview of risk management in the GCC.

Wood started the debate with a clear account of maturity levels: "Risk management, as a practice, is relatively new to the region. Within the GCC and MENA, the focus is on laying the foundation of risk management. Once the fundamental blocks are in place, a more advanced framework can be implemented. Businesses and their employees are on a journey ; they are building risk awareness and, once this has been achieved, a more consistent and sophisticated risk management approach can be shaped."

The panel commented that project risk management – whereby risks are managed on a project-by-project basis – takes precedence over the holistic ERM framework.

Desitter said: "Risk management is viewed as a governance process and many companies want to implement the function – doing so is seen as best practice. The main objective for many companies in Qatar is to adopt similar governance principles and mechanisms as companies in Europe.

"However, the function is in its infancy, particularly processes such as ERM. Businesses here are more familiar with project risk management and safety risk management than with the ERM concept.

Focus

"Having said that, ERM has been successful in some companies. I have started to implement the framework and other organisations, particularly those in the energy and aviation sectors and semi-governmental organisations, have been doing the same."

Irgin added that although there has been an "upsurge in ERM and project risk management with encouraging success", challenges exist in terms of engaging executive management. "A risk framework may be designed to the point of excellence and sought to be implemented vertically and perhaps horizontally across an organisation, but challenges remain for those who must follow and report upwards on such models. Chief executives lack understanding of risk management and they therefore do not prioritise it. Their main focus is on revenue generation and profits," he said.

Talent and resource scarcity

The discussion moved on to the main risks affecting businesses in the GCC. Talent acquisition and resource scarcity, particularly for the construction sector, are two of the biggest challenges for the region.

GCC states rely heavily on expatriates. Indeed, in 2011, most people in the UAE and Qatar were foreigners (87% and 84% respectively, according to a study by the Kuwaiti-based think tank Diplomatic Centre).

With $1trn worth of construction projects, competition for skilled migrants and materials is fierce. "The scale and pace of developments within the GCC are a catalyst for risk," Wood said. "The region is undergoing so much development and there are many major construction projects, that the availability of resources is scarce and, on the ground, the increased interface risk must also be carefully managed to avoid potential delays/bottlenecks. Companies are competing for skilled staff and materials such as steel and cement."

Desitter added: "One way to improve talent retention is to offer attractive terms and conditions, but this can only go so far. Other limits make talent acquisition and retention ever more challenging.

"Take for instance, the numerous rail projects planned across the GCC – a metro network is being built in Doha and an even larger network in Riyadh, Saudi Arabia.

"There are limits in terms of the pool of skilled workers who have the knowledge, skills and experience to do the job across the world. Then, there are limits in terms of the number of skilled staff willing to leave their home town and set up base in a foreign country in order to take the job. So, businesses are competing for a limited pool of talent."

He added: "The lack of materials is likely to affect the completion date of these projects. It may be the case that some companies would need to reconsider their plans and schedules if they are unable to get supplies into the country on time."

Emerging and intangible risks – particularly cyber risks – are also attracting the interest of risk managers. Cyber crime was cited as the second-most reported type of economic crime in the region, behind asset misappropriation, according to a 2014 report by PwC.

The report, surveying 230 organisations in nine Arabic countries, found that 37% of organisations that reported economic crime had been victims of cyber crime in the previous 24 months. Such attacks were most common in financial services and were particularly prominent in the UAE, Oman and Lebanon in 2012 and 2013.

Delegates at the ninth Multaqa Qatar reinsurance conference at the St Regis hotel in Doha, Qatar

Governments are taking action: the UAE has enacted the Cyber Crimes Law 2012 and Saudi Arabia has drawn up the Arab Cybercrime Agreement 2012. However, risk managers are still struggling to engage chief executives.

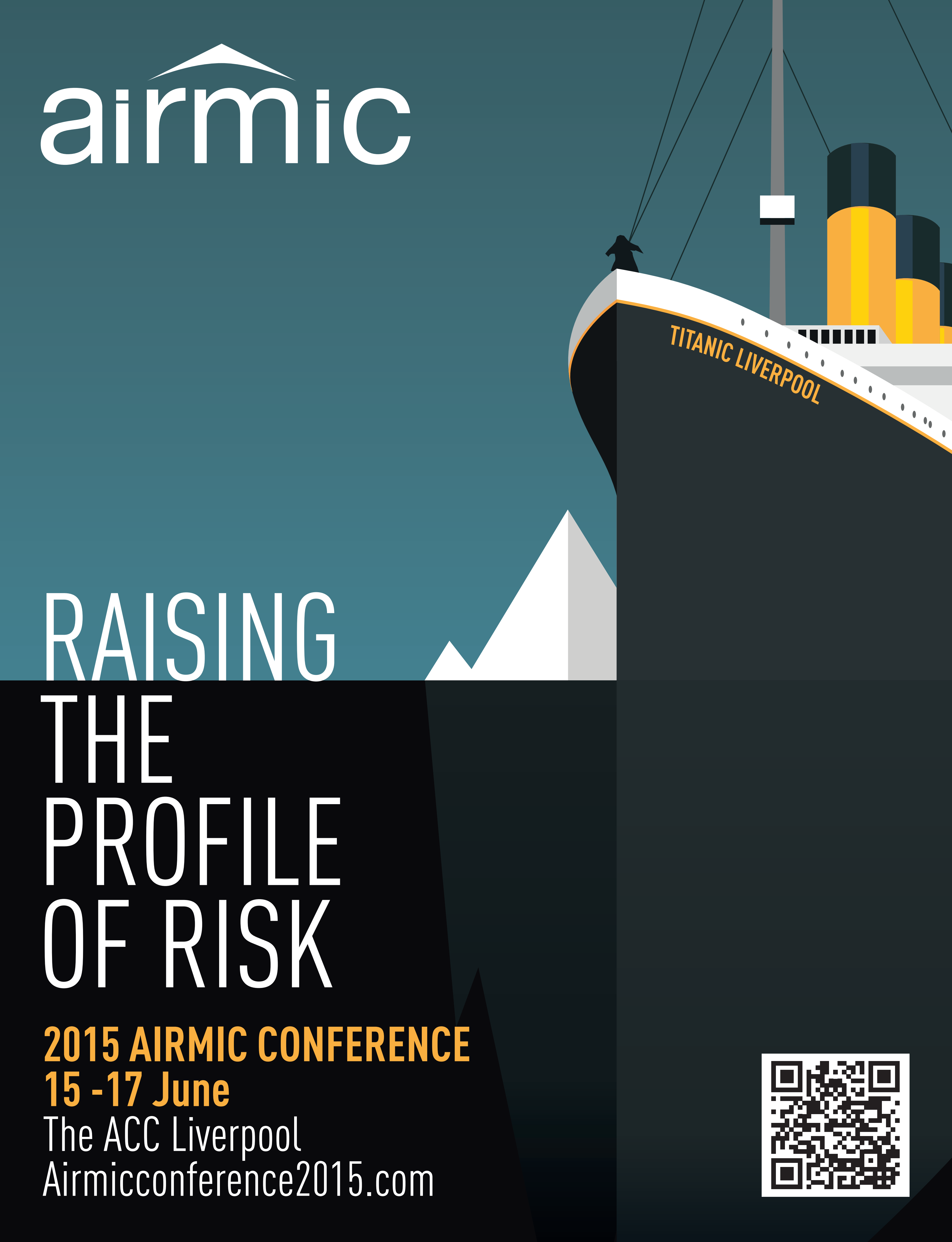
"Cyber insurance remains a hot topic and there is a definite lack of understanding within the corporations I have liaised with as to why they need [insurance] and how it could affect their business in a tangible way," Irgin said.

"The challenge for businesses is how to translate the benefit of insurance to chief executives, chief information officers and chief finance officers, who all have differing levels of understanding. Some of these executives have no comprehension of why insurance is required and some have a false perception of how secure their business and IT systems are.

"In plain English, cyber threat is real and it is being ignored at one's peril. If it were to be compared to monetary terms and ignored, the executive committee that respond with such inaction would surely be dismissed swiftly."

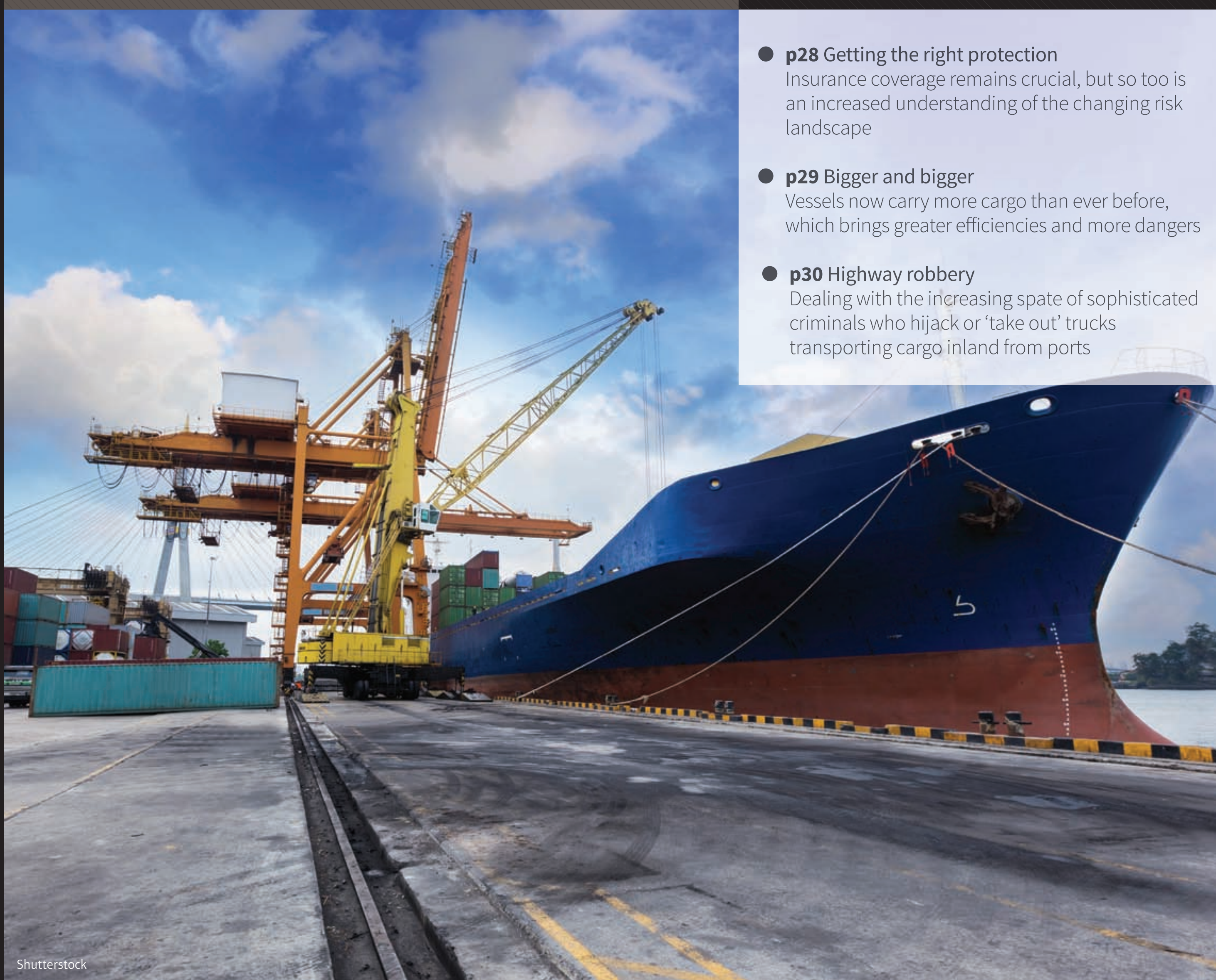
Reputational risk and political instability in neighbouring countries were two more risks that the panel discussed. Both risks were identified as having the potential to interrupt business, exposing them to expensive losses.

