StrategicRISK

RISK AND CORPORATE GOVERNANCE INTELLIGENCE

Summer 2015 Issue 101

www.strategic-risk-global.com

BEYOND THE HORIZON

How the future of risk is shaping the development of the profession


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®

StrategicRISK

Issue 101
Summer 2015
www.strategic-risk-global.com

Editor Mike Jones
Deputy editor Kin Ly
Managing and legal editor Hélène Préchac
Asia editor Jessica Reid
Executive editor, Asia-Pacific 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

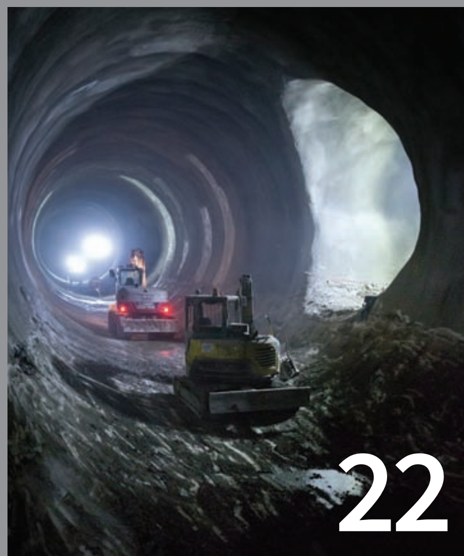
Email: firstname.surname@nqsm.com

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

QUALIFIED BY EXPERIENCE

There is no substitute for the wisdom gained by experience in risk management – but certification may enhance the profession

DESPITE THE increasing use of profiling tools and software technology, the ability to assess and determine risk effectively comes down to how information is interpreted.

The decision-making process relies on the judgement of risk professionals to highlight details, data and discrepancies that enable stakeholders within a business to make appropriate choices.

Some might turn to instinct or intuition, but the skills and wisdom required are generally derived through experience.

A long road

The value of this is being recognised formally by the IRM and FERMA through their certification programmes, which are being launched this year.

Much of the debate around the merit of the FERMA system has centred on how to credit the achievements of older risk professionals without forcing them to sit examinations alongside other relative newcomers to the profession as though they were all final-year university students.

On a flight to Dubai to launch *StrategicRISK* in the Middle East (pp14-15), I spoke with FERMA president Julia Graham, who talked passionately about the federation's new certification system.

Together with the certification project chairman Michel Dennery, Graham has been driving the programme even before the concept was first revealed publicly at the association's symposium in Versailles almost three years ago.

It has been a long road since then to obtain the support and agreement of Europe's national risk management associations, but a general consensus has been reached. FERMA will now give awards to its first founder certified risk management professionals at its Venice Forum.

Advocates of certification maintain this is the only realistic way to achieve the recognition risk managers need and deserve.

A move towards enhanced professionalism will perhaps provide greater leverage and more time with the board.

This is a moot point, but certainly anything that enables greater traction with the stakeholders who are the ultimate decision makers is something that deserves merit.

In this issue, we take an in-depth look at other ways in which the profession is likely to evolve in the future (pp17-21).

Coping with a risk landscape that is continuously moving means risk professionals must also change to enhance their scope of understanding.

Mike Jones, editor

> **"Anything that enables greater traction with stakeholders deserves merit**

Analysis

'Firms must prepare for a reputational crisis like they would for a fire'

As reputational damage was voted the top risk in Aon's *Global Risk Management Survey 2015*, Alain Gravier, risk manager at Française des Jeux, gives his views on how organisations can protect themselves against the risk

> **Firms need to constantly monitor what is said about them and their products on the web, especially social media**
> **Alain Gravier,** Française des Jeux

Reputational damage is a key risk for businesses and risk managers need to prepare for a potential crisis with the same diligence as they would for a fire hazard, according to French national lottery firm Française des Jeux risk manager Alain Gravier.

Gravier was responding to the news that reputational damage was voted the top risk to businesses globally in 2015, according to Aon's biannual *Global Risk Management Survey 2015*.

The survey collated the views of almost 1,500 business leaders from 28 industry sectors, at firms of all sizes in 60 countries across the world. Respondents were asked to rate risks in terms of their threat and reputational damage was considered the most formidable risk globally. In the inaugural survey, released in 2013, respondents identified economic slowdown/slow recovery as the top global risk, while damage to reputation/brand was the fourth highest ranked risk.

The perceived rise of reputational damage as a risk to corporates owes much to the power of social media and 24-hour news sites, according to Gravier.

"In the past five years, social media and 24-hour news have deeply changed the way to prevent and circumvent reputational damage. Firms need to constantly monitor what is said about them and their products on the web, especially social media," he says.

Corporates should appreciate the power of social media and digital technology in spreading negative sentiment towards a brand, company or product, says Gravier and be able to respond quickly if a reputation crisis develops.

"A reputational crisis is like a bush fire: if it is detected early and appropriate action is taken quickly, the firm maximises its chances of controlling the crisis," says Gravier.

"If a firm is too slow to detect and react to a crisis burgeoning, the firm can quickly find itself in big trouble. As with fires, businesses must be prepared for reputational damage to be effective when the need arises."

Although Gravier upholds the importance of reacting quickly to a reputational crisis, he says responding appropriately is of equal importance, but finding the right balance is difficult.

"Five years ago, a firm had time to build its response [to a reputational crisis] by working with its legal team for example, but the growth of social media does not allow for the same time to plan a response," he says.

"However, sometimes in a crisis, it is better to wait to answer correctly and this also applies in the age of social media."

Creating a dialogue

Establishing a dialogue with industry stakeholders and influential bodies is an important step firms can take to manage a reputational crisis before it occurs, says Gravier. Furthermore, he says businesses should have an open dialogue with clients and customers on social media to improve the chances of stopping negative sentiment towards the brand from spreading further.

"Expressing the company's views publicly on issues related to the firm, its services or products is now well demonstrated by most large business-to-consumer companies. I am not so sure that B2B companies have the same awareness or ability, but they should," adds Gravier.

Elsewhere in Aon's report, cyber risk entered the top 10 for the first time as the ninth most formidable global risk, which Aon chief innovation officer Stephen Cross says could be linked to the rise of reputation damage.

"It is little surprise to see cyber risk enter the top 10 at the same time there is increasing concern about corporate reputation because the two issues are a great example of the interconnectivity of risk," Cross says. SR

EU adopts stronger rules to combat money laundering and terrorism financing

The package will ensure full traceability of funds transfers within, to and from the EU

In May, the European Parliament, voted to adopt new rules to help fight money laundering and terrorist financing. This marks the final adoption of the EU anti-money laundering package.

Věra Jourová, the EU's commissioner for justice, consumers and gender equality, said: "Serious and organised crime is driven by profit – tracing the illicit proceeds of crime back to the criminal networks is essential both to detect, prosecute and dismantle those networks and to seize and confiscate their criminal wealth. The rules adopted [last month] will help us follow the money and crack down on money laundering and terrorist financing."

The new anti-money laundering framework aims to fight terrorist financing and money laundering by:

- facilitating the work of Financial Intelligence Units from different member states to identify and follow suspicious transfers of money and facilitate the exchange of information;
- establishing a coherent policy towards non-EU countries that have deficient anti-money laundering and counter-terrorist financing regimes; and
- ensuring full traceability of funds transfers within, to and from the EU.

Commenting on the announcement, Chrisol Correia, director AML Global, at LexisNexis Risk Solutions, said: "The endorsement of the fourth Anti-Money Laundering Directive is to be welcomed. It is certainly a positive development and will hopefully provide financial and other obligated institutions with further direction and support on tackling money laundering and its predicate offences, including tax evasion and terrorist funding. Nonetheless, the real work will be starting soon as member states transpose the directive into national law. How each member state enforces the directive and how the forthcoming registers of beneficial ownership will function across national boundaries in particular is a really interesting issue to watch and one that may pose a major compliance challenge.

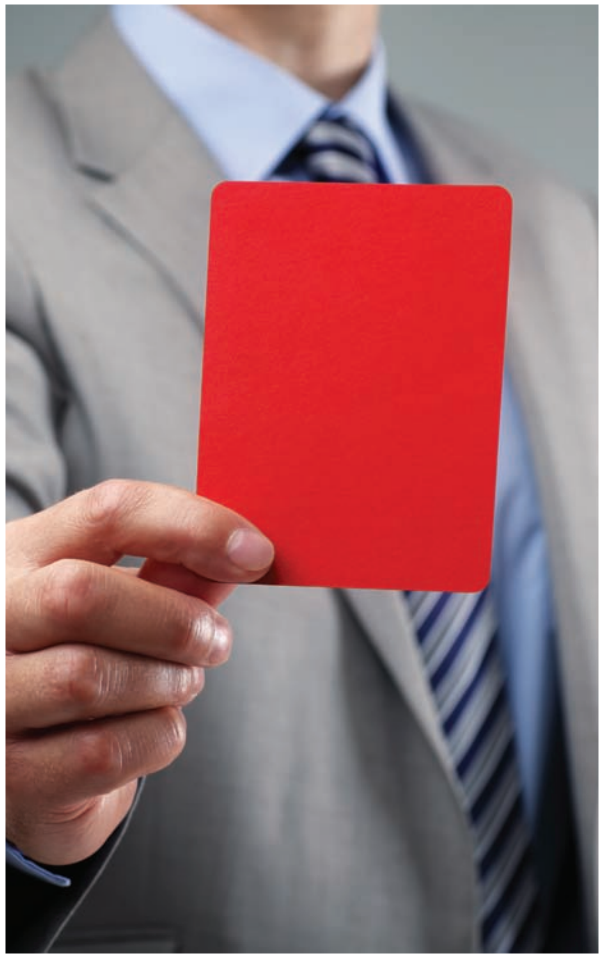
From the UK perspective, the biggest impact, in my view, will be on the commercial and residential real estate sectors, especially in London. This is a sector that is not only subject to major capital inflows of foreign capital, but also one that perhaps does not have the same compliance tradition or existing capabilities as say the banking sector. There will be major change and investment ahead and many estate agents and the organisations that support them will have to upskill very quickly on the basics of KYC and tracing the source of funds to be compliant with the directive and resulting national legislation." **SR**

> **"Tracing the illicit proceeds of crime back to the criminal networks is essential to detect, prosecute and dismantle those networks**
>
> **Věra Jourová**

Analysis

Moore Stephen's Tackling Financial Crime whitepaper spells out the dangers to brokers if they do not invest in personnel to mitigate financial crime

Brokers face millions in fines if they fail to invest in compliance and audit functions



Insurance brokers are paying a heavy price for failing to meet Financial Conduct Authority (FCA) standards on financial crime risks, according to a new whitepaper released in May by global accountancy and consulting network firm Moore Stephens International.

The whitepaper, *Tackling Financial Crime: How insurance practitioners can ensure they are doing enough*, cites findings from an FCA thematic review published in 2014 that concluded "most insurance intermediaries did not adequately manage the risk that they might become involved in bribery or corruption".

> "Firms should have a clear governance structure, which includes regular committee or board meetings

The review published fines issued to three global brokers between 2009 and 2014. Willis was fined a total of £6.89m (€9.52m), Aon was fined £5.25m (€7.25m) and JLT paid £1.88m (€2.6m) for breaching anti-bribery and corruption (ABC) regulations.

In its analysis of the thematic review, the whitepaper found that firms were failing to invest in resources required to mitigate financial crime risks, often owing to budgetary constraints. As a result, companies have incurred substantial FCA fines for not complying with ABC regulations.

The report suggests that brokers should invest in resources for compliance and audit functions to enable effective risk management. However, it says that cost restraints are often cited as "a barrier to employing sufficient personnel", but concludes that: "failure to appropriately resource an oversight function not only demonstrates a lack of understanding of the risks involved but also has been shown to be a false economy, as can be seen from a number of regulatory fines and skilled persons reviews".

Improvements required

In addition, the report identifies a number of structural improvements companies should make to ensure they meet FCA standards on ABC, anti-money laundering (AML), counter-terrorist financing and sanctions, systems and controls. Appointing a board member as money laundering reporting officer was one recommendation from the report.

The report states that financial crime controls are more likely to be effective when "the executive, senior manager and all staff have a clear insight into their client base, market, transaction activity and changes within the regulatory environment, as well as sanctions lists, Financial Action Task Force reports and money laundering requirements.

"To demonstrate that appropriate governance arrangements are in place, firms should have a clear governance structure, which ideally includes regular committee or board meetings to discuss risks, including AML, ABC and sanctions risks. These meetings should be supported by good quality management information, which contains sufficient granularity to enable senior management to properly discharge their functions." SR

Is cyber security at third-party vendors a threat to your business?

Although firms know they should take their own cyber security seriously, they often overlook the one at third parties

As organisations have become increasingly aware of the significant legal and business risks posed by cyber security breaches, they have begun to devote substantial resources to identifying and eliminating internal vulnerabilities and to mitigating their exposure resulting from potential cyber security incidents. Organisations have found they must address cyber security risk management from multiple angles, including investing in robust IT security systems, conducting employee training, considering the purchase of cyber security-related insurance policies, developing a data breach response plan etc.

An important, but sometimes overlooked, element of that process is third-party risk management. At a speech in February, Benjamin Lawsky – the superintendent of the New York State Department of Financial Services, which regulates many global financial institutions – observed that "a company's cyber security is only as strong as the cyber security of its third-party vendors".

Below are some of the issues organisations should consider in seeking to mitigate their cyber security risk in connection with third-party service providers.

Take stock of existing vendor relationships

A first step is to ensure that your organisation has a complete understanding of who has access to what data. Does your organisation store information in the cloud? Does your organisation use a vendor to host its website? These days most, if not all, organisations provide some kind of data or systems access to at least some third-party vendors, whether the vendor be a law firm, a business consultant, a data storage provider, a printing services provider, a payment processor or even the manager of an office building's HVAC systems.

Limit access and segregate data

Although it may be necessary to share some data or systems with outside vendors, such access should be only a need-to-know basis. The well-publicised and very costly credit card data breach recently experienced by Target Inc started with the theft of credentials granted to Target's HVAC vendor, Fazio Mechanical Services.

The attackers infected the vendor with general purpose malware through an email phishing campaign.

While many lessons can be gleaned from Target's misfortune, one of the most obvious is that the compromise of an HVAC vendor's credentials should never have led to the compromise of payment system data.

Review existing contracts

A well-designed contract will serve as a crucial foundation for a relationship with third-party vendors. If it has not already done so, your organization should review existing vendor contracts with an eye towards mitigating cyber security risk. A number of contractual protections might help to manage such risk:

1. consider extending your own security standards to vendors. Contracts can include provisions requiring vendors to comply with specified security procedures
2. consider requiring the vendor to make representations or warranties regarding its cyber security practices or authorising your organisation to conduct audits regarding the vendor's ability to meet and sustain your security expectations
3. require that the vendor provide timely notification of any security incidents that it experiences. Such a provision might also define your organisation's rights to control any responses or disclosures to third parties in the event of an incident
4. control and limit downstream transfers of your data
5. require the vendor to destroy copies of your data in the manner you specify on termination of the relationship
6. consider how to allocate liability through indemnification provisions or limitations on liability based on the nature of the relationship and the sensitivity of the data involved
7. consider requiring the vendor to maintain cyber security-related insurance coverage. Relatedly, organisations should consider whether and to what extent data breaches stemming from third-party vendors fall within their own insurance coverage.

Develop a vendor management plan

After reviewing existing contracts, a firm should consider whether such contracts can and should be renegotiated. Additionally, the organisation should develop guidelines for future contracts. These guidelines may include standard provisions such as those described above and may also aim to structure the analysis of when the benefits of outsourcing outweigh the associated risks.

The fact that Target's breach originated from a third-party vendor did not prevent Target for incurring enormous losses in the form of, among other things, litigation expenses and lost customer confidence. For that reason, the primary goal is to prevent an incident. If, however, an incident does occur, the robustness of an organisation's procedures and practices with regard to third-party vendors could help to limit its liability in subsequent litigation, which could include a shareholder suit against directors and officers or a customer or employee data privacy suit, or regulatory scrutiny.

Indeed, regulators have begun to place increasing scrutiny on third-party relationships in the context of cyber security. For example, the New York Department of Financial Services will now examine banks within its purview on, among other things, their protocols concerning the cyber security of third-party vendors.

Moreover, organisations should expect scrutiny regarding this issue to continue to increase.

Scott S. Balber is a partner and US head of investigations and financial services litigation and John J. O'Donnell is a partner in the New York office of Herbert Smith Freehills LLP

Analysis

A step into the unknown

The result of the UK general election has provided a boost to business, but dangers remain ahead

It was meant to be the closest election in living memory, but when the British public voted in the May parliamentary election, they delivered an unexpected decisive verdict.

Months of conjecture about the inherent dangers of a hung parliament and speculation around which party could break down the necessary political barriers to secure itself a viable and stable coalition came to nothing.

Instead of an impotent stalemate, David Cameron's Conservative Party defied the predictions of opinion polls to secure enough seats to rule with a small working majority that should just about hold firm for five more years.

> **'The Conservatives' political agenda is a risky one that threatens to partition not only the UK from the EU, but also divide the country'**

Experts across the political spectrum considered that such a result was highly improbable, but their views were contradicted spectacularly by the first exit poll prediction moments after voting stopped at 10pm on 7 May.

Although some pundits scoffed in disbelief and sought to discredit the poll, the City needed no further persuasion. Its relief was palpable and immediate. Within seconds of the prediction being released, the prospect of a Conservative majority propelled sterling almost two cents higher against the dollar after weeks of downward pressure.

When the UK stock exchange opened the next morning, the uncertainty that had drifted for weeks around the markets like a choking fog lifted and so did the mood of traders of all persuasions. Currency, equity and bond markets all moved in a sharp upward trajectory.

Concerns about political deadlock removed, the Conservatives are now free to continue their growth through austerity economic programme with renewed vigour. This has been credited with giving the UK fiscal stability after the global financial crisis and won praise from the International Monetary Fund for laying secure foundations for the UK's economic future. However, it has also been criticised by opponents, who cite the cutbacks as being too restrictive, socially divisive and an inhibitor to genuine economic development. Moreover, more spending cuts are forthcoming – even deeper this time.

Market jitters alleviated, some wider risks for companies operating in the UK also eased after the election. The main opposition Labour party, which was routed at the ballot box, had threatened greater regulation and increased taxation for companies, with those under non-UK ownership coming under particular scrutiny.

The majority of firms believe they can now look forward to an economy that, for the time being at least, continues to strengthen and prosper.

However, such optimism might have to be tempered in light of other concerns that already cast a shadow over the UK beyond the term of the current parliament. For the Conservatives' political agenda is a risky one that threatens to partition not only the UK from the EU, but also divide the country.

In or out referendum

The UK has long been an outsider within the EU – detached by geography and, increasingly, ideology. It is understandable therefore that the Conservatives' win was met with dismay in many European capitals, for it effectively initiated a debate that will decide the UK's role and future in the EU.

Two years ago, Cameron promised the British people the opportunity to vote in a referendum to decide whether the country remained part of the EU. This referendum would, he pledged, take place in 2017 provided the Conservatives won the 2015 elections, which they now have.

Ahead of any referendum, Cameron has vowed to restore to UK government control certain decision-making powers from Brussels, particularly around immigration and the welfare rights of migrants. These are controversial and complex issues. Nonetheless, Cameron's stated aim is to secure enough concessions to convince the British electorate that remaining in the EU is in the UK's best interest. Should Cameron get the powers he demands he has vowed to campaign for the UK to remain part of the EU "with all my heart and soul". Failure to do so cannot be an option for Cameron but it remains a possibility.

It is a high-stakes gamble from Cameron for a number of reasons. First, there is no guarantee Britain's EU partners will agree to his demands and cede control of anything – particularly given the rapid timescale for negotiation proposed by the British government. Some of the changes go to the core of the EU's central values in terms of freedom of movement, for example. The proposals also beg the question

of why the UK should be given special status when many of the issues at stake are as divisive in other EU countries. If the UK is granted privileges, other nations might demand concessions of their own and what does this then mean for the future of the EU, particularly given the continuing problems around the Greek economy?

Even if Cameron wins back some control of the powers requested from Brussels, this might still not be enough to convince British voters to remain in the EU. The United Kingdom Independence Party (UKIP) might have won only a solitary seat in Westminster in May, but it received more than 12% of the votes.

It is hard to tell from the results of an election, where many issues are at stake, how much the UKIP vote was driven solely by its opposition to the EU, but this vote indicates that Cameron might not get the referendum result he seeks, particularly since many members of his party are eurosceptic as, indeed, are many Conservative voters.

Chastening experience

A Britain out of the EU would be a disaster for both sides economically, particularly from a business perspective, as although it might open up new markets, it would impinge on the UK's ability to operate with its largest trading partner.