Nonetheless, the panel concluded on an optimistic note. Although risk management is less mature than in Europe, the US and parts of Asia, risk appetite is healthy. As Wood said when he opened the debate: "Businesses and their employees are on a journey." That begins with the basic building blocks of risk awareness, risk culture and risk management. **Kin Ly**


airmic
TITANIC LIVERPOOL
RAISING
THE
PROFILE
OF RISK
2015 AIRMIC CONFERENCE
15 -17 June
The ACC Liverpool
Airmicconference2015.com

SPECIAL REPORT

MARINE TRANSPORTATION



Shutterstock

Marine transportation

GETTING THE RIGHT COVER

The risks of not having an international programme

THE SCALE OF THE marine sector is truly huge. Ninety percent the world's trade is carried by shipping and almost everything that is bought and sold passes through ports in 12m containers.

In 2011, 360 US commercial ports took in international goods worth $1.73trn (€1,63trn), which amounts to 80 times the total value of all US trade in 1960. The UK shipping industry employs almost 635,000 people.

However, the sea will always remain a risky place. Globalisation is taking businesses to new markets presenting new risks, and larger and larger vessels are creating more complex exposures, making the right insurance choices ever more essential for large and small firms.

INSURANCE: KEY POINTS

1. Get cover from a global provider with the right local presence or partners who know the detail
2. Find an insurer that can help with on-the-ground risk management advice
3. Cost is not everything: focus on a good relationship that will last
4. Work with your suppliers and partners to stress test your operations from top to bottom
5. Keep your broker and insurer informed about operations and expect the same level of detail in return

ALL RISK MANAGERS NEED to consider the reach of their insurer, depending on where they ship from and to and on where they manufacture. "Your insurer needs to have the breadth to cover you," says Daniel Desjardins, senior director, global risk management and insurance at planes and trains manufacturer Bombardier.

"People always focus on the ability to pay claims – and this is important [since] ultimately it is why [businesses] buy a policy. However, with the current marine complexity, one of the elements Bombardier is looking for is a company that can help it with [global] risk management."

Key to achieving this is having someone in the insurer's organisation who can help evaluate risk globally and guide businesses through the process to ensure they understand their exposure.

"I want a global policy that I understand, that my insurers understand," says Desjardins.

Daniel San Millan, risk manager at infrastructure and services operator Ferrovial, agrees.

He says: "The insurer has to be as genuinely global as Ferrovial. We don't want to have discussions between countries or regions of a so-called 'global' insurer".

"I want to negotiate with underwriters with authority in all Ferrovial portfolio countries… I hate to hear 'sorry but you have to deal with the guy in Chicago for this specific risk'."

Really international

The risks of not having a genuinely international programme with the right local expertise can be significant for multinationals and middle market companies alike. For example, if a subsidiary encounters a problem that disrupts a supply chain, this could mean dire consequences for a manufacturer.

Furthermore, as Carole Chupin, directeur Département Maritime & Transports at ACE France, explains: "There could [also] be problems with legal issues or non-payment of tax, or you could have a lack of coverage or be relying on an insurer that perhaps doesn't have the funds to pay your claim".

> *'The quality of the information given by the local insurance company and the local broker is a critical point be able to provide efficient information to the corporate risk manager on minimum premium level and taxes'*
>
> **Jean-Yves Laville,** Aon

The advantage of an international programme (over a single global policy or patchwork of policies taken out with local insurers) is that it co-ordinates local cover within an efficient, standardised strategic framework.

Having a global insurance programme, incorporating local policies, enables risk managers to control their insurance conditions and be sure that the insurance cover in place for all countries is issued on the basis of conditions agreed and decided by them. This also helps control insurance costs.

The right partners

"Of course, it's also necessary to choose partners – brokers and insurers – that are in a position to manage a global programme through their own network to obtain the best service and reporting," says Jean-Yves Laville, technical director, transport at Aon France.

"A business can have the best insurance conditions, but this is useless without good partners to issue local policies [as part of a global insurance programme] when necessary and to explain [how to] respect local compliances and obligations.

"From my point of view, [as part of a global insurance programme] the quality of the information given by the local insurance company and the local broker is absolutely a critical point to be able to provide efficient information to the corporate risk manager on minimum premium level, taxes, the time limit for the issuance of the policy or settlement of the premium."

He adds: "A global insurance programme also has to be 'flexible' to provide local solutions to local problems," says Laville.

The correct global insurance programme also has to strictly respect the rules in all the countries covered by the policy.

"This is a day-to-day challenge that requires full co-operation between the client, the broker and the insurance company," says Laville.

"For example, obtaining the settlement of a premium before the date of inception in Japan can be a challenge if you do not choose an insurer able to issue the policy and premium very quickly."

Not at all cost

Getting all this in place means not always making cost the prime consideration and focusing instead on long-term partnerships. "[The price of cover] has to be reasonable for both parties, otherwise there is no incentive for the insurer to be flexible and it has to be able to build up some reserves to cover a loss when it occurs," says Maya Zeller, corporate insurance-risk manager, Cofra Holding AG. "[However,] we have a great relationship with our insurer and it listens to us when we want to change something."

> **USING BIGGER SHIPS: KEY POINTS**
>
> 1. Make sure you know how much of your cargo is at sea on any one vessel – and what a loss or delay could mean
> 2. Look to your risks loading and unloading large vessels
> 3. How does increased overland transport affect your exposures?
> 4. How do harbour side changes such as concentrating cargo on one site affect your risk?
> 5. Are your broker and insurer equipped to assist with complex claims like general average?

BIGGER AND BIGGER

Cargo ships are getting larger, but so are the risks

ONE AREA OF MARINE where risk managers need to ensure that their insurance is evolving fast and adapting to the rapidly developing exposure is in cargo, and particularly the use of bigger and bigger vessels, such as the massive 18,000 TEU EEE vessels now being delivered to Maersk.

Bigger boats offer obvious economies of scale, but they also aggregate risk by bringing significant amounts of cargo together. "If something happens to the ship, [the loss is bigger]," says Carl Leeman, chief risk officer at Katoen Natie.

"For example, on fire risk, although the risks are getting better, they are getting bigger at the same time. There is a greater concentration of risk in a small area."

Paolo Poddigue, marine manager southern European region at ACE, says: "It can take weeks to load and unload a vessel and, if for any reason, a vessel is delayed owing to a storm, it is not possible to merely switch to another ship. [This creates] a more attractive target for terrorists. There is also a greater pollution and fire risk. In addition, it's not always clear what is in containers and with 18,000 [of them] on board the risk of one containing explosives or another dangerous material is obviously higher.

"For insurers, the major issue is always concentration of risk, and these vessels concentrate a lot of risk."

Risk managers should also understand the exposure to their supply chain represented by having a significant amount of cargo at sea at one time on one vessel.

"I'm not sure people are up to speed with this," says Daniel Desjardins, senior director, global risk management and insurance at planes and trains manufacturer Bombardier. "I know that [Bombardier is], because we have had some new manufacturing challenges that have drawn us to look at it, and the size of these ships and the amount of cargo they can carry are frightening. These ships are big, but there are no ships of a sufficient size yet to load them, so it is important to consider the number of barges required to get the cargo on board. It is vital to look at loss prevention."

> *'The schedules of shipping mean goods and containers are coming into fewer centres, and this means concentration at those sites'*
>
> **Carl Leeman,** Katoen Natie

In addition, because these ships require a deep water berth and can therefore use only certain ports, firms can face another inland leg. This creates an additional exposure.

"The schedules of shipping mean goods and containers are coming into fewer centres, which means concentration at those sites," says Leeman. "If something happens at sea, and the [ships] need to get to port, they might have a long trip as a suitable port could be some distance away.

"In addition, there are changes in the harbour. Even competitors firms often co-operate to hire sites in ports and, instead of three or four sites, they rent one. This means that all the haulage operators that service these sites are all concentrated as well, which creates new risk. This situation is made worse because more and more [cargo] is going by road because it is cheaper."

Desjardins says: "The issue has led us to do a real deep dive into our operations to look at not only the risk posed by our goods while on board, but while travelling to port and from the port on the other side towards their ultimate destination… It is vital to know what is going on and structure policies accordingly."

General complex average

One area of particular concern for everyone is the rise in the number of complex general average (GA) claims associated with bigger vessels. "It is important that risk managers look at their exposure to this risk in a careful way," says Cristiano Cavalieri D'Oro, marine claim supervisor at ACE Italy.

"A GA is a loss that arises from the voluntary sacrifice of part of a ship or cargo to save the residue of the ship or cargo or from extraordinary expenses incurred in protecting the interests involved under pressure of a common risk and that is shared proportionally by all parties concerned. When the vessel docks, the master refuses to release [an owner's] cargo until it has paid towards the GA, which is why a marine cargo policy is necessary to take care of this. Then, [the owner's] insurer will release a guarantee and it will receive its cargo. Otherwise, it will need to pay cash to take possession of its goods. In addition, many lawyers can become involved to resolve who pays what, which can be expensive.

"However, with the right insurance, again this [problem does not arise]. The owner gets its cargo and the insurer takes over."

Marine transportation

HIGHWAY ROBBERY

The growing risk of theft in transit

RISK OBVIOUSLY DOES NOT disappear when an owner's cargo rolls onto the quayside and theft of goods is a global problem.

However, as European firms look for growth in the BRICS and other emerging economies, so their exposure is increasing and this is a particular problem in Latin America.

"Theft of cargo is a major issue here," says Phil Skelton, head of transportation risk management, ACE Overseas General. "Because of the huge distances travelled between ports and markets, trucks can be on the road through rural areas for more than a week and are vulnerable to attack during this time.

"These attacks vary between highly organised, armed gangs taking out vehicles, to what they call 'tippings', where, because road conditions are bad, if a truck breaks down or tips over, the local population strips the vehicle and the police can do nothing about it."

In response, firms have adopted specific security arrangements, primarily the use of so-called 'risk management companies' that monitor and even escort the vehicles, train and vet staff and provide armed personnel.

"Nothing of any value moves here without one of these companies being involved," says Skelton. "The good companies have better intelligence gathering than the police."

SECURITY IN LATIN AMERICA: KEY POINTS

1. Be aware of the risk: cargo theft and hijack are common
2. Take risk management advice. Talk to your insurer
3. Use a reliable 'risk management' firm for security
4. Plan routes carefully and analyse all losses for lessons to learn
5. Consider additional technology such as hiding GPS devices in cargoes.

A close relationship

A good insurer can demonstrate its value in helping develop the relationship between firms and their security.

"I went to São Paulo on behalf of a client," says Peter Kelderman, senior transportation risk manager at ACE in Germany. "The company was transporting a lot of products around the country and facing losses from theft. In response, we created a complete new risk management approach, which so far seems to be preventing any losses.

"The key was a close working relationship between everyone involved; we looked closely at the routes being used and, of course, used a good risk management company. We made sure that every theft, every accident, was thoroughly investigated.

"In addition, although the use of GPS in vehicles is common, so is the use of 'jammers' by criminals that block the signal and allow scammers to 'disappear' the truck.

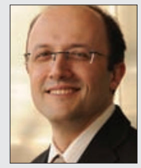
"To get around this, we advised the use of additional mobile GPS devices that are hidden in the truck. Then, if the truck is taken and the main signal jammed, the vehicle can still be tracked."

In the end, protecting cargo, be it at sea or on the open road, depends on paying attention to the basics. It is important for cargo owners to get to grips with the detail of their risk.

"If [a cargo owner does not] understand its new exposures and present them properly to its underwriter, then that could be its biggest risk," says Daniel Desjardins, senior director, global risk management and insurance at planes and trains manufacturer Bombardier. "If [an owner] fails to do internal work, then it could end up uninsured.

"A loss is a loss. However, knowing where that loss has come from will mean it can't hurt as much." SR

THOUGHT LEADERSHIP



BENOÎT CHASSEGUET
Marine manager, Continental Europe & CEE, ACE Group

Container ships have revolutionised business and made the world seem like a much smaller place. However, there is that the dangers of open water could be forgotten in the rush for growth.

It seems so easy to transport items thousands of kilometres across the sea. However, the sea is just as dangerous as it always has been. In fact, climate change means that even more extreme weather risks are emerging.

Risk managers need to acknowledge this fact. For instance, internet footage of container ships ploughing across the North Atlantic in winter are good reminders of how fragile marine transport can be. Sinking, stranding, rough weather or general average could have disastrous consequences to a just-in-time supply chain.

In addition, manufacturers are building bigger ships that can aggregate enormous amounts of goods on a single vessel as well as in ports.

In order to mitigate the risks related to marine transportation, risk managers need to look at their coverage, ensuring they have proper covers in place and the claims experts on side who can help them if the worst happens.

In this environment, excellence in risk management is vital and partnering with an insurer able to offer good advice is essential, especially when expanding overseas.

For example, many companies have recently increased the scale of their operations in Latin America, where the risks of violent theft and other cargo losses has also increased.

However, ACE's strong presence across the region providing risk management and loss prevention advice represents formidable added value to help our clients.

Furthermore, having good insurer support can make all the difference in negotiating tortuous 'general average' claims; when the captain has to sacrifice some of the containers on board to save the ship, then that loss is shared by all those with goods on board.

In these circumstances, working out who pays what is complex and time consuming; and with larger and larger ships, these claims will become even more complex in future.

Nowadays, risk managers need to know their risks. They need to ensure they have the right solutions and claims handlers who really know this business and are properly equipped to engage on their behalf.

Only then is it really safe to set sail.

REGULATION & LEGAL

TACKLING THE GROWING SPECTRUM OF CYBER RISKS

Considering the scale of the losses that can result from a cyber attack, businesses should ensure they understand, take steps and insure against crime and data breaches

SCARCELY A DAY GOES BY WITHOUT NEWS HEADLINES reporting yet another data breach or cyber crime incident, which can have devastating consequences for any business in terms of reputation and balance sheet. In contrast with many other forms of risk, cyber risk cannot be readily confined. With increasing automation and interconnection between information systems, a compromise of information in one area of the business could affect an entire organisation and its customers. No industry or organisation is immune.

Most cyber attacks are motivated by the desire to secure some form of economic advantage, whether by stealing financial assets, intellectual property or critical personal information of clients or customers. The spectrum of cyber attacks is growing as cyber criminals develop ever more sophisticated ways of attacking network systems: see box.

Cyber criminals are increasingly using subtle social engineering techniques to quietly penetrate an organisation, deploying customised malware (malicious software) that can live undetected in network systems for months. Cyber criminals can then remotely and covertly steal a firm's most valuable information, whether in the form of personal customer information, credit card data or potentially trade secrets or intellectual property. The different types of malware continue to snowball at an alarming rate, which means that keeping ahead of the game in terms of network security has become an increasing challenge. The means of access are also growing as organisations make increasing use of third-party vendors or so-called "cloud" providers, which facilitate storage of data off-site. As FBI director Jane Camey said in October 2014, there are only two types of companies: "those that have been hacked and those that don't know it yet".

The management of cyber risks is not merely an IT issue. Experience has shown that even the most sophisticated, state-of-the-art security systems are breachable. Many attempts to compromise information involve the successful manipulation of people and human nature. It is often easier to trick someone into clicking on a malicious link in an email than it is to hack into an IT system. The attack on Target, the US retailer, whereby hackers gained access to its computer system and stole the financial and personal data of 110 million shoppers is reported to have been the result of hackers tricking the employee of an outside vendor into clicking on a malicious email.

> The loss or compromise of personal customer information or credit card data carries with it not only potential legal and regulatory issues but immediate reputational and brand damage

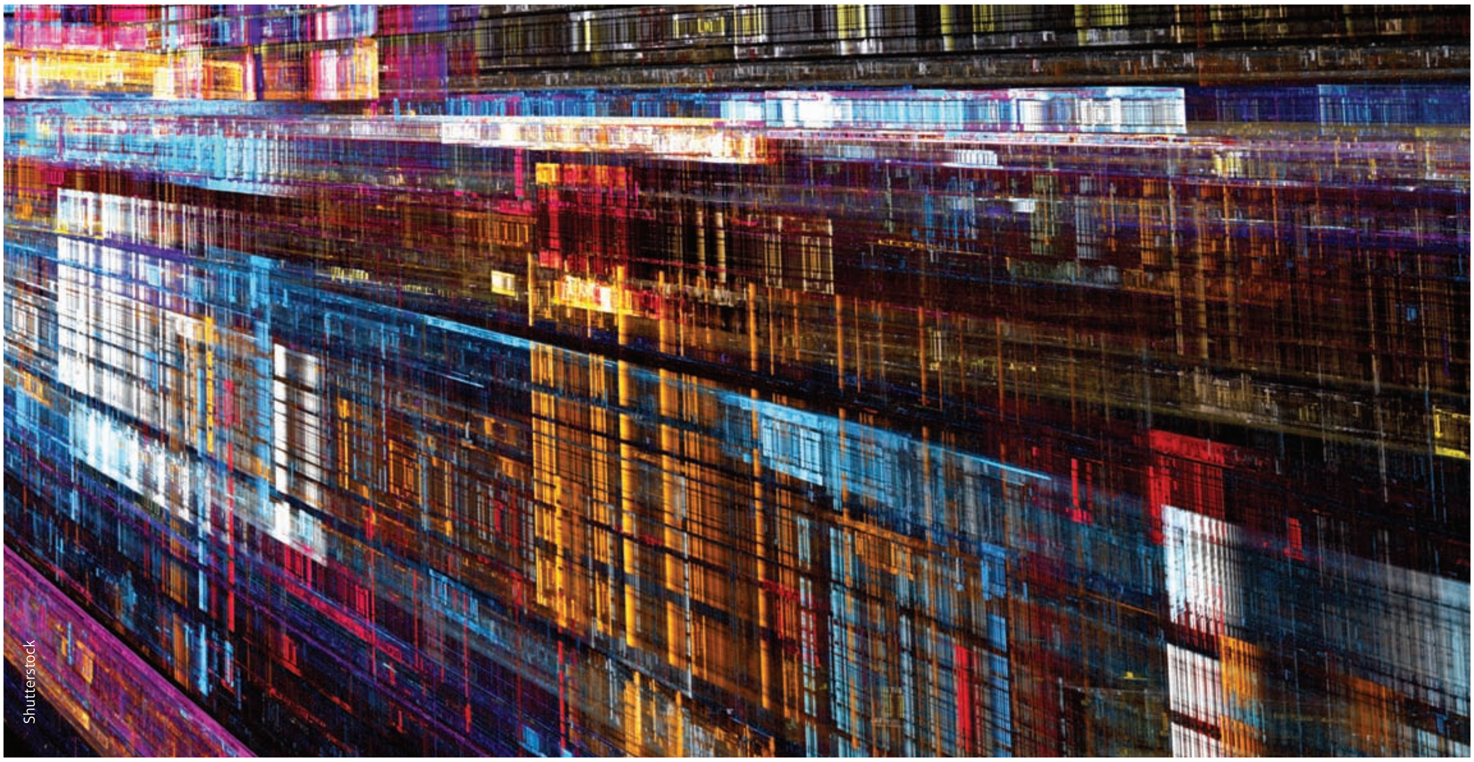
Management of cyber risks needs to be high on the boardroom agenda. Stakeholders and partners are increasingly seeking assurances regarding cyber security and, in the future, this is likely to include regulators, investors, customers, employees and lenders. The board needs to take a proactive approach to cyber risk and ensure that it is given the same level of attention as other legal, regulatory, financial and operational risks. Failure to do so could result in severe criticism being directed at the board and in potential claims against individual directors for breach of fiduciary duty.