UK business leaders estimate that the country's EU membership adds about £100bn per year to its economy; a figure that cannot be ignored but is seldom discussed by the wider public whose opinions on the EU are often shaped by concerns over immigration, human rights and rules over whether eggs can be sold by the dozen

With a right-wing populist media driving much of the anti-EU rhetoric, it is difficult to predict which way a referendum might go.

Cameron would be wise to learn from the chastening experience of last year's referendum on Scottish independence, which saw the people of Scotland vote narrowly in favour of remaining part of the UK. The British prime minister had banked on such an outcome being relatively straightforward and this resulted in a campaign that was complacent – some might argue, almost negligent. It allowed those supporting independence to take control of the narrative to such an extent that the nationalists almost won and continue to dictate the agenda despite being defeated.

Although the nationalists failed to achieve independence, they reinvigorated Scottish nationalism and remain a thorn in the side of Cameron's Conservatives. In the May general election, the Scottish National Party (SNP) won almost all the Scottish seats and increased its representation in Westminster from six to 56. This astonishing performance makes the SNP the third largest party in the UK by the number of seats, if not by percentage of votes.

In a sense, Cameron has some cause to be grateful for the SNP fervour because it prompted many people outside Scotland to vote Conservative to thwart an SNP-Labour alliance that looked the most likely government in the run-up to election day.

It is doubtful that Cameron will show much gratitude to the SNP for this, but he will be forced to deal with the party's demands at some stage.

One-nation Conservative

Even with his new administration in its infancy, Cameron was facing pressure to give Scotland more control of its affairs with members of parliament from his party urging him to "call the SNP's bluff" and grant Scotland full fiscal autonomy. Although the British government has ruled out such a move, the power of the SNP is now so strong Cameron is likely to be forced to agree to another independence referendum sooner rather than later.

The SNP has proved to be extremely skilful at mobilising its supporters and may well succeed in a second poll, which would end a union that has lasted more than 300 years.

Once again, such a vote would raise serious questions for businesses on both sides of the border.

Cameron, of course, is aware of many of the dangers ahead on the path he has chosen to follow. This is why in his first speech following his election victory, he spoke powerfully about being a "One-Nation" Conservative.

"I want to bring our country together, our United Kingdom together, not least by implementing as fast as we can the devolution that we rightly promised and came together with other parties to agree both for Wales and for Scotland," he said. "In short, I want my party, and I hope a government I would like to lead, to reclaim a mantle that we should never have lost: the mantle of One Nation, one United Kingdom."

The message was clear to the British public and also to those in his party that the country is better served by staying together. Whether Cameron succeeds or rips Britain apart remains in question. This is a genuine political, economic and business gamble in which the risk of losing is all too real.

Mike Jones

Viewpoints

Frédéric Desitter, director of enterprise risk management, Sidra Medical and Research Center

A MAN ON A MISSION

After developing risk management at various leading European outfits, Frédéric Desitter, the director of enterprise risk management at Sidra Medical and Research Center, is now promoting the discipline in Qatar

THE ECONOMIC AND INDUSTRIAL BOOM IN QATAR HAS had positive repercussions for local corporate risk management. Indeed, in the past few years, a new wave of expatriates – risk managers from risk-mature Europe – has moved to the country to build robust risk defence programmes and introduce complex and systematic ERM frameworks to the many new corporations and industries being established as the country seeks to diversify its economy.

Among them is French-born Frédéric Desitter, who has almost 20 years of risk management experience across several sectors, from oil and energy to airport installations.

A self-confessed missionary for the discipline, Desitter has been at the forefront of pioneering risk frameworks and promoting standards in the less risk-mature Europe of the 1990s and early 2000s when the concept of ERM first emerged. Of all his achievements during ERM's formative period, his seven-year stint at UK-based consulting firm, Euro Log from 1997 and three years at Aéroports de Paris from 2008 are particularly telling of his ambition and passion for risk management.

At Euro Log, Desitter worked on billions of euros-worth of contracted deep offshore oil development projects for oil multinational Total. The project was to secure several massive floating oil platforms off the coast of Angola. Each project was worth upwards of $5bn (€3.67bn), with drills operating at sub-sea depths of 1,300m (BP's disastrous Macondo oil well in the Gulf of Mexico operated at about the same depth). The project was the first of its kind and with a sound risk management plan, Desitter helped Total to meet its objectives. That risk plan eventually became the company standard and was spun out to Total's contractors globally.

Before moving to Qatar, Desitter worked for Aéroports de Paris, which is responsible for developing and managing the Paris airports. He had to design and implement its ERM system from scratch. He drew up the company's first risk map, established a collaborative and transparent risk culture, and led the 25-strong risk team to manage efficiently the myriad potentially costly risks that can affect international airports, from operational to strategic threats.

Now entering a new challenge in his career, Desitter will again face the onerous task of constructing a holistic and culturally compliant ERM structure for the developing Sidra Medical and Research Center in Qatar's capital, Doha.

A new challenge

Desitter's new position as Sidra's director of enterprise risk management, will perhaps be the most challenging role of his career to date. This is not least because Sidra is a new company with an ambition to establish itself as a world-class medical centre that will set standards for patient care and help improve the region's healthcare system, but because risk management and, in particular ERM, are in their infancy in the region. ERM in the Gulf Cooperation Council (GCC) countries has, until recently, existed only as a theory, discussed by insurance professionals, but with few corporations putting it in practice.

However, like Desitter, large and new corporates in Qatar are preparing an action plan to propel risk management from backroom discussions to the fore of company objectives, with fully fledged, integrated risk defence operations in the form of ERM. "There is a strong will among new and large businesses to establish ERM programmes to manage their portfolio of risks," says Desitter.

"When I was considering moving to Qatar three years ago, numerous businesses were looking to hire risk professionals to lead their newly created risk functions and drive ERM. This was certainly the aim for semi-governmental organisations in aviation, energy and education, for example.

"Businesses here want to put in place what they consider is best practice in corporate governance and they want to adopt the types of governance and risk management principles found in many businesses in Europe.

"However, at the moment, ERM is new here. When I talk to business people in the region, conversations about ERM can often be rudimentary and much time is spent defining what an ERM framework is before getting onto the benefits and logistics of building such a programme.

"Businesses are more familiar with project risk management [practices used predominately in the construction sector], but not ERM."

In simple terms, the difference between ERM and project risk management lies in the entity to be protected: a project or a business. For more context, the UK-based Project Management Institute defines project risk management as a framework that aims to prevent threats or uncertain events from bringing a project's objectives to fruition, such as those that could harm, for instance, cost, quality or schedule.

ERM, on the other hand, is a system that protects the entire company from myriad risks and is defined by the US risk management association, RIMS, as: "A strategic business discipline that supports the achievement of an organisation's objectives by addressing the full spectrum of its risks – [from financial, operational, reporting, compliance, governance, strategic, reputational] – and managing the combined impact of those risks as an interrelated risk portfolio." ERM is known for bringing benefits such as a holistic view of risks and cultivating a risk-focused culture throughout the entire organisation.

ERM strategy

So what does it take to develop the latter in Qatar? From the many lessons Desitter learnt in Europe when ERM began to surface as a solution to enterprise-wide risk resilience, the key, he says, is to "keep the message simple".

"When I started working as a risk manager in France, no one knew what risk management involved. The challenge in Qatar is the same as it was for Europe when ERM came into the limelight, namely convincing chief executives that a systematic and integrated risk framework is beneficial and will add value.

"Risk managers, even the most experienced, cannot arrive at an organisation in which a risk function does not exist and expect to go from nothing to having the best-in-class ERM programme in only a few months. The key is to keep the message simple and to start the ERM build by understanding the main areas of interest of the board and chief executives. This information should be used to make quick-wins, offering the board ERM solutions to its concerns.

"Risk managers should work on the board's main business concerns and devise a risk plan to prevent and mitigate these risks first. Once the executives and other colleagues have seen that their concerns have been adeptly addressed, risk managers can then begin to work on other risks that were not originally on the agenda.

"Risk managers need to phase in the development and gradually increase the scope of ERM to embed it in the organisation's operational and strategic processes."

Having the opportunity to "phase in" ERM and "be involved in risk management early on in a new company" is part of the attraction of working in Qatar, according to Desitter. Local risk appetite is healthy and a new community of risk managers is taking advantage of every chance to drive forward the discipline. A formidable force in the making, these risk managers could, in years to come, be known as the risk professionals responsible for producing best practice in risk management. Perhaps the next step is to establish a Qatari risk management body to join the likes of RIMS in the US and FERMA in Europe. The opportunities are certainly there. Kin Ly

TOP RISKS FOR QATAR

1. The rapid pace of development is one of the key risks. Numerous large construction and infrastructure projects are taking place across the GCC – developments of new cities and rail links for instance, as well as the high-profile builds in the exhibition site for the World Expo 2020 event in Dubai and the stadia for the World Cup in 2022 in Qatar. This has created tough competition for resources, both in terms of materials such as steel and cement but also competition for skilled workers. Delay in receiving supplies could affect the completion date of these projects.
2. Further, infrastructure particularly roads and ports, are still being developed. This can create challenges in terms of getting supplies delivered in time and of running logistics smoothly.
3. Regional political instability. The crisis in Syria, for example, could deter workers from moving into the Middle East.

Greg Case, president and chief executive, Aon

MAKING THE CONNECTIONS

President and chief executive Greg Case reflects on the findings of Aon's *2015 Global Risk Management Survey* and considers how the interconnectedness of risk requires strategic change among businesses

ONE THING IS CERTAIN ABOUT TODAY'S GLOBALISED economy: no company or country can afford to operate in isolation. It is also clear that not every company or country is ready for the complexity that comes with globalisation. The days of unencumbered growth from simple cross-border mergers and acquisitions have been replaced by the hard reality of managing global supply chains. The blue-sky rhetoric of promising trade agreements has also given way to the long-term challenges of regulating increasingly interdependent economies.

There is no question that globalisation offers tremendous potential in terms of international partnership, technological innovation and business expansion. However, it also has a multiplier effect, significantly increasing the magnitude, complexity and speed of risk. When I meet with our clients around the world, this dominates the conversation. They understand the promise of globalisation, but are mindful that the risks are greater than ever before.

There is no question the risks our clients face – traditional and non-traditional – are growing, but the pace of change is also greater, and the interconnected nature of risk is unparalleled. A natural disaster such as the earthquakes in Nepal can have a tangible impact on operations, but a cyber attack could be as instant – and ultimately, much further-reaching – with a sustained impact on intangible assets such as corporate reputation.

As the leading provider of risk and human resource solutions, Aon appreciates the challenges these issues create and the opportunities as long as they are properly addressed. This is why Aon continues to invest in industry-leading analytical capabilities. We believe our clients are managing through an era of unparalleled complexity, and we are committed to helping them to better understand the new dimensions of risk.