Potential consequences of a cyber attack?

Cyber risk can take many forms and can affect the business in a number of ways, many of which can have a devastating effect. The loss of the "crown jewels" in the form of trade secrets or intellectual property could completely undermine competitive advantage, effectively destroying the financial stability of a business overnight. Any retail businesses with an online presence, if subjected to a denial of service attack, might lose customers to competitors with the resulting loss in sales and damage to reputation. This risk is heightened at particularly busy sales periods.

The loss or compromise of personal customer information or credit card data carries with it not only potential legal and regulatory issues but immediate reputational and brand damage. Cyber attacks naturally affect customer confidence, especially when customer funds or data are lost or stolen. In the current digital world, these concerns are likely to be exacerbated by social media and online communication forums that spread news of such an attack at an unprecedented speed. The potential downturn in sales combined with the costs of restoring reputational damage as well as the cost of investigating the cause of the attack and repairing cyber defences can be significant. In addition, a business may face the additional cost of notifying affected customers as well as potential fines and penalties, depending on the relevant legal and regulatory framework. Customers may claim compensation for any losses alleged to have been suffered as a result.

Currently, in the UK, the Information Commissioner has the power to impose fines (up to a maximum of £500,000 (€697000)) for serious contraventions of the Data Protection Act 1998. This is due to increase under the proposed new EU Data Protection Regulation, to fines of up to €1m or up to 2% of annual worldwide turnover for certain compliance failures, including failing



to notify data breaches, transferring data to a territory without ensuring appropriate safeguards or failing to designate a data protection officer. These proposed changes will affect all EU countries and represent a dramatic increase on the level of fines currently being imposed within the EU.

At present, there is no mandatory requirement in the UK to notify the Information Commissioner about data breaches (outside of certain regulated sectors) and this is the case in all EU countries. This could change under the proposed regulation to a system of mandatory reporting. This would require all data controllers to have continuous monitoring and reporting systems in place at all times.

Practical steps to mitigate cyber risk

Every organisation should consider a number of key steps as part of its risk management regime in an effort to mitigate cyber risk, including:

- establish a cyber risk management policy and ensure that this is part of the company's governance framework and, as such, give it the same level of attention as financial and other risk management regimes;
- undertake an initial risk assessment which includes consideration of the amount and type of personally identifiable information, customer data and confidential corporate data maintained by the organisation and the manner in which that information is used, transmitted and stored. The company's technology infrastructure needs to be evaluated as well as potential threats to the network security and the likely consequences of significant interruptions to online working or customer transactions. Also consider the risk of third party claims arising from the company's media content and the services provided to support e-commerce;
- ensure internet safety and network security. Networks should be protected against external and internal attack and steps taken to reduce the scope for penetration, for example by controlling access to removable media (such as memory sticks) and scanning all media before incorporating them into network systems. Consider who needs access to what. If an employee does not need access to sensitive data, they should not have it;
- adequate training and user awareness. Every organisation has a cyber defence weak spot in its own employees. An adequate cyber security system should not only have the relevant defences and policies in place, but staff should be adequately trained on all relevant policies and procedures;
- ongoing management. Planning and analysis of risk serves no proper purpose unless a company properly implements its findings. As cyber crime continues to evolve, companies must constantly monitor the adequacy of their cyber security and re-evaluate the threats pertinent to their business; and
- establish an incident response and disaster recovery team and put in place an incident response plan that has been adequately tried and tested. This should include legal team members to be called on to advise in relation to potential legal or regulatory issues, including the need to notify regulators and customers. Their advice may benefit from legal professional privilege. The umbrella of legal privilege can be particularly beneficial in the cyber crime context given the potential legal, regulatory and reputational ramifications.

Insurance for cyber risk

Insurance can play a vital role in the management of cyber risk, particularly when preceded by a thorough risk assessment, which should facilitate an in-depth understanding of the types of cyber risk, and the potential losses and liabilities that could affect the business following a cyber attack or data breach.

The question that first needs to be addressed is the extent of coverage already provided for cyber risk under existing insurance policies, including professional indemnity/civil liability, crime/fidelity and property/business interruption policies. Such policies have not historically been designed to cover the risks revolving around intangible assets, and network related risks, so a careful assessment of the coverage provided by these policies is essential. There are likely to be gaps in cover and the company will need to consider how those gaps should be filled, whether by enhancements to existing policies or through new cyber products being offered by insurers.

The cyber insurance market has developed rapidly in recent years and a number of insurers are now offering dedicated cyber insurance policies. However, the wording of cyber policies varies enormously and there can be huge discrepancies in the scope of cover provided. Some policies contain particularly onerous terms and conditions and others have exclusions that may serve to undermine the purpose for which the cover is being bought. A careful analysis of the coverage being offered is essential to ensure, not only that the particular risks and exposures faced by the company are covered, but there are no exclusions or conditions that could prevent pay out in the event of a significant claim.

The types of loss and liabilities that cyber policies typically cover include:

- **Data liability**. This should cover damages and defence costs resulting from any claim against the insured resulting from any data breach that compromises personal information or any claim alleging that information has been lost or compromised as a result of unauthorised access to or use of the insured's computer systems. It is important to ensure that this covers not only loss of an individual's personal information but employee data and confidential corporate data, including third-party trade secrets, customer lists, marketing plans and other information that could be beneficial to competitors and could result in liability if compromised.

- **Media liability**. This should cover damages and defence costs resulting from any claim against the insured for infringement of copyright and other intellectual property rights, misappropriation or theft of ideas or media content. This may not extend to content published in a personal capacity, but this should ideally be included because the organisation may face significant liabilities as a result of the use by employees of Twitter, Facebook and other social sites and networks.
- **Regulatory coverage**. This should cover the cost of responding to any administrative, government or regulatory investigation following a data breach or cyber attack (for example by the Information Commissioner's Office, the Financial Conduct Authority and the Securities Exchange Commission) and any fines or penalties imposed. However, coverage will typically be limited to civil fines and penalties (criminal fines and penalties are not insurable in many jurisdictions) and some regulators prohibit regulated firms from recovering any fines or penalties they impose from insurers.
- **Remediation coverage**. Most policies provide coverage for the additional costs associated with a data breach. This should include costs incurred by the company in notifying those affected, notifying relevant authorities (where required), credit monitoring those affected and setting up call centres to field enquiries from concerned clients. Coverage may also extend to the costs of forensic services to determine the cause and scope of breach as well as PR expenses and other crisis management costs.
- **Information assets coverage**. The policy may include coverage for the cost of recreating, restoring or repairing the company's own data and computer systems. Such coverage may also extend to third-party data that has not been captured by back-up systems or has been corrupted or lost, for example, as a result of negligence or technical failure.
- **Network interruption coverage**. The policy may cover lost revenue owing to network interruptions or disruptions resulting from a denial of service attack, malicious code or other security threats to networks.
- **Extortion coverage**. Many policies include cover for the costs of responding to demands for ransom or extortion to prevent a threatened cyber attack.

As mentioned, the scope of coverage provided by cyber policies varies and the specific policy terms and conditions should be analysed carefully to ensure that the coverage provided meets the company's likely loss scenarios and potential exposures. One particularly important consideration is whether the coverage extends to information in the hands of third parties where data handling, processing and storage has been outsourced to third parties, including cloud service providers. If the organisation has outsourced data handling, coverage should be sought for any loss or business interruption arising from data that is managed by third-party service providers.

Another point to watch out for is the "retroactive date" as cyber policies will often limit coverage to cyber attacks or data breaches that occur after a specified date, which may be consistent with the policy inception date. It is important to request retroactive coverage for network security breaches that may have occurred before the inception date, given that it is not uncommon for cyber attacks to remain undetected for a considerable period.

Although it can take six months or more after a breach to determine the full financial consequences of a cyber attack, estimates suggest that one of the latest cyber attacks on a technology and media company will cost about $100m. The financial cost of the reputational damage and lost business opportunities is hard to quantify. Given the scale of the losses that can flow from a cyber attack, it is ever more important that businesses understand, take steps to mitigate and where possible insure against cyber risks. A proactive approach to cyber risks and insurance is essential.

Sarah Turpin *is a partner in the cyber law and cybersecurity and insurance coverage groups and* ***Sasi-Kanth Mallela*** *is special counsel in the cyber law and cybersecurity and government enforcement groups at K&L Gates in London*

THE SPECTRUM OF CYBER ATTACKS

- **Advanced oersistent threats (APTs)**: nation state-sponsored attacks that are targeted, persistent and advanced and typically result in loss of trade secrets or intellectual property.
- **Cyber criminals** typically attack using exploits and malware (malicious software designed to remain undetected) as a means of stealing valuable information or financial assets. Cyber criminals also deploy ransomware, a form of malware that makes itself known on purpose and gives criminals the ability to lock the victim's computer from a remote location, claiming the victim will not be able to access it unless they pay a ransom.
- **Denial of service attacks** or **distributed denial of service (DDoS)** attacks that are designed to make a machine or network resource unavailable to its intended users.
- **Domain name hijacking** or **domain theft**, whereby registration of a currently registered domain name is transferred without the permission of its original registrant.
- **Corporate impersonation** and **phishing**, whereby emails purporting to be from reputable companies are used to induce individuals to reveal personal information, such as passwords or credit card numbers.
- **Employee mobility** or disgruntled former employees who may seek revenge by compromising network systems or stealing valuable information.
- **Lost or stolen** laptops and mobile devices that may contain valuable commercial or client data.
- **Inadequate security and systems**: third party vendors that may provide another means for criminals to access network systems.

Q&A

How a new regulation will change data protection in the EU

Q: From higher fines to new notification requirements, what should risk managers know about the forthcoming changes to data protection legislation?

A: Current data protection legislation in EU member states is derived from Directive 95/46/EC, which came into force in 1995.

However, since this time, there have been major technological developments and changes in the way in which data is used. By way of example, when the Directive was under development, the internet was still a relatively new phenomenon and social networking sites, location-based services or cloud computing did not exist. Twenty years on, a new law that specifically addresses the use of personal data in today's world and beyond is required.

Regulation v Directive

The proposed new legislation is in the form of a regulation, which differs from a directive.

A directive sets out a goal that all EU countries must achieve, but leaves it to the individual countries to decide how to do so. For this reason, current data protection legislation varies between member states as each has implemented the Directive into their national laws slightly differently. This has led to difficulties for international businesses that operate across a number of EU jurisdictions because they have to comply with slightly different requirements in each country.

In contrast, a regulation is binding and must be applied in its entirety across the EU. Here, this means that, once the Regulation has come into force, one set of rules should govern data protection in all member states.

Key changes

The Regulation will introduce numerous changes that cannot all be covered in this article. Some of the changes likely to have the greatest effect on businesses or that have been particularly high profile, are described below:

- **higher fines:** fines will be significantly increased. Current proposals range from between 1%-5% of an organisation's annual worldwide turnover or up to €1m, whichever is greater;
- **data protection officers:** certain organisations will have to appoint a data protection officer. The threshold for triggering this requirement is not yet confirmed; current proposals include having at least 250 employees or processing data of at least 5,000 individuals;
- **territorial scope:** the Regulation will in some circumstances apply to data controllers that are not based in the EU. This will be the case if a data controller:
  - processes personal data of individuals residing in the EU; and
  - such processing activities relate to offering them goods or services or monitoring their behaviour;
- **one supervisory authority:** there will be a "one-stop shop", that is one data protection authority will be responsible for the supervision of a business across all its EU operations. The supervisory authority that will be responsible for a business will be the one in the country of that business's main establishment. This will be the country in the EU where the main decisions about the processing of personal data are taken;
- **notification of data breaches:** the Regulation introduces an obligation to notify the supervisory authority of personal data breaches. A personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed";
- **consent:** where consent from individuals is used to justify the processing of their personal data, only express consent will be valid. Businesses will no longer be able to rely on implied consent; and
- **right to be forgotten:** individuals will have the right to require businesses to erase their personal data where the individual withdraws consent or objects to the processing on certain grounds. If the business has made the data public, it will have to make reasonable efforts to inform third parties of the request to delete any links to, or copies of, the data.

What next?

At present, the Regulation is still in draft form. Based on the current timetable, a final text is likely to be approved at some point this year. The Regulation will then come into force following a transitional period of two years to give businesses time to understand the new requirements and make any necessary changes.

In the meantime, businesses can prepare by making sure they have a good understanding of the ways in which personal data is used within their organisation, including how it is obtained, shared, transferred, retained, destroyed etc. Once data flows are mapped out, the business should ensure it has a robust internal governance framework with the necessary policies and procedures, and appropriate controls in place. Every business processing personal data should ensure that a designated person has responsibility for data protection across the business. Training should be rolled out along with initiatives to raise staff awareness of the relevant issues.

Robyn Palmer is a senior associate in the intellectual property and technology group at DLA Piper

REGULATION & LEGAL

RETENTION OF COMMUNICATIONS DATA: ARE WE THERE YET?

With the underlying EU Data Retention Directive ruled invalid, new UK legislation rushed onto the statute books to replace it, and further changes being recently introduced, is the upheaval yet over for retention of communications data laws?

THE RECENT INTRODUCTION OF NEW DATA RETENTION powers in the Counter-Terrorism and Security Act 2015 is the latest development in a period of unprecedented upheaval for data retention legislation. This article takes stock of the changes to date and considers the future direction of travel of this topical area of law in the current post-Snowden political climate.

The principle of data retention legislation is to oblige companies providing communications networks or services to the public to retain the "metadata" relating to their customers' communications for a period of time so that it can be made available to intelligence services and law enforcement agencies in the course of a criminal investigation or a secret intelligence operation. Metadata is typically described as the 'who, where, when and how' of a communication, but not its content. The term is broad, for example often encompassing geo-location data relating to mobile phones, and IP addresses assigned to devices accessing the internet.

> The current legislative framework governing the intrusive capabilities of the UK's intelligence services needs a complete overhaul

Until April 2014, data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). The Directive was introduced in the midst of heightened national security concerns about the threat of international terrorism in the first part of the last decade. It was transposed into law in the UK by the Data Retention (EC Directive) Regulations 2009 (the 2009 Regulations).

The Directive required providers of publicly available electronic communications services or public communications networks to retain certain types of metadata relating to their customers for a period of time of between six months and two years. This obligation was carved out of the existing overarching rule that customer metadata could be retained only for the time necessary to enable a communication to take place or for invoicing-related purposes.

On 8 April 2014, the Court of Justice of the European Union (CJEU) ruled that the Directive was invalid. Following a few months of uncertainty in the UK about the legal status of the 2009 Regulations, on 10 July 2014, prime minister David Cameron announced emergency new primary legislation to replace them.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) passed into law just seven days later under the emergency fast-track legislative process. The accompanying Data Retention Regulations 2014 (the 2014 Regulations) came into force on 31 July 2014. DRIPA's data retention provisions were then extended by the Counter-Terrorism and Security Act 2015, which received Royal Assent on 12 February 2015. By any yardstick, the pace of legislative change in the UK has been rapid.

An invalid Directive

The CJEU's declaration of invalidity was the conclusion of its judgment in the case of *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* C-293/12 joined with *Karnter Landesregierung* C-594/12. The two joined cases were preliminary references from the Irish and Austrian courts. Each court asked the CJEU to clarify, among other things, whether the Directive was compatible with two fundamental rights enshrined in the EU Charter of Fundamental Rights (the Charter):

- Article 7 (the right to respect for a person's private and family life, home and communication); and
- Article 8 (the right to the protection and fair processing of a person's personal data).

The CJEU found that the obligation imposed by the Directive to retain customer metadata was itself an interference with the privacy rights guaranteed by Article 7 of the Charter. The provision of access to this data to intelligence and law enforcement agencies was a further interference with Article 7 rights. In providing for the processing of personal data, the Directive also interfered with the fundamental rights granted under Article 8.

The CJEU's description of the Directive was startlingly unequivocal: its interference with Articles 7 and 8 was "wide ranging, and... particularly serious" and "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". In short, the Directive constituted "an interference with the fundamental rights of practically the entire European population".

Nonetheless, the CJEU did make it clear that meeting the objectives of the Directive could in theory be a ground for a justifiable limitation of Charter rights. It found that because the Directive did not allow access to the content of communications, it did not adversely affect the essence of the Article 7 and Article 8 rights. It also recognised that fighting international terrorism and serious crime are objectives of general interest that might justify limiting such rights.

Instead, the focus of the CJEU's criticisms was on the Directive's lack of proportionality, particularly its imprecise scope and its failure to limit its own interference in the Charter rights. The judgment contained a long list of deficiencies, with some key themes being that the Directive:

- was too generalised and overly broad in scope, without any level of differentiation, limitation or exception;
- set no limits or conditions to the access granted to competent national authorities to the relevant data, or their subsequent use of it; and
- did not contain any rules relating to security, protection or destruction of data in light of the vast volumes of data (much of it sensitive) retained.

Uncertainty ensues

As might be expected, the judgment created considerable uncertainty. Although EU data protection regulators and privacy advocates welcomed the decision, from the UK government's point of view, the prospect loomed of telecommunications service providers unilaterally deciding to stop retaining metadata, and then deleting what they had retained in order to comply with data protection laws.

The UK unveils DRIPA

Even so, when the UK government announced DRIPA, to some surprise, it stated that DRIPA was not only necessary in order to plug the legislative hole created by the Directive's invalidity, but also to address another issue that threatened to undermine the legal basis of the government's investigatory powers: the scope of the Regulation of Investigatory Powers Act 2000 (RIPA) was being challenged by various (unnamed) telecommunication service providers based outside the UK.

RIPA is the UK legislation under which the intelligence services, law enforcement agencies and to a limited extent other government bodies can be granted powers to secretly monitor individuals, including to intercept communications, acquire metadata of communications (now retained under DRIPA) and undertake covert surveillance.

The UK government did not provide much detail about the nature of the challenges to RIPA. Nevertheless, DRIPA's amendments (described as 'clarifications' by the government) gives RIPA (among other things) an explicitly extra-territorial reach. It ensures that any communications service provider anywhere in the world that offers communication services to customers in the UK can be served with an interception warrant under RIPA, which may include the requirement that action to implement the warrant be taken outside the UK.

Other amendments related to RIPA's defined terms. RIPA has always used a different set of definitions to describe the components of a communications network or service than those introduced in the EU Framework Directive (2002/21/EC) and then used in subsequent EU legislation relating to the telecommunications sector, including in the 2009 Regulations.

DRIPA not only uses RIPA's definitions rather than those from the 2009 Regulations, it also amends one of the most important ones within RIPA: that of 'telecommunication service', by supplementing the existing definition of "any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system" so that this includes a service that "consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted by means of a such a system".

It is hard to avoid the conclusion that this small change may have far-reaching effects in practice. The amendment appears to bring the IT infrastructure underpinning internet communications platforms and services anywhere in the world under the potential scope of RIPA. Such infrastructure may include, for example, data centres in the US supporting popular email, video calling and social media software applications.

Thus, from the UK government's point of view, DRIPA killed two birds with one stone by implementing a single legislative solution to two potentially serious legal difficulties. From the point of view of DRIPA's critics, the fact it was ushered through the legislative process so quickly, while going beyond replacing the 2009 Regulations to make far-reaching amendments to RIPA, only intensified the suspicion that a significant expansion of the government's investigatory powers has been smuggled onto the statute books without the opportunity for proper public debate or parliamentary scrutiny.

DRIPA's powers extended

The Counter Terrorism and Security Act amends DRIPA by adding a new category of metadata to it: relevant internet data. This is defined to mean data that may be used to identify, or assists in identifying, an IP address used to access the internet, or other "identifier". The drafting of the Act is not always easy to follow, but it seems that this is intended to include port numbers or MAC addresses of devices.

The amendments are cast as an attempt to solve the investigatory hurdle posed by the sharing of IP addresses, whereby a temporary IP address is automatically allocated to many customers simultaneously, making it impossible to definitively link a subscriber's device to the IP address at any point in time. The identity of websites visited, or of individual browsing histories, has been explicitly excluded.

More laws to come?

To its critics, DRIPA, the 2014 Regulations and the Counter-Terrorism and Security Act fail to replace the 2009 Regulations with a mandatory data retention regime that adequately accommodates the criticisms of the Directive made by the CJEU.