In keeping with that commitment, Aon recently released the results of its *2015 Global Risk Management Survey*. Conducted in the fourth quarter of 2014, the survey gathered input from 1,418 respondents at public and private companies of all sizes around the world. Predictably, the results of this work reinforced our belief in the interconnectivity of risk. The survey also highlighted the importance of alignment between perceived risks in senior management [the C-suite] and actual priorities being addressed by risk managers.

The Interconnectivity of risk

In this year's survey, Aon's global clients selected damage to brand and reputation as a top concern across almost all regions and industries. This ranking can be attributed to the growing challenges businesses are facing from the risks found elsewhere on the top 10 list, including cyber risk, business interruption, property damage and the failure to innovate.

> 'The increasing complexity of risk management requires its integration into strategic planning and regular collaboration'

With 24-hour news cycles and the advent of social media, when an organisation faces a significant crisis event – whether a data breach, product recall or leadership change – public scrutiny is magnified and public trust threatened, thus instantly compromising the organisation's hard-earned reputation.

Given the growing number of major data breaches in the past 24 months and their widespread reputational impact, it is of little surprise that cyber risk entered the survey's top 10 for the first time ever this year, at number nine. Recent high-profile breaches at global companies such as Sony have demonstrated the real damage posed by the interconnectivity of risk. Every company faces these challenges, and it is a question of when – not if – they will be forced to address them.

Aon helps organisations of all sizes to manage cyber risk. We work side by side with our clients and market partners to address capacity needs, but we do not stop there. We are also helping clients to understand the root causes of security breaches and ready their organisation to protect its reputation in the event of an incident. Our cross-functional approach is designed to reinforce IT security, strengthen data and privacy policies, develop training programmes to improve monitoring and accelerate response plans in the event of an attack.

The evolving role of risk management

This year's survey also reveals a surprising disparity in the respective concerns of C-suite leaders and risk managers. Aon's clients' senior management teams readily identified financial and economic risks – including commodity prices, economic slowdown and technology failure – as most damaging, while their risk managers identified liability-related risks such as cyber, property damage and third-party liability.

This lack of alignment illustrates a potentially alarming gap between strategic priorities and tactical realities. The increasing complexity of risk management requires its integration into an organisation's strategic planning process, and demands more regular collaboration between senior leadership and the risk-management function.

For example, many of our clients use financial structures such as captive insurance vehicles and multinational pools to manage their global risks. That number grew to 18% of respondents this year, up from 15% in 2013 – and that trend is expected to continue. These sophisticated solutions have many benefits, but they also underscore the need for risk managers to work more closely with company leadership to ensure everyone understands which risks are being retained, and which are being transferred.

It is also important that senior management recognise the growing importance of people risks. This year, the failure to attract and retain top talent and the failure to innovate both landed in the global top 10. There is no question that organisations are under intense pressure to nurture the ingenuity and maximise the potential of their people.

The survey results reinforce the fact that companies that cannot appropriately align and incentivise their workforce will quickly lose ground to the competition. That perspective was most acute in North America and the Asia-Pacific region, where clients ranked failure to attract and retain top talent as the second most significant risk, behind only brand and reputation.

As leaders in human resource solutions, our team at Aon understands that connection, and uses insights from industry-leading research, such as its *Top Companies for Leaders* report, to help our clients understand that growth strategy begins with talent strategy.

The findings of the *2015 Global Risk Management Survey* reinforce that Aon's clients – across the finance, risk management and human resources functions – will have an increasingly important seat at the table as their companies wrestle with the massive opportunities and inherent complexities that come from further globalisation. As they are being asked to play increasingly collaborative and strategic roles within their organisations, leading brokers will be judged by their ability to supplement their traditional transactional role with more nuanced insights into the interconnected nature of the risks their clients face.

This is why Aon is so committed to investing in its data and analytics capabilities. The company believes its ability to help clients recognise and prepare for the growing speed, magnitude and complexity of risk is directly connected to their ability to achieve their business goals.

Learn more about the findings in Aon's 2015 Global Risk Management Survey, *and the interconnected nature of risk, at http://www.aon.com/2015GlobalRisk/default.jsp.*

Events

DRIVING GROWTH IN THE MIDDLE EAST

Risk professionals discuss their concerns and professional development at a panel marking the launch of *StrategicRISK* in the Middle East

THE MIDDLE EAST AND NORTH AFRICA (MENA) region has witnessed phenomenal growth in recent years. Oil and gas might have fuelled, in every sense, the initial boom, but they are no longer the sole economic driver.

Diverse economies abound across the region, with finance, construction, transportation and tourism being some of the many sectors currently bolstering expansion of the Gulf Cooperation Council (GCC) states of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE).

Many global corporations have long-established operations within GCC nations, but these countries are also home to a range of thriving domestic enterprises. Sometimes government-owned, they often represent enormous business entities, by any measure.

Hot topics

Operating within this mixture of international and regionally owned commercial enterprises is a growing and highly motivated group of risk professionals, comprising both expatriates and Middle Eastern nationals.

In April, some of these attended a panel discussion hosted by *StrategicRISK* in Dubai as part of the launch of this publication in the Middle East. The panel comprised respected and influential risk professionals from the GCC, with a range of experience between them: Scott Saunders, risk and compliance manager at Qatar Foundation; Andrew King, head of claims, MENA, at Aon; Mostafa Ramzy, senior enterprise risk management expert at Emirates Nuclear Energy Corporation; and Amair Saleem, director, safety, risk, regulation and planning department at Dubai's Roads and Transport Authority (RTA).

Saleem was named 'Risk management professional of the year' at the Institute of Risk Management's 2015 Global Risk Awards, while Ramzy collected the award for Building Risk Management Capability at the event. Such recognition is testament to how far risk management has progressed in the Middle East.

FERMA president Julia Graham also joined the panel, lending an international perspective to the topic. The aim of the discussion was to highlight some of the primary risks facing businesses in the Middle East, now and in the future, and also to assess the profession's development within the GCC.

Although there was a broad consensus regarding the risks themselves – geopolitical issues, governance and the growing complexity of risk in general – several issues came under scrutiny. Careful to emphasise that "a region cannot be treated as a country", Graham highlighted water scarcity, supply chain and cyber as her top three risks. Saleem spoke of the increasing threat of regional terrorism, "now that we are becoming involved in regional conflicts".

Linked to this, King cited staff safety and security, broadening the scope to encompass other human-capital issues: "There is a lack of talent in the region in terms of getting enough people into a business to take it forward. There is also a lot of competition for good people and this is driving the crisis."

King also cited reputation as an increasingly prominent risk: "Risk managers are very worried about damage to their brands and their reputation," he said.

The business of reputation

Part of the reputational issue in MENA is that "expectations here are very strong," said Saleem.

He also raised the issue of the pace of change as having potentially serious business ramifications. MENA has enjoyed impressive growth in the past 40 years, but the speed of that change also generates particular risks.

"To keep pace with this [evolution] is a challenge. Technology is also changing rapidly, so inherent risks are embedded in projects related to this."

As head of risk for Dubai's RTA, Saleem said he was operating "very much in a project environment", and "a lot of [my company's] risks are focused on project delivery issues".

Business continuity is another danger that greatly concerns risk managers, according to King.

However, in Saunders' view, not every MENA country is advanced in terms of dealing with this threat. "Business continuity is a discipline that is gaining more and more attention in Qatar. There are many different models demonstrating where business continuity management (BCM) fits within an organisation. At Qatar Foundation, BCM sits within the risk group and we look at it as a mechanism to ensure the foundation can recover from unexpected disruptions."

Dubai's RTA is an example of where business should be going with BCM, according to Saleem: "We have incorporated our business continuity function and our risk management function into one department to make plans for unusual circumstances. We also have an accident investigation group that looks back at causes and then feeds into the risk management function."

Not just a tick box exercise

Risk management culture was considered by Ramzy to be a major concern. Although risk professionals operating within the GCC are generally highly skilled, greater understanding within the business of the need to manage risk is also required.

"Risk management should be embedded in the decision-making process so that no decisions can be taken without proper risk management being in place," Ramzy said. "A change of mindset is also required to understand that risk management is not only a tick box."

However, change is happening and is being driven from the top – at government level – in several GCC countries."The Qatar national vision includes risk management, and it has been fantastic to have this document and be able to reference it," Saunders said.

The effectiveness of the government commitment is being seen. "I started work in Qatar eight years ago, and the risk-management system in place now, compared with how it was then, shows exponential growth," said Saunders. "Qatar Foundation put in place a maturity model several years ago that was designed to measure how an organisation could get from where it was at a certain point, to where it wanted to be in four or five years' time. That maturity model has been used as a measure of progress."

The UAE is similar, agreed Saleem. "The government feels strongly about risk management and local authorities have been engaged in a 'programme of excellence' framework for some time. This incorporates elements of risk management, business interruption, business continuity and crisis management," he said.

King said government endorsement was crucial: "It helps that rulers are mandating this – that is a powerful tool." In addition, he said, foreign businesses were also driving change by "insisting that companies they deal with have a properly developed risk management framework".

He added: "Financiers are bringing their expertise to the table to make sure that all of the risk management framework and the insurance placements are available. Since the recession, they have been insistent that this risk management understanding is put in place."

Ahead of the curve

Raising the profile of the profession is another way to increase the understanding of risk management and FERMA is hoping to achieve this through launching its new certification programme in Europe in October.

FERMA president Graham said the programme would be available outside Europe when the association was ready: "There is a lot of interest in other parts of the world and FERMA would be delighted to talk to colleagues in the Middle East because [risk management] is a global subject. FERMA represents 22 different associations in 20 countries, which can have different levels of maturity when it comes to managing risk. However, the level for attaining professional recognition will be the same."

2015 MEA RISK AND INSURANCE EXCELLENCE AWARDS FINALISTS

Finalists for *StrategicRISK*'s inaugural 2015 MEA Risk and Insurance Excellence Awards have been announced.

Shortlisted entrants had an opportunity to make a 10-minute presentation to a panel of judges at our Dubai event in April, after which the finalists were decided.