Although some safeguards have been introduced in DRIPA, notably in relation to data security measures, the detail of the obligations to be imposed is left to the discretion of the Secretary of State on a case-by-case basis. This leaves DRIPA vulnerable to judicial review on the basis of incompatibility with the Charter. Indeed, the human rights organisation Liberty has been granted permission to launch such a judicial review of DRIPA.

The UK government's position is that DRIPA is a temporary stop-gap measure. It contains a sunset clause that means the Act is automatically repealed on 31 December 2016. On 12 March 2015, the first official indication was made of what might replace DRIPA, when the Intelligence and Security Committee (ISC), which has statutory oversight of the UK's secret intelligence services, published its much anticipated *Privacy and Security Report*.

The ISC's report had little to say on the question of DRIPA's compatibility with the Charter. However, it concluded that the current legislative framework governing the intrusive capabilities of the UK's intelligence services needs a complete overhaul. It recommended that the relevant laws (including DRIPA and RIPA) be replaced by a new, transparent, legal framework under a single Act of Parliament, and that this process should start early in the next parliament.

Assuming that the government follows this recommendation, it is to be hoped that the passage of the new draft Bill envisaged by the ISC follows a more consensual and transparent process than was the case with the current data retention regime.

__Charlie Hawes__ is an associate and __Mark Taylor__ is a partner at Hogan Lovells International LLP

Shutterstock

TO BREXIT OR NOT TO BREXIT? THAT IS THE QUESTION

As some politicians clamour for the UK to leave the EU, what would happen to the EU-derived employment laws in such an event? Would everything change or would it remain the same?

UK PRIME MINISTER DAVID CAMERON HAS promised that should the Conservative Party win the next election in May 2015, he will seek to renegotiate the conditions of the UK's EU membership and put the new terms to the public in an 'in-out' referendum in 2017. If he makes it that far, what will be the implications of a vote for a so-called 'Brexit'?

In particular, what will happen to all EU-derived employment law: discrimination rights, holiday entitlement, duties to agency workers, data protection obligations, works councils and myriad other matters that have become entrenched in the UK legal system? Perhaps someone should tell Cameron – not to mention UK Independence Party supporters – that there are good arguments to suggest that little would change.

Legislative challenges

To some extent, what happens to UK employment law will depend on how the government tries to extricate itself from the EU. European law has been incorporated into UK law in a variety of ways. Some UK laws are secondary legislation, that is, regulations introduced by a government minister under powers granted by the European Communities Act 1972 (the statute enacted to incorporate EU law). One example is the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE), which implements Directive 2001/23. Other UK-implementing legislation, such as the Equality Act 2010, is primary legislation (that is, an Act of Parliament).

If the government simply repealed the European Communities Act, the regulations passed under it (for example, TUPE) would probably fall away. In contrast, freestanding acts of Parliament (for example, the Equality Act) would remain in force. The result would be inconsistent and confusing for businesses. Repealing all primary and secondary legislation in one swoop would result in an avalanche of legal changes for employers and their staff. A more realistic approach following an exit from the EU would be to maintain the status quo and address particular laws individually over time. This could be done by repealing them or merely tinkering to make them more palatable to the UK business environment.

> Perhaps someone should tell Cameron – not to mention UK Independence Party supporters – that there are good arguments to suggest that little would change

Case law

If this happens, a major issue will be the post-exit treatment of European Court of Justice (ECJ) decisions. Presently, UK courts must interpret EU-derived legislation in accordance with ECJ rulings and a body of UK case law has built up that does so. On leaving the EU, the ECJ would no longer have jurisdiction and its future decisions would not be binding on UK courts. However, it seems likely that if the UK were to retain any laws originating from the EU (which is probable), the UK courts would still take account of future ECJ judgments as persuasive – albeit not binding – when ruling on those laws. In this case, the ECJ would continue to exert an appreciable influence.

A further complication concerns pre-existing case law. Past ECJ rulings have become entwined with UK court decisions and legislation. For example, ECJ decisions on what amounts to a TUPE transfer, that sex discrimination includes gender reassignment and that pregnancy discrimination is unlawful without the need for a comparator have been written into the law. Additionally, when taking into account ECJ decisions, UK courts have incorporated them into their own jurisprudence. For instance, the leading Supreme Court decision on the types of factor that might justify age discrimination depends on ECJ reasoning. Sometimes, UK courts go a long way to make UK legislation consistent with ECJ rulings. Prominent examples include recent cases on holiday pay in which the courts have read additional wording into the relevant UK legislation to give effect to ECJ decisions.

Past decisions remain binding on lower courts, subject to their ability to distinguish them because the particular facts of the case are different. Possibly, UK courts would treat the fact that they are no longer obliged to apply ECJ judgments as a materially different circumstance justifying a complete departure from previous rulings. However, it seems more likely that they would continue with many established doctrines (if for no other reason than to preserve legal certainty) – perhaps retreating from more extreme decisions that have required words to be read into legislation.

Possible outcomes

The ensuing period of uncertainty could prove a real headache for businesses. Employers would be unable to predict with any confidence whether the courts would feel obliged to follow or depart from existing precedents. There might be several conflicting lower court decisions until a case came before the Court of Appeal or Supreme Court and a binding precedent was set.

What if the UK were to get rid of all legislation of EU origin? Once deleted from the statute books, the related court decisions would be of merely historical interest. It seems unlikely that all EU law will be consigned to the UK's legislative dustbin, for two main reasons.

First, both employers and employees consider much of the body of EU law to be a good thing. Most employers would not argue that they should be free to discriminate or even that there should be no right to paid holiday. In reality, a handful of laws would probably be scrapped owing to unpopularity (the Agency Workers Regulations being the most likely example) and some fairly minor modifications might be desirable for certain others.

Removing entire laws would be much easier from a legal perspective, because it would not give rise to the uncertainties discussed above; but on a practical level, it would engender many other issues. Even if employers and employees wanted to discard all existing EU legislation, large numbers of commercial agreements have been based on it. Abruptly terminating TUPE, for example, would cause havoc with commercial outsourcing arrangements, which all contain provisions based on the assumption that TUPE will operate to transfer the employees if the agreement terminates (and have been priced accordingly).

An even more compelling reason to retain the bulk of EU legislation is that the UK would want to stay in a relationship with the EU. It is the UK's biggest export market and, as such, the UK will want some sort of free trade agreement with it. Practically speaking, the options for the UK would be either to join the European Economic Area (EEA), like Norway, or to negotiate bilateral agreements with the EU, like Switzerland.

EEA membership

The EEA is made up of the EU and three of the European Free Trade Association (EFTA) member states: Norway, Iceland and Liechtenstein. As part of this arrangement, the EEA EFTA states are obliged to accept the majority of EU regulations without being part of the EU decision-making process or able to influence it. Norway, Iceland and Liechtenstein thus participate in most EU social and employment policy. For example, the EEA agreement incorporates many EU directives, including the Equal Treatment Directive, the Collective Redundancies Directive, the Part-Time Workers Directive, the Posted Workers Directive, the Parental Leave Directive, the European Works Councils Directive, the Acquired Rights Directive, the Working Time Directive and the Agency Workers Directive. Further, the influence of the ECJ would still be felt because the EFTA Court, which interprets the EEA rules, is obliged to follow ECJ case law.

Bilateral agreements with EU

The Swiss model does not offer much more hope to UK 'eurosceptics'. Switzerland has more than 120 agreements with the EU – many of which incorporate EU law – and Swiss legislation often follows EU law, even in sectors not covered by these agreements. In practice, Switzerland has data protection, TUPE, discrimination, collective redundancy and working time laws and the Swiss courts often follow ECJ case law.

Even the most fundamental goal of many eurosceptics – namely to reduce EU immigration into the UK – may not be achievable under either of these types of arrangement. The free movement of persons is an integral part of the EEA agreement and Switzerland had also signed up to this principle. A recent Swiss referendum resulted in a vote to cap immigration, but this has put the entire basis of the bilateral agreements between Switzerland and the EU at risk, and it is not yet clear what type of arrangement may emerge from the renegotiation.

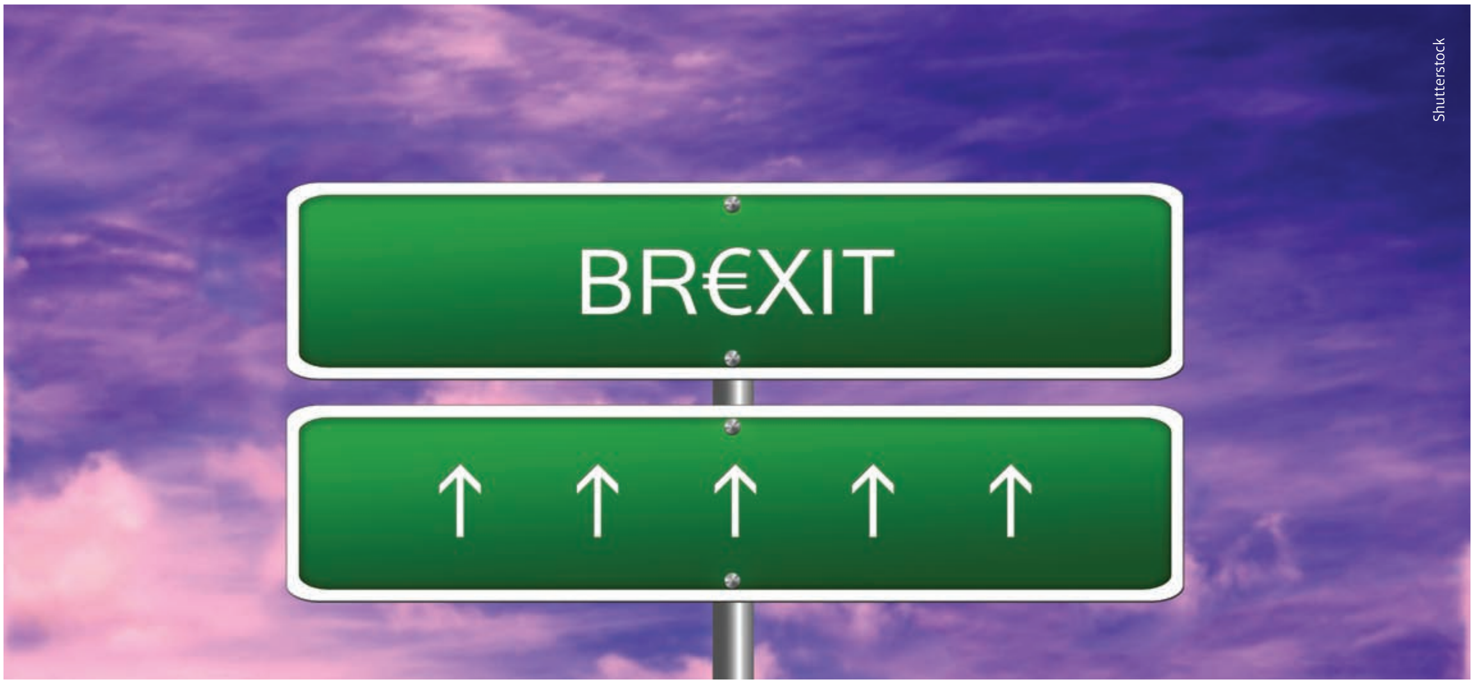
No major transformation

It is doubtless true that either as a part of the EEA or under bilateral agreements with the EU, the UK would be able to negotiate some exemptions from EU employment law. However, the EU would be reluctant to permit 'social dumping' and allow the UK to undercut EU states through lower employment standards (for example, removing paid holiday or scrapping collective redundancy consultation) while remaining part of the free market. The EEA agreement and the agreements with Switzerland allow these countries to access the single market only in return for signing up to significant portions of European law. France and Germany are especially unlikely to allow the UK – as a key competitor and larger economy than the existing EFTA countries – to gain a competitive advantage through free access to the EU market with lower levels of employment regulation.

Clearly, if the UK did scrap all EU-derived employment law and abandoned the free movement of persons, it would have major consequences on UK employers – and on businesses from other EU member states that work in the UK or are in competition with UK firms. However, the relatively minor changes that are, in our view, more likely would do little to exaggerate the already significant differences between the employment law regimes in different EU member states.

In short, even if the UK were to leave the EU, it seems unlikely that UK employment law will be transformed in significant ways.

James Davies *is joint head of employment and* ***Bethan Carney*** *is a practice development lawyer at Lewis Silkin*



RISING M&A STILL UP AGAINST OLD-FASHIONED RISKS

As foreign investors look for new investment opportunities, mergers and acquisitions have flourished in Central and Eastern Europe. However, what are the key business risks presented by such deals?

FOLLOWING THE GLOBAL DOWNTURN AND THE eurozone crisis of 2007-12, M&A activity surged in 2013 and the first half of 2014 in parts of Central and Eastern Europe (CEE) as recovery took root. Furthermore, the recent results of banking sector stress tests conducted by the European Central Bank showed solid results for banks – including their parent institutions – operating in several core CEE countries, notably the Czech Republic, Hungary, Poland and Slovakia.

A resultant expected rise in bank lending to corporates and small- and medium-sized enterprises should have a positive knock-on effect on M&A in the region as foreign investors look for new investment opportunities. This has clear implications for risk management, compliance and due diligence, given that regulatory reform continues in much of the region.

M&A activity in CEE has picked up since 2004, when several countries joined the EU. Despite blips in activity between 2008 and 2012, owing to a sovereign debt and growth crisis in the euro area, M&As picked up noticeably in 2013 and are likely to have exceeded expectations again in during 2014.

The recovery of growth prospects across Europe, greater credit provision, an improvement in CEE infrastructure owing to larger flows of EU funds and the re-emergence of solid levels of foreign direct investment (FDI) have all helped facilitate this trend.

Background

The value of M&A transactions surged by just over 35% in the first half of 2014 across eastern European emerging markets, compared to the same period a year earlier, according to recent estimates. Supporting this positive trend was a large number of deals recorded in Poland and the Czech Republic, which offer two of the largest M&A markets in the region, just behind the front runner, Turkey.

Rising investor interest – domestic and foreign – was apparent in several key market segments, notably real estate, energy, healthcare and telecommunications (including IT). In contrast to previous years, an increase in private equity (PE) investment and greater involvement of private investors from domestic markets signifies a new feature of these latest M&A deals.

Improvements in PE in parts of the region, coupled with better prospects for greater SME financing and government-backed incentive schemes, is good news for foreign investors. Despite evidence of increased domestic M&A originating from a large rate of wealthy local private investors across CEE, an assessment of the country of origin for numerous deals shows plenty of interest from countries such as Germany, the Netherlands and the US.

Two notable deals of 2014 were US-headquartered Henry Schein's acquisition of an 80% stake in Poland's Medivet SA, a local distributor of animal health products, and Deutsche Telekom's purchase of the remaining 40% stake in T-Mobile Czech Republic.

Challenges ahead

M&A, which involves devising growth strategies for newly acquired assets, is always a risky business involving complex deals in particular geographical climes. This is particularly true in CEE countries, despite the gigantic strides made by individual countries to improve institutional flexibility and legal transparency since their accession to the EU in 2004.

Distinct challenges therefore remain for foreign investors looking to buy and sell assets, company shares and target businesses in this part of the world, which is home to unique local market conditions. The prospect of crowding out the marketplace with local investors, overpricing of assets by domestic target companies and ensuring good returns signify just three micro-problems facing the acquiring business or investor. The others come in the form of potentially significant macro hurdles or business risks:

- reputational risk by association (via direct business partners and counterparties);
- corruption risk;
- regulatory burdens; and
- significant levels of state involvement in pockets of the market.

All four areas relate to the buying side of M&A deals and signify business, rather than purely financial, risks. Financial risk is less of an issue, given the relative stability and liquidity of the banking systems in CEE. Yet, all of the areas above have the potential to affect the outcome and growth strategy inherent in M&A deals.

These risks are present in several notable areas, which straddle the political, regulatory and legal environments across CEE, including:

- significant levels of perceived corruption in business and politics;
- in turn, the blurred line between politics and business leads to heightened corruption risk;
- widespread red tape and old-fashioned bureaucratic procedures in business operations;

- heavy administrative burdens arising in part from unnecessarily complex systems of corporate taxation that apply to certain types of businesses;
- clunky legal systems, particularly relating to local courts, which tend to be politicised and bureaucracy-ridden; and
- persistent non-transparency in public procurement procedures, despite the introduction of new laws.

What can be done?

The successful conclusion of any M&A transaction from the buyers' perspective – following the successful agreement of purchase price, legal structure and contractual details of the deal – depends on the correct identification of these salient risks. In this respect, foreign investors entering these markets for the first time can take practical steps to mitigate pitfalls arising from pervasive business risks.

Rigorous due diligence by the buyer on the seller or target business presents an effective method for identifying and managing integrity risks associated with M&A. This is especially the case in CEE countries, where ongoing regulatory reform – which should help streamline contract enforcement, insolvency procedures and tax compliance – is yet to take root.

Due diligence targeted at prospective partnerships, major mergers, acquisitions and joint ventures is a particularly effective tool when it comes to gauging the extent of reputational risk arising from engagement with the management teams of local businesses, as well as the potential risks associated with acquisition targets and third parties involved further down the transaction chain.

When supplemented with in-depth pre-transaction market analysis – this can involve competitor/subsidiary mapping and an assessment of the financial conditions in individual businesses – it provides an overall picture of the regulatory environment, including notable institutional quirks specific to particular countries.

This in turn shines light on otherwise grey areas that impinge on business ethics:

- who are the key decision-makers and how companies are run;
- whether their ownership structures are fully transparent – as is often the case in CEE, parent entities are registered in offshore jurisdictions;
- the level of political exposure to parties, politicians and interest groups operating at the national and local levels;
- whether they have ever faced financial or regulatory difficulties (and whether the target businesses are solvent); and
- whether internal audits are undertaken on a regular basis.

A clear perspective on these aspects of CEE business increases the likelihood of a profitable conclusion to M&A in the region.

Furthermore, a general lack of sophisticated compliance culture in much of the region, owing to an inconsistently rigorous regulatory environment, enhances the importance of due diligence conducted on agents, distributors and other third parties. Targets often have few anti-corruption policies and procedures compared with their western counterparts.

> It is critical the buyer tests what it is being told, through a risk-based review of the books and records

If they do exist, they should be tested pre-transaction to understand the extent to which policies such as third-party due diligence are adhered to and the controls in place to mitigate the corruption risk. This will also help ascertain the requirement for further measures to be put place post-acquisition.

Alongside the discussions with the local management during the due diligence period, it is critical the buyer tests what it is being told, through a risk-based review of the books and records. Sampling of typical red-flag transactions – such as payments to government entities, supply contracts with consultants and entertainment expenses – will give a level of comfort over what is being bought.

TOP RISKS

- Consolidation in the CEE M&A market set to bring heightened compliance risks, despite significant progress made by individual countries to improve institutional flexibility and legal transparency
- Significant risks, including high levels of perceived corruption in business and politics, remain
- Importance of due diligence reinforced by lack of sophisticated compliance culture across much of CEE, owing to an inconsistently rigorous regulatory environment
- Investors must take steps to identify salient risks and mitigate pitfalls across political, regulatory and legal environments
- Rigorous due diligence on the seller or target business proven to be a particularly effective strategy for identifying and managing M&A integrity risks in CEE

Outlook

The outlook is seemingly bright, particularly as pundits continue to expect a deeper consolidation of the M&A market in CEE in the next few years. However, this expectation is subject to certain risks, irrespective of foreign investors following the correct procedures when clinching deals.

The most notable short-term downside risk for further M&A activity, particularly in Poland's case, is a sluggish initial public offering (IPO) market because of a lack of investor demand, despite high expectations at the start of 2014. According to recent estimates, the Warsaw Stock Exchange – the largest bourse in the region – featured only 10 IPOs in the third quarter of 2014. This signifies a significant slowdown compared to the period a year earlier.

Furthermore, headwinds to economic growth arising from a new slowdown in the euro area and the impact of economic sanctions on Russia could also serve to dampen M&A in the near term, particularly as fresh foreign investment originating from Ukraine and Russia continues to fall.

Inward and outward FDI from Russia has been important for growth across a number of sectors, including the Czech industrial base and Hungary's energy sector in recent years. Counterbalancing this, however, is a further expected rise in PE investment across CEE and a renewed bout of privatisation activity in key areas, such as energy and telecommunications.

These factors should help sustain the recent positive increase in M&A activity as some of the largest companies in the region look for new foreign investors in 2015.