Finalists for each category are as follow:

MEA Commercial Broker Initiative of the Year
Apex • Marsh • UIB

MEA Commercial Insurer Initiative of the Year
AIG MEA Ltd/American Home Assurance Company (AHAC) • Jordan Insurance Company

MEA Business Partner of the Year
Bin Shabib & Associates (BSA) • EBIX Europe • Milliman • Moody's Investors Service

MEA Risk Communication Strategy of the Year
Abu Dhabi Airports • Dana Gas • Emirates Transport • IRM Jordan & Palestine Regional Group • Saudi Basic Industries Corporation

MEA Enterprise Risk Management Programme of the Year
Abu Dhabi Airports • Dana Gas • Emirates Transport • Marsh • Qatar Foundation • Roads & Transport Authority, Dubai

MEA Best Risk Financing Approach
Marsh • Saudi Basic Industries Corporation

The awards are an opportunity to bring together the Middle East and Africa's leading risk managers, brokers, insurers and reinsurers to recognise hard work and innovation and celebrate success.

In the first year of this event, we are seeking to find the most successful and innovative individuals, teams and companies to reward their achievements.

As such, the awards are a platform for risk and insurance professionals to share best practice, showcase innovative solutions and demonstrate market leadership. They help to celebrate the successes of the region's finest risk and (re)insurance executives, and the professionals who make sure they get the best results.

Organised by the publishers of *StrategicRISK* and our reinsurance-focused sister publication *GR*, the awards will be handed out at a gala dinner on 27 September in Dubai.

The event will be the first in the region to combine risk and insurance professionals, as well as the only awards event to cover the Middle East and the entire African continent.

Saleem confirmed there would be clear interest in the Middle East around certification. "People here are very committed to learning and development, particularly as business has become so international," he said.

Dealing with risk effectively also means looking ahead. Graham described risk managers as "professional meerkats scanning the risk horizon," particularly in terms of dealing with strategic risks – an area that resonated with the panellists.

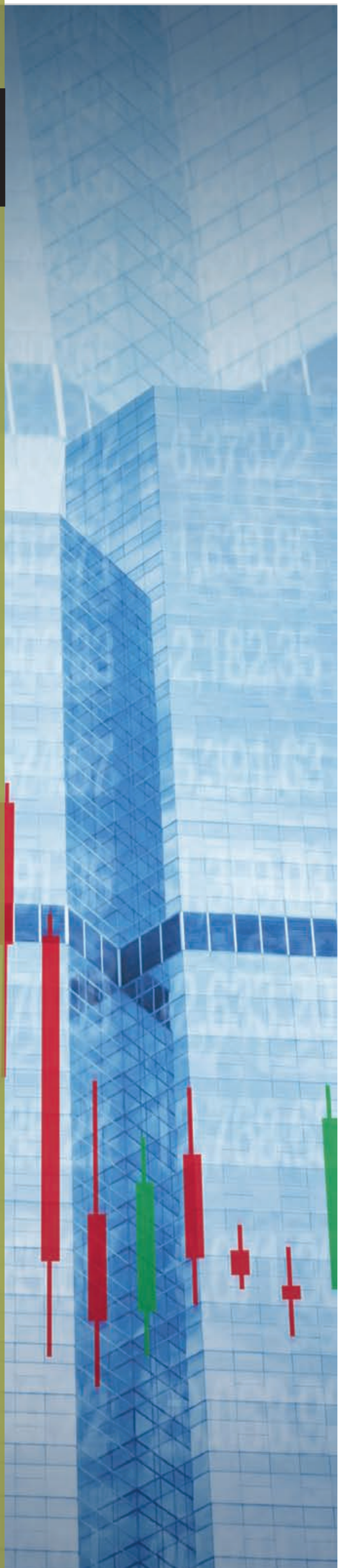
"We embed risk management into our strategic plans," said Qatar Foundation's Saunders. "We make it mandatory for each entity to consider the strategic as well as other risks. We are also working to integrate risk management within certain employees' job descriptions to build a more risk-aware culture."

Saleem added: "We also have a five-year strategic plan, which is linked to the Dubai plans for 2020 and 2030, so we have long-term strategic planning. In terms of strategic risks, we go through a process of bringing together all our board members to look at the strategic risks and then feed this back into our operational plans for the organisation."

King, whose career experience includes working across the wider EMEA region, said MENA businesses were ahead of those in many other regions when it came to forward thinking: "I see more emphasis in this market among organisations on long-term planning than I do in many so-called mature economies, whose only target is the next three-month statement they are going to make to the stock market," King said. "Often, that is the extent of their strategic planning." **Mike Jones**

Focus

FUTURE OF RISK



FROM HERE TO THERE

Thanks to global events, the role of risk managers is moving up the executive chain

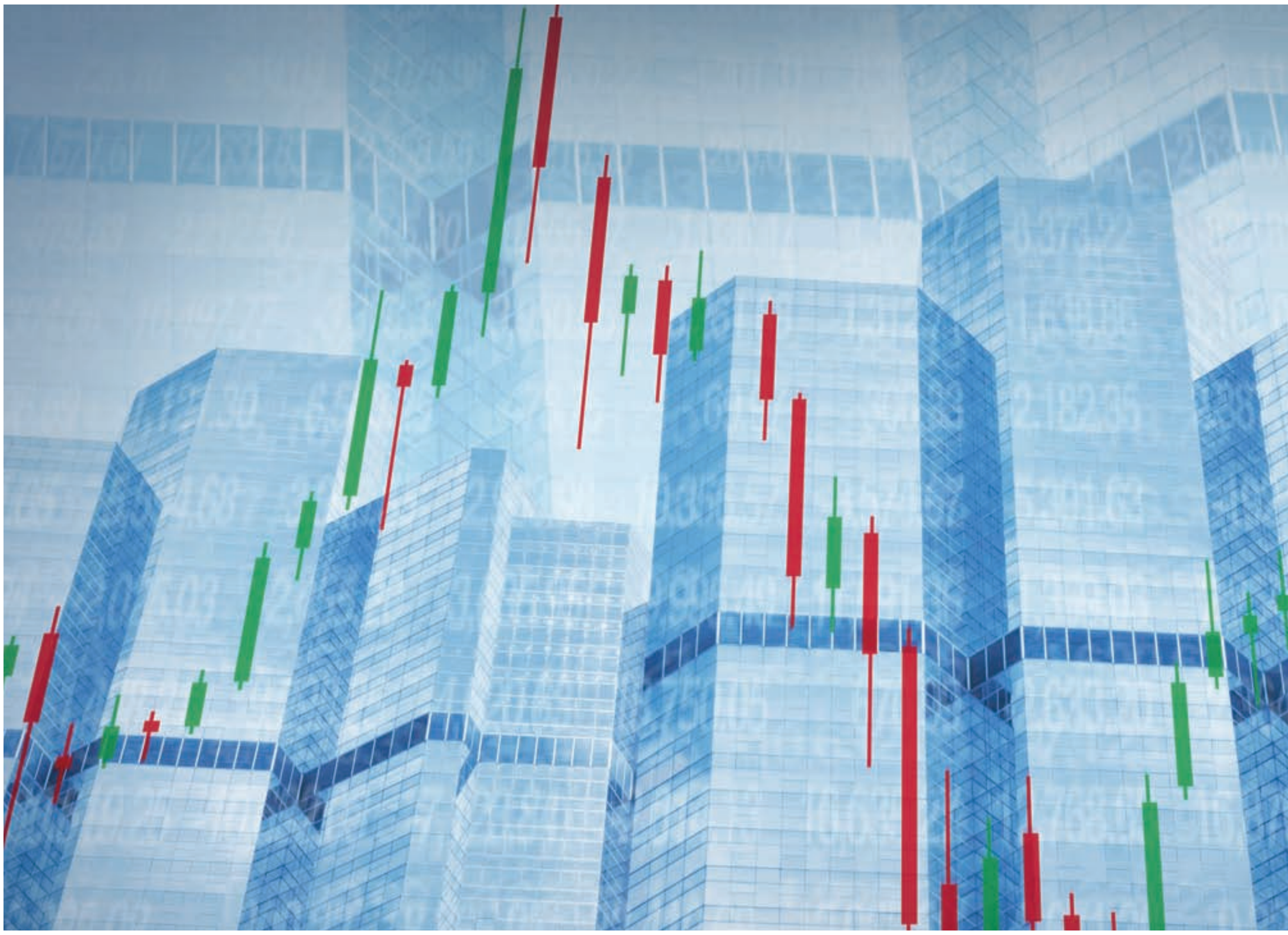
BLAME THE FINANCIAL CRISIS. NO OTHER event in the past few years – not even the disastrous Thailand floods – has had such a profound effect on risk management as the implosion of some of the world's biggest banks and insurance companies.

This devastating event destroyed the complacency of the financial sector, governments and regulators concerning the effectiveness of their oversight of the industry and triggered a series of official reactions that continue to influence the climate of risk management today.

Legislative responses occurred across crisis-hit regions – Europe and the UK, much of Asia-Pacific and, above all, the US. "The crisis was a big driver of risk management skills," says Tom Teixeira, a managing director at Alvarez & Marsal in London, who has 20 years of risk management experience with a swathe of big companies.

"[The crisis] has made risk managers more analytical in nature and that's occurred across most industries – aerospace, engineering, property, resources. Risk managers must now present trends and numbers to the board."

As others have done, Teixeira cites the Financial Reporting Council's increasingly specific recommendations as having



profound consequences on the way risk is being monitored within preset, agreed tolerances and in the way the results are presented to the board. "Directors now want to see numbers," he adds. "Further, the analytical techniques that have been adopted by the financial sector are coming into other industries."

Lloyd's

In a timely example of the way advanced practices are percolating through the broader commercial world, some of Europe's best and brightest risk managers assembled at Lloyd's of London in April for six days of hothouse tuition. A series of speakers introduced these relatively young executives, all with three to five years of experience, to the burning issues of the day.

Among other topics, they were given insights into emerging risks, an overview of how Lloyd's tackles risk appetite and its management and claims management.

Launched in 2013, these seminars are certain to improve risk management techniques – and make companies safer – in the coming years. FERMA president Julia Graham is not alone in seeing the Lloyd's sessions as a crucible of talent.

Looming threats

There is a growing recognition that because too many companies failed to see the dangers that befell them the onus is increasingly on risk managers to head off threats before it is too late.

According to a consensus of views, risk managers are moving into a much more prominent role. As such, they are expected to confront the boards, if necessary, on looming threats. This is what many directors need. "Generally, boards have a poor oversight of short-term risks and their consequences," concludes John Hurrell, chief executive of Airmic. "They don't have to micromanage everything, but they do need effective oversight." Yet, the more remote the board, the less likely it is to have that oversight.

Recently, Hurrell had a meeting with a titan of the banking industry in an office perched high above Canary Wharf. "It must be very difficult [to be aware of the risks] in such splendid isolation," he suggests.

"It will become more and more important to behave all the time as though your offices are in a greenhouse, rather than in a fortress such as Dover Castle."

Sharman report

The Financial Reporting Council's Sharman report proved to be a wake-up call.

"All directors have responsibility for managing risks," explains Hurrell. "In this environment, it will be risk professionals who must be their eyes and ears.

"Boards need more guidance. There's a strong need for leadership in reporting to the board."

Indeed, the analysis of recent commercial disasters tells a sorry story of bewildered boards. In all too many case studies highlighted in *Roads to Ruin*, the report conducted by Cass Business School for Airmic, the risk management function was buried so far down the executive hierarchy that directors were largely unaware of the menace that caused all the damage. The authors of *Roads to Ruin* – which should be obligatory reading for all directors in all industries – describe this tendency as "board blindness".

As Hurrell points out, most companies have about half a dozen management layers and risk management usually lies somewhere near the bottom. He believes the

> '[The crisis] has made risk managers more analytical in nature and that's occurred across most of industries'
>
> Tom Teixeira, Alvarez & Marsal

function should have a floating role: access through all levels, so risk managers can gain an in-depth insight into commercial threats from within as well as from without. Armed with that insight, they are then in a position to take their case to the C-suite.

"Boards don't need to know everything, but they must be confident that the company is not at risk," explains Hurrell.

Better or worse

Essentially, directors need to know only one thing: "Have things become better or worse?" asks Teixeira. That requires information-rich risk managers with better presentation skills than most have at present.

Typically, says Teixeira, boards are confused by too much data. It may appear as though the risk manager is doing their job, but this will not be sufficient in tomorrow's world. "Boards can't separate the wheat from the chaff," he points out.

Today's smartest risk managers are using simple colour-coded graphs – or often dashboards – to summarise complex data in a form that is easily assimilated by paper-burdened directors.

Litigation

The phenomenon cannot be blamed on the financial crisis, but Asian risk managers are learning how to deal with the growth of a Western phenomenon: litigation.

As Singapore-based Gabriel Chew, head of insurance programmes and training at palm-oil giant Inter-Continental Oils and Fats Pte Ltd, explains: "The main change in Asia in the past few years is in the area of liability. Historically, the region has seen relatively little litigation – for instance, incidents of bodily injury haven't normally gone to court – but the old practice of settlement out of court is gradually being replaced by a culture of litigation. This is the result of growing foreign investment in the region."

This has led to a demand for more highly trained risk managers to look beyond the mere transference of risk. Increasingly, insurers are pressurising them to do so.

Liability

Developments in law are complicating the landscape. In India, for example, since the 1984 Union Carbide chemical disaster in Bhopal, public liability protection has been mandatory under law in certain industries such as oil and gas. In these designated industries, it is obligatory to pay immediate relief payable to affected employees and inhabitants.

However, as Chew points out, there are wide variations across the region: "Practices in Singapore are in line with those applying in international liability."

Supply chains

Risk managers are also coming to grips with lengthening supply chains because of the explosion in pan-Asian trade. Most companies in the region developed as vertically integrated, family or partially government-owned businesses and had little need to take much notice of what was happening elsewhere, except in terms of compliance with local regulations. However, this is changing as risk managers learn how to negotiate often vastly different regulations in different countries.

In short, whether in Asia or elsewhere, the role of the risk manager is moving up the executive chain and moving outward into new geographies. **SR**

THE BAR IS RISING FOR RISK MANAGEMENT

The traditional role of risk managers is changing. In the future they will have to adopt an integrated approach and a more can-do attitude and help firms take risks, rather than to avoid them

A MASTER OF PITHY SAYINGS ABOUT investment, Warren Buffett also made a shrewd observation about risk management. "Risk comes from not knowing what you're doing," he once said. As a summary of the position of many companies floundering in a sea of risks, it is typically insightful.

Given the number and variety of potential threats and the problems many businesses are experiencing as they struggle with current problems and face new ones, their predicament is hardly surprising.

Julia Graham, FERMA president, quotes Buffett's observation in support of her commitment to professional-standard certification and continuous education for risk managers in Europe.

She sees FERMA's development of ongoing courses as a game-changer that will reap dividends across Europe.

FERMA's certification programme is likely to become international. In short, it could become the default standard outside Europe, particularly in the Middle East and Asia. "Possibly, it could become the standard," she says. "However, it is important to start in your own backyard. Will other [regions] join in later? Probably, but FERMA must remember who it represents."

In any case, the outcome will be the same. Companies with highly trained risk managers will be far more likely to know what they are doing.

Trial by YouTube

For some, that stage cannot come fast enough. The past two years show just how vulnerable the business world is to a multiplicity of threats: the chaotic process of globalisation, breakneck advances in technology and exposure to random, merciless 24/7 media.

The last threat will probably turn out to be the most serious. "Even five years ago, it was hard for companies to get ahead of the media in a crisis," explains John Hurrell, chief executive of Airmic. "Now, it's practically impossible."

In this round-the-clock environment, the future is just around the corner. "Things that will bite companies on the bottom are short-term issues," warns Hurrell. "The risks are immediate and boards must be prepared for short-term events."

A chairman's worst nightmare could become trial by YouTube, as an avalanche of information – much of it misinformed – pours into the digital world following a power outage, boardroom scandal or juicy news item.

Resilience

In an era of fast-approaching risks, the watchword will be resilience. Because it is impossible to protect against every threat, resilience will be built on the speed of response. "Do companies want to act like tortoises or shoals of fish?" Hurrell asks. "A crisis management plan must be in place before the crisis." At the very least, the company should be in a position to move at the speed of the crisis, or preferably, be a move or two ahead.

In this scenario, the risk manager of the future will have an influential role. Tom Teixeira, a managing director of Alvarez & Marsal in London, predicts that the traditional, somewhat negative role of somebody who is preoccupied with prevention and avoidance will be transformed into that of guidance and recovery.

"Risk managers will be involved in crisis management to minimise business disruption," he explains. "Business continuity [will also be essential]. The two roles cannot be separated these days; it's the new, integrated approach."

Also, the contemporary risk manager will be seen as a facilitator, an executive with the tools that enable the company to take risks rather than avoid them.

"Too often, risk managers are seen as blockers," explains Jonathan Salter, director of global consulting at

RSA, the division responsible for risk management and loss prevention. "Risk managers should have a can-do attitude. They should be able to go to the board and say, 'Tell me what you want to do and we'll find the solution.' That's probably of number-one importance for risk managers today."

Positive rather than negative managers will gain the confidence of the board. In Salter's experience, risk managers are most effective in such an environment. "The more influential risk managers have cracked that board and chief executive relationship," he says.

The creative risk manager will deploy a range of tools to keep boards informed about the nature and depth of the risks a company is running. "Risk is not easily quantifiable," adds Salter. "It's more dynamic than, say, finance. RSA has invested heavily in tools that allow risk metrics to be measured and made more transparent. However, the information must be robust and reliable. It must be joined up and correctly interpreted."

He thinks the use of these sophisticated tools will become standard practice.

Fundamental principles

Clearly, the need for formal training has never been as great. FERMA bases its programme on several fundamental principles. The resulting certification must be objective, consistent, based on continuous learning, recognisable across all EU nations and founded on a code of ethics. In short, a thoroughly professional qualification that produces trusted advisers.

Just as in other professions, one organisation – in this case, FERMA – will be seen as the standard bearer in the development of risk management.

Finally, in the interests of maintaining standards, the providers of the learning programmes must be licensed. "The benchmarks must be the same, wherever risk managers are," says Graham.

However, nothing can replace experience and Salter believes today's risk experts – risk managers, brokers and insurers – have a duty to pass on their knowledge. "We need to educate the next generation," he says.

Revolution in Asia

A growing number of those risk managers will be in Asia as the philosophy and practice of risk management fast moves up several notches. Because tariff walls are collapsing and markets are opening up, particularly in rapidly developing Association of Southeast Asian Nations (ASEAN) countries, risk managers are expecting an onslaught of unfamiliar challenges.

Many manufacturers are facing Western-style product liability litigation for the first time and believe the trend will only increase. They will be forced to become familiar with often wildly differing liability laws as they export to nations across the region. The era of free – or freer – trade will also affect them. Not only will they be forced to deal with different governments and contradictory regulations, but they will face new competitors.

"Things are moving fast," says Gabriel Chew, head of insurance programmes and training at Singapore's Continental Oils and Fats Pte Ltd. "There's an opportunity of risk coming for some industries."

Ginger groups

In the wake of highly publicised campaigns, Asia's risk managers are also being forced into the public arena on environmental issues, a relatively new phenomenon in a region where economic growth has sometimes come at an ecological cost. Companies will be required to become good environmental citizens as highly politicised ginger (internal) groups learn how to publicise their grievances. Pressure is also coming from governments.

"The regulatory authorities are more concerned now," adds Chew, a regional standard bearer for improved risk management practices. "The level of scrutiny varies across the region, but the pressure is on companies to ensure good environmental practices are in place."

Ear of the board

In Asia as elsewhere, the fast-rising prevalence and diversity of commercial threats have fuelled a call for risk managers to be given higher status and authority within companies, including a seat on the board.

However, this may be unnecessary, says Graham: "Each organisation has to decide for itself. There's no single blueprint. Usually, chief executives have overall responsibility for risk management, and they are on the board. However, if risk management is not on the board, it's more often co-opted. Certainly though, risk management is taking a more strategic position in companies. That means the bar is rising."

Others see a convergence of risk management functions. For one, the Brussels-based European Confederation of Institutes of Internal Auditing (ECIAA) believes the link between risk managers and internal auditors will strengthen. Indeed, it sees this as inevitable in the wake of EU legislation designed to enforce better corporate behaviour and governance.

The ECIAA and FERMA have produced a joint guide on the eight Company Law Directive. Its purpose is to help risk managers and auditors work through the onerous requirements. As the guide points out: "Co-operation between the audit committee and the risk committee is crucial to ensure a common risk management approach."

Some companies are expected to comply with the directive by imitating the financial sector, where the risk management function is now enshrined in regulation. If so, they will establish dedicated risk committees with a firm grip on information of vital commercial importance. Armed with this data, the risk management function will be in a position to challenge management and even the board.

> 'Risk managers should have a can-do attitude – they should say to the board, 'Tell me what you want – we'll find a solution'
>
> Jonathan Salter, RSA

Last bastions

The gold-plating of the risk management function will likely occur first in the utilities and other sectors with a public presence. Hurrell says this is already happening in much of the oil and gas, water and telecommunications industries, each of which has a natural exposure to reputational damage. Other sectors with strong brand values, such as high-street retailers, are also following the trend.