Dr Katya Kocourek is a senior associate in the intelligence and due diligence practice of Stroz Friedberg

Up and coming general managers have a new set of priorities for their work-life complexities and businesses overlook this at their own cost

GENERATION 'NO'

FOR THE FIRST TIME, PARTICULARLY IN PROFESSIONAL SERVICES, talented Generation Y general managers are looking at senior partners and articulating with increasing confidence that they do not see them as inspiring role models. They are also sending out the message that their personal lives will not always come second to work.

There is no one-size-fits-all approach to handling the complexities of work and personal life, but if businesses are to survive the western demographic time bomb, where companies fight over a shrinking pool of talent, it must be tackled.

If senior executives fail to create the right work environment for Generation Y talent, they will neither attract nor retain the brightest and the best and company performance will start to suffer.

Despite experts' predictions that many people will now live to the age of 100 and work well into their 80s, a survey by London Business School has discovered that less than half (40%) of senior executives rank their work-life balance as a high priority when considering their development for the next three to five years.

This is in direct contrast to the priorities of their Generation Y employees. Last year, London Business School revealed the results of a five-year survey of participants from its Leading Teams for Emerging Leaders executive education programme. The survey found that Generation Y puts work-life balance at the top of the priority list, leaving promotion prospects in third place behind organisational culture. This is not a bull market but a genuine change in attitude of a generation determined to enjoy the journey.

One explanation is that first-time general managers are most at risk of burnout. The first general management role is exceptionally tough. This stage of life is known as the double crunch as many people start families and their first general management job at the same time.

The demands from work and personal life have never been greater. Added to this, for the first time in their careers, these managers cannot rely on their technical expertise. Their new 18-hour-day roles demand a different set of skills. Their job centres less on what they know but more on how they manage and lead a team and build relationships across the organisation. Added to this, they have genuine accountability and relatively little control, and what starts as quality control all too easily becomes exhausting micro-management.

Although senior executives have survived the middle management years, they would do well to listen to their successors. More than 95% of the senior executives I work with tell me they are 'hurry sick', namely addicted to email and disillusioned with inefficient meetings.

Crises after a missed promotion, redundancy or a death in the family are disturbingly common, prompting them to reflect on their priorities. Realising that they have achieved everything they thought would make them happy, but finding they are unhappier than they have ever been is at the heart of the mid-life crisis. Although not inevitable, it is a disturbing phenomenon that can be observed all too often.

Merely climbing the corporate ladder does not make staff happy and this pattern is not what is going to inspire the next generation of employees to join and stay loyal to an organisation. Individuals almost certainly need to spend more time asking themselves what matters most in their lives.

A retired hospice nurse who spent her entire career looking after people who were dying recently wrote a wonderful book, *The Top Five Regrets of the Dying*. Having spent all this time talking to these people, she says five main regrets emerged: living the lives others expected of them rather than being true to themselves; working too hard; not having had the courage to express their feelings; not having stayed in touch with friends; and not having allowed themselves to be happy.

This question of what matters to a person most in their life is something that everyone has to figure out as an individual. Typically, there are five key areas: relationships, friends, you, health and family. It is important not to lose sight of a significant other, the one person who should still be there when the children have left home. Failure to invest in these key relationships is a common mistake. Spending time with friends is important too, although that does not mean sending a Christmas card once a year. It means regular catch-ups every fortnight or so. Research shows that people who have strong relationships with their friends live longer than those who do not.

It is important to remember oneself too – those things called hobbies and interests that a person used to have. These are the first casualties in the double crunch of work and family. Looking after ourselves and doing the things that help recharge our batteries is critically important. A person may also have a spiritual, community life, volunteering and taking part in other areas that are important to them.

When looking at where work fits into this picture, the problem quickly becomes apparent: work essentially overlaps everything else. The problem is that if someone is serious about their career and they care about their work, work easily explodes the boundaries. Once upon a time, there was a home life, a commute and work. Nowadays, with 24-hour email, that does not exist, and when not careful, work expands. People can now work all the time, even on holiday. Most executives will not book a holiday unless they can guarantee there is wi-fi in the hotel, by the pool or in the ski chalet.

Setting the boundaries

So how can the complexity of work and personal life be managed? First, it should be understood that the concept of a work-life balance is a false dichotomy. It assumes that one is good and one is bad and that they are clearly defined and so can be equally balanced. That, unfortunately, is something of a fantasy.

Boundaries should be created, things in one's life that are non-negotiable. The truth is that no one else is going to look after you. This is not HR's responsibility nor the boss's responsibility; it's each individual's responsibility.

If these non-negotiables are created about all the things a person cares about in their life, it helps to protect their energy. By the age of 40, the choices an individual makes have a permanent effect on the quality and the length of their life. For example, giving up smoking before the age of 40 does not affect life expectancy. After the age of 40, although it is still important to give up, the reality is that, statistically, the person will die younger.

As people get older, the consequences matter. Protecting a person's energy means they are more stable and less susceptible to the type of energy spikes that leave them going to bed tired but wired. Only then can they focus on what matters. All the latest research demonstrates that it is not stress that is the determining factor in wellbeing but the attitude to stress. It is human nature that we underestimate future uncertainty – the number of bumps in the road that will be encountered.

For some people, these bumps will be big. No one can control what happens, but what can be controlled is the response to it. It is the attitude to positive and negative events that determines everything: happiness, longevity and health.

If managing the complexities of work and home life is an individual responsibility, one might ask if companies can do anything to respond to these calls from Generation No for a more balanced life. They can.

More continuous professional development focused on attitudes and mind-set would be a promising start. Most companies reviewing their professional development opportunities would find a heavy weighting towards skills development.

Well-being 360˚ reviews are a good next step. London Business School is rolling out health diagnostics and six-month reviews with participants on its new general management programmes, Transition into General Management and Senior Executives Programme.

Involving employees in determining how best to achieve the company's purpose is also essential. If an employee is not in a fulfilling work environment, it affects every other relationship in their life. A collaborative approach to strategy will encourage people to bring their minds to work and go beyond the minimum.

Ninety percent of good ideas do not come from the executive suite. The senior executive's job is to create a context in which others have confidence and purpose. It might take courage to relinquish the command and control mandate of our industrial forefathers, but organisations are more robust than is generally thought. Millennials more intuitively grasp this way of working and, arguably, they will do a better job of running organisations than the previous generation.

People are always being told to be careful in their careers, to the point where it can feel as though companies are as fragile as china shops. The reality is that organisations are not china shops; they are more resilient than everybody thinks. People have to take risks and, in the words of Mark Twain, "sail away from the harbour".

Richard Jolly is adjunct professor of organisational behaviour, London Business School, and teaches on the school's Transition into General Management and Leading Change programmes for business executives

Stay in touch and join the debate

Connect with us on LinkedIn and Twitter

www.strategic-risk-global.com
@StrategicRISK
www.linkedin.com/groups/StrategicRISK

DIARY

20 April
SR Risk management in the Middle East debate
Four Seasons, Dubai, UAE
The fourth *GR* Executive Briefing will include a 'Risk Management in the Middle East' spotlight-session for the first time. The session will explore the key concerns for risk professionals in the region
bit.ly/193O491

21 April
fastTrack foundation: Administration of insurance programmes
Allianz House, London, UK
CII/IRM
CDP Points: 3 hrs (structured)/5
bit.ly/1Ncf1q7

23 April
StrategicRISK Forum 2015
Four Seasons Hotel, Singapore
StrategicRISK's second yearly Asia conference for corporate risk and insurance managers, chief financial officers and corporate treasurers responsible for risk management and insurance at Asia's largest corporates
bit.ly/1BshmWy

24 April
NARIM congress 2015
The Polar Hall, Utrecht, Netherlands
bit.ly/1GstwV1

26 to 29 April
RIMS annual conference and exhibition 2015
Ernest N Morial Convention Center, New Orleans, US
bit.ly/1CRqqIS

29 April
Developments in Enterprise Risk Management
Madinat Jumeirah Hotel, Dubai, UAE
bit.ly/1GZ5FdE

30 April
Uncertain prospect: the UK 2015 general election
Tower Place, London, UK
This talk will discuss possible outcomes, the implications of the Fixed-Term Parliaments Act 2011, the role the Scottish National Party may play in Westminster and the implications of political instability for policies on the economy, the welfare state, immigration and the EU
CII/IRM
CDP Points: 3 hrs (structured)
bit.ly/1CRloMF

28 and 29 May
AGERS Congress of Risk Management and Insurances
Auditorio Rafael del Pino, Madrid, Spain
bit.ly/1BrYbeo

3 and 4 June
RusRisk Forum
Golden Ring hotel, Moscow, Russia
bit.ly/19ndA9d

TOP TWEETS

1 StrategicRISK tweeted: "bit.ly/1HqlOgo Should #insurers and policyholders turn their backs on #arbitration?@MichelmoresLaw"

2 Lee Knight (@AlgorithmLab): "No, arbitration should be actively encouraged between policyholders & insurers!"

3 Megan Wright (@MeganAlexWright): "Why? The downsides to arbitration are often higher costs and no legal precedents for [insurance] law"

4 Lee Knight (@AlgorithmLab): "Certainly a call for a bigger pool, of specialist insurance mediators & arbitrators!"

WHAT WE ARE DISCUSSING ON LINKEDIN

"What does the future of insurance look like? Lockton's Mike Hammond says the future of insurance is to avoid silo approaches to create insurance solutions for emerging risks. Do you think insurers should take a new approach to emerging risks?"

COMMENT/ANSWER

Airmic chief executive John Hurrell:
"The challenge for the insurance industry is that assets are now more difficult to define or identify. Assets are often intangible, such as brands, IP and technological advantages, and the threats are difficult to predict and manage. For example, insurers write conventional business interruption (BI) insurance based on damage to physical assets in a different department from where they write cyber insurance for cyber-related BI. However, the policyholders do not make this distinction and would prefer to have these risks covered under a single policy to avoid gaps and complications."

TSB Bank insurance manager Emmanuel Fabin:
"A holistic view of emerging and traditional risks is vital. Emerging risks can affect a range of policies, new and traditional. For example, with cyber risk, as an insurance buyer, I want insurers to explain when cyber ends and BI/crime/fraud begin. If an emerging risk could transcend a single policy, it is important to know insurers have a joined-up, clear and robust approach to underwriting and claims management."
Have your say here: linkd.in/1FWIfqL

FINAL WORD

"As an industry, we need to understand not so much the emergence of new risks, but how existing risks may merge into new ones"

Lockton chairman of international operations Mike Hammond