Eventually, risk management will invade what Hurrell describes as "the last bastions – obscure business-to-business companies with little or no brand values". He sees this happening in the next five years or so.

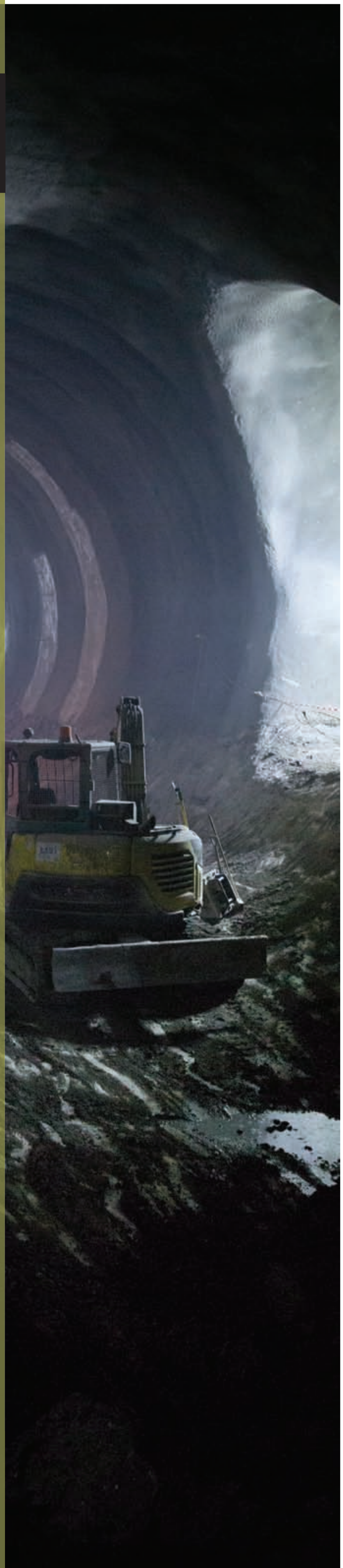
The China conference

By then, Asia may be teaching the West a few lessons in risk management. For example, China's knowledge of the function is increasing fast. *StrategicRISK* organised groundbreaking roundtables on risk management in 2014, and the fast-growing Pan-Asia Risk and Insurance Management Association will host China's first full-scale risk management conference later this year.

It is a sign of the times that, together with a strong international contingent, some 60 Chinese companies had already signed up by early 2015. SR

Focus

Construction risks



Lessons from Crossrail

Risk management has been central to the success of Europe's largest infrastructure project, owing much to sustained engagement with the board and senior management

AT THE END OF MARCH, EUROPE'S LARGEST construction venture, Crossrail, initiated the final stages of building a 42km tunnel network under London. Six years ago, the project began with the construction of eight new stations and servicing of 38 existing stations to accommodate the new railway. The completed railway will stretch from Reading (west of London) to Shenfield (to the north east) and Abbey Wood (to the south-east).

The project is meant to increase London's rail capacity by 10%, with the first trains expected to run through the central tunnelled section in 2018. According to Crossrail, the new railway will bring a further 1.5 million people to within 45 minutes of the city centre. Moreover, the development is likely to support regeneration and add £42bn (€57.6bn) to the UK economy.

The size, complexity and high-profile nature of the project has placed greater pressure on the risk management function to ensure the project is delivered on time and within budget. That pressure was intensified owing to the poor performance of a number of large UK infrastructure projects in the years prior to Crossrail, such as the London underground Jubilee line extension, which scarred the industry, according to Crossrail head of risk management Rob Halstead.

Underground risks

Supporting the numerous parties involved at the different stages of the development has proved a difficult task for Halstead and his team. He says tunnelling beneath London's complex underground infrastructure has been a particularly risky process.

"The tunnelling has almost been concluded. The scale and complexity of the project meant there was a lot of risk regarding interfaces between different parties on the project," he says.

"A lot of infrastructure is underground, which must be protected when tunnelling underneath. In terms of risk, that presented us with a significant challenge at the early stages of tunnelling, owing to a number of critical infrastructures under the city."

Having embarked on building 42km of tunnels in the summer of 2012, Crossrail announced at the end of March that the final two 750m drives had commenced between London's Liverpool Street and Farringdon stations. Although some of the risk team will continue to support those managing the final tunnel drives and the construction of new stations, Halstead's main focus has now turned to ensuring the railway is built, tested, approved and handed over to its operator on time.

The task is further complicated by the ongoing disruptions to train services passing through London Bridge – the city's busiest station – after the government-funded Thameslink Programme began redeveloping the railway operating system in September last year.

"Building the railway and bringing it into operation at the end of the job [challenging]. We are looking ahead to help people [involved in the project] think about what the risks are when introducing a new railway and help them manage those risks," Halstead says.

Ensuring each stage of development is commenced on time and within budget on such a large scale may seem unrealistic to some. However, six years after construction commenced, Crossrail remains on time and on budget, despite its budget having been reduced by £1bn in the government's Comprehensive Spending Review of 2010 – a cut partly due to reduced risks associated with revised construction sequencing.

Board engagement

Halstead says the success of the project so far owes much to quality engagement with the board and senior executives on risk management matters, which has been impressively high from the start.

Reporting to the programme controls director, Halstead meets with the independent board five times a year and with senior executives every four weeks to discuss the risk management agenda.

Although a heightened interest in risk management at board and executive levels may stem from external pressures and expectations, Halstead says the onus is firmly on the risk function to sustain that interest and maintain engagement.

Crossrail London route

Photos: Crossrail

"No senior manager will say that managing risk is not important.

Everyone knows that managing risk is important, but the trick [to improving board engagement] is giving senior management something to engage with that supports that aspiration," he says.

"Clearly, directors and executives are busy and have a high-level perspective of the project. Therefore it's important to respond to that and give them information to which they can relate."

The team drew together a set of risks in 2009-10 to engage the project's board. The list remains relevant and is still in use and Halstead believes initiatives such as this can improve and sustain board engagement with risk management.

"Risk management tends to be dry, with lots of risk registers, analysis and academic reports. What we have done here is provide a process and a set of tools that the senior team can understand and relate to in order to help them manage risk," he says.

"Increased board engagement requires the leadership to have the appetite [to engage in risk management], but the risk team also needs to give them something to sustain their interest and deliver value."

Halstead finds himself being stretched with various queries from the board but he recognises this as a positive endorsement for the importance of risk management. With risk management a key focus for the board, the Crossrail project is an example of good practice for the wider risk community in terms of enhancing professional recognition for risk managers. **SR**

> 'The scale and complexity of the project meant there was a lot of risk regarding interfaces between different parties on the project'
>
> **Rob Halstead,** Crossrail

Risk-managing the threats of Sweden's construction market

With a plethora of new projects taking place in Sweden and Scandinavia, *StrategicRISK* asked Anders Esbjörnsson, the group head of risk and managing director for insurance at NCC AB – the second largest construction company in the Nordic region – about the state of the Swedish market

Growth prospects for the Swedish construction market look positive, with the country projected to achieve 4.80% compound annual growth by 2018. However, what challenges does the local market face?
The construction market is fragmented. None of the main construction companies hold a market share of more than 7%. Some large infrastructure projects are ongoing, mainly in the regions around the larger cities and many large projects have been planned. The housing market is doing fine. The demand for housing in the larger cities is significant, but the number of projects under construction remains modest.

With the largest projects, Scandinavia is experiencing more overseas competition. For example, a Chinese firm has been contracted to build a bridge in Norway and this is possibly a result of numerous large projects taking place in the Nordic region.

Are you managing any of the large projects planned for the Nordic region?
The risk management department becomes involved in all large projects: those exceeding €50m. For example, the construction of a city tunnel under Stockholm (for commuter trains), two large property developments in Stockholm and a road near Gothenburg – the second largest city in Sweden and the fifth largest in the Nordic countries.

The risk team also arranges insurance cover for all activities, and this forms the base for our work. Big projects often fall outside our annual policies, meaning we have to be more involved in risk assessment and we do this by conducting various risk surveys. The first of these risk surveys ensures that all liabilities are handled properly. Then, we run a survey scheme together with the different leaders of the project. With large projects, we are generally involved from start to finish.

Do these risk assessments and surveys form part of an ERM framework or is project risk management a more effective method in the construction industry?
This is a difficult question. The NCC strives to broaden the scope of risk management, but construction projects require a ground-up approach and clear guidelines are necessary on how to manage risks for different projects.

The entire company must also have a clear risk management strategy and manage risks across national borders and between business areas.

What are the top three risks facing the construction industry in Scandinavia?
The top three risks are environmental; HR/health and safety; and slow innovation.

In respect of environmental risks, authorities are getting tough and are frequently applying strict enforcement when companies fail to comply with environmental laws.

With regard to HR/health and safety, businesses must consider the welfare of subcontractors. All members of staff – whether in-house or part of a third-party entity – are still getting severely injured and sometimes fatal accidents occur. This is not acceptable.

Last, innovation is slow. The construction industry is too conservative and it needs to find new, sustainable solutions.

What about emerging risks? Some are bound to challenge businesses in the next few years?
IT, which is increasingly used in the planning and designing stages of a project is an emerging risk. The risk lies mainly in human error and whether staff members are following IT security procedures correctly, rather than in the technology itself.

Furthermore, recruiting the best people is a long-term challenge. A large number of construction workers are approaching retirement age and the industry needs to win the fight for the best engineers and technicians in the coming years.

The focus must be to make the construction industry attractive to younger people who have different preferences than older generations. SR

Green infrastructure is good for society and the environment and is increasingly touted as offering business benefits, but how feasible is it to construct green buildings?

Could green construction attract new business?

CONSTRUCTION COMPANIES ARE UNDER increasing pressure to develop environmentally friendly, 'green' infrastructure as carbon dioxide levels continue to creep to dangerous levels. In May 2013, CO_2 concentrations in the atmosphere passed the symbolic mark of 400 parts per million – the highest level in human history.

Indeed, the construction industry uses a lot of energy in the creation of buildings and infrastructure, emitting significant levels of CO_2 and other pollutants in the process.

Against a backdrop of growing urbanisation, global population growth and a high demand for new housing and other facilities, the majority of construction companies may prioritise completing projects on time and on budget over 'going green'.

However, construction companies, among others, would be wise to consider the long-term damage to the environment and society of ignoring the green agenda.

Chris Whitehead, head of programme management office at Balfour Beatty – a company of which about 26% of its US turnover comes from green infrastructure – sums up well the consequences. "Pollution is impairing air quality in the largest cities. For example, 92% of the largest 70 cities in China have an average annual particle pollution of 2.5 – worse than the national standard. [Pollution] is also an issue in European cities."

To contain the average temperature rise to no more than 2°C by 2050, as recommended by the Intergovernmental Panel on Climate Change, construction businesses "need to reduce their emissions year on year, yet presently [CO_2 emissions] are still on the increase," Whitehead says.

One way of tackling the problem is to develop green infrastructure. These builds make use of natural components. For example, instead of building flood protection, a green solution would be to let a natural wetland absorb the excess water from rain, thus preventing CO_2 emission from the construction of flood barriers. Additionally, features such as green roofs, parks and greenways will remove CO_2 from the air.

There are some success stories. For example, an urban renewal project, undertaken between 1998 and 2002, of a social housing estate, Ekostaden Augustenborg, in Sweden delivered many positive outcomes.

The estate was built between 1948 and 1952 to international acclaim, offering, what then to be high-quality social housing, schools, shops and employment. However, over the years, the estate fell into disrepute owing to general neglect and economic decline.

Buildings suffered from severe damp and bad ventilation because of poor insulation. During renovation, the outer wall covering were removed and new sustainable insulation layers were installed. As a result, energy efficiency increased by approximately 35%, compared with when the premises were first built.

The project cost about €22m and, according to the European Commission – which has adopted a green infrastructure strategy – the benefits from this investment are stacking up. Rainwater runoff rates have declined by 50% and biodiversity has increased by 50%.

Competitive advantage

Green infrastructure may also give business a competitive advantage. Anders Esbjörnsson, group head of risk at NCC AB, the second largest construction company in the Nordics, says old buildings are hard to sell to investors because they are energy consuming and investors would opt for green buildings instead because they could give them competitive advantage.

However, sustainable builds and green infrastructure, are in real-term cash value, expensive. "People generalise that low-carbon infrastructure costs less, but that is not true for all classes of infrastructure," Whitehead says. "Although the 'low carbon = low cost' theme of the Infrastructure Carbon Review [published by the UK government in 2013, setting out actions to reduce carbon emission] holds good for economic infrastructure, green buildings need investment over and above the norm.

"Therefore companies can produce carbon efficient buildings only in collaboration with an enlightened client."

How then, can businesses promote green infrastructure?

Business should follow their clients and local legislation, argues Whitehead. From a UK perspective, he says: "Look at the demand from large corporates such as Google and PwC for low-impact buildings. Look at the sales figures for housing developments such as Little Kelham in Sheffield. Understand the implications of the latest building regulations such as the government's Energy Savings Opportunity Scheme and the carbon strategies of the National Health Service."

Although expensive and challenging to get off the ground, green infrastructure will yield many benefits. If that is not convincing enough, then as Whitehead concludes: "As clients become more environmentally aware, they will select companies that can deal with the green agenda." **SR**

SPECIAL REPORT

TERRORISM AND POLITICAL VIOLENCE

Terrorism and political violence

DANGEROUS TIMES

The rise of IS, the 'law of unintended consequences'

Although it is true that the events of the Arab Spring have changed the Middle East and North Africa (MENA) region, it is perhaps more accurate to say that the process is still ongoing, since so much is still in flux.

"The Arab Spring has unleashed a lot of uncertainty that [some areas are] struggling to absorb, either economically or politically," says Anthony Skinner, director and head of MENA at Verisk Maplecroft.

Just as some historians have argued that the second world war ended only in 1989 with the collapse of the USSR, so it is impossible to know at this stage what the full impact of the political upheavals of the past five years will be or where they may yet lead.

Legacy of uncertainty

The most significant legacy of the post-2010 upheavals is uncertainty. In many instances, this has resulted in the creation of a political and security vacuum that is being filled by unpredictable, difficult-to-control and often violent extremists.

"The decline of the state structure in countries such as Libya and Syria has meant a number of non-state actors have been able to tap into weapons and other resources, and then use them to pursue their own agenda," comments Skinner.

Falling oil prices have only added to the political uncertainty. Topping the list of political risks currently facing emerging-market investors is the increasing instability in already-fragile oil-producing countries such as Iran, Iraq and Libya, according to analysis by Aon Risk Solutions.

"Libya has become a base not only for Islamist groups at home, but as a launching pad for groups sending fighters to neighbouring states," says Skinner.

The rise of IS

The single most significant new force to emerge in recent years marches under the black flag of the Islamic State (IS) and the rise of this group is a powerful reminder of how the 'law of unintended consequences' is increasingly shaping events across the region.

IS emerged from a loose alliance of forces opposed to president Bashar al-Assad's rule in Syria. The West now finds itself propping up the same regime it discussed taking potential military strikes against only two years ago, considering it the lesser of two evils.

Despite coalition airstrikes and the best efforts of the Iraqi army and the Kurdish Peshmurga, IS remains in control of a significant area across Iraq and Syria, which includes access to immense financial reserves and manpower.

"IS in Syria and Iraq is incredibly robust and the resources needed to eliminate this group are considerable," says Jonathan Wood, associate director, Global Risk Analysis, Control Risks.

He adds: "There isn't the presence of a single, cohesive force that could do so and the groups that are currently keeping IS in check, such as the Kurdish Peshmurga, have their own internal divisions."

> ***'The decline of the state structure in countries such as Libya and Syria has meant a number of non-state actors have been able to tap into weapons and other resources, and then use them to pursue their own agenda'***
> **Anthony Skinner,** Verisk Maplecroft

While this situation persists, IS is having a galvanising effect on Islamists across the region and the wider world, potentially acting as an inspiration for terrorist attacks in countries from Canada to Europe.

Not only does IS make its presence felt through brutal attacks in urban centres – such as the March assault on the Bardo Museum in Tunis, which killed 21 people, including 18 tourists – it is also increasingly making full use of its ability to attack targets online many hundreds of kilometers from its headquarters in Raqqa, Syria.

NEW TACTICS

Be prepared for the unexpected

In January, the 'CyberCaliphate' group hacked into the Twitter and YouTube accounts of the US Central Military Command, scrawling "I love you Isis" on the page and tweeting images of US personnel and military documents.

JM Berger, co-author of *Isis: The State of Terror*, says: "Isis [or IS] has been recruiting hackers for some time now. Some are virtual collaborators from a distance, but others have been recruited to emigrate to Syria. Activity targeting the West is just part of their portfolio. "IS has not been extremely visible yet, carrying out more sophisticated activities such as high-level cyber crime or destructive attacks, but I suspect this is just a matter of time. This is a low-cost way to publicise its cause and harass its enemies."

The region's long-standing sectarian divide is also becoming increasingly significant. The battle for hegemony between Shia and Sunni protagonists is fuelling violence through proxy warfare, insurgency and political manipulation on both sides. "[The coalition attacks on] Yemen are the most recent example of how this is playing out," says Verisk Maplecroft head of MENA Anthony Skinner. "Sectarian issues are influencing security."

Although direct military spillover into Gulf States remains unlikely, there is an increased risk of terrorist attacks given the number of fighters returning to other countries after fighting with IS in Iraq and Syria.

The key message is to be alert to the unexpected and be prepared.

EUROPE – A CHANGING RISK PROFILE

Instability is also felt closer to home, with new risks being manifested

Since 9/11, the Western world has been acutely aware of the risk of terrorism. Although political extremism may not be new to a continent that has already faced groups such as Baader-Meinhof and the IRA, the Islamic State (IS) has driven up the size and scale of attacks, bringing with it a greater ferocity, as seen in its soft targeting of civilians.

Within those parameters, however, the nature of the terrorist risk has changed dramatically in 15 years, with larger-scale attacks such as truck bombs becoming less likely, even as the threat of a 'lone wolf' hitting a soft target with improvised weapons or firearms has risen. Many experts are concerned about the potential for returning jihadis with experience in Iraq and Syria to increase this risk further.

Informational risk

"The level of co-operation and information-sharing between the security services has increased dramatically over the years, together with increasing sophistication of monitoring, which has made things more difficult [for terrorist groups]," says Global Risk Analysis associate director Jonathan Wood. "However, this has come at a time where there is a growing breakdown in some aspects of society."

Of particular concern is the risk of alienation within minority elements of British and French Muslim communities. Verisk Maplecroft MENA head Anthony Skinner says: "Since 9/11, the 2004 Madrid train bombings and the 2005 London bombings, carrying out major transnational attacks has become harder.

"After many years of failing to carry out a follow-up attack, the strategy has changed to leaderless, improvised, lone-wolf attacks.

"The risk increased recently because the rise of IS has been accompanied by some sophisticated use of propaganda – especially through social media – and this may result in a rise in the number of lone-wolf attacks, although this is not yet proven."

Skinner continues: "It's not just the attack itself that is important, but the scale of the publicity afterwards: this is where social media comes in."

> *'Sophisticated use of propaganda – especially through social media – may result in [more] lone-wolf attacks'*
>
> **Anthony Skinner,** Verisk Maplecroft

Arguably, there is more political radicalisation across Europe now than at any time since before the second world war, as support for nationalist parties and more radical movements grows in response to socioeconomic problems and a perceived failure by elites to deal with the situation or prevent the crisis.

"We're just coming out of a nasty recession that has affected people's attitudes – commercially and politically – and as a consequence, there is a lot of unrest and many minority groups are in a strong position because of this weakness," says Stuart Poole-Robb, chief executive at KCS Strategic Intelligence and Corporate Security. "The rise of nationalism in Europe is an expression of a broader and deeper instability across the world."

However, despite past attacks by groups such as the IRA, the main risk posed by rising nationalism currently comes from political instability and the increased risk of criminal-type activity such as riots, arson or attacks on individuals.

Business interruption

At a corporate level, the likelihood of being targeted by a bombing or shooting in Europe is low; the real vulnerability is business disruption here or overseas. "Organisations should ensure there are measures in place to cope with a variety of scenarios," says Wood. "However, it is also vital to ensure local communities have a stake in your business succeeding at a local level.

"Oil and gas investors should pay particular attention to unstable environments where political conditions can change rapidly, and have well-prepared crisis plans in place. They also need to be aware of their vulnerabilities in other areas.

"If local security staff go on strike and are not doing their job, all of a sudden, in an unstable context firms could face the real risk of their plant being taken over by more odious elements."

Skinner adds: "It's important to maintain situational awareness, at the sub-national level (what is happening around your project?) and at the strategic level (what is happening nationally, politically, where are sectarian relationships?).

"It is also vital to be aware of the kinds of targets at risk – and is this changing. Do attacks tend to be targeted against key assets? Or are they like to be more opportunistic?"

Key security lessons from InterContinental Hotel Group

- Situational awareness – internally and externally – is king
- Time spent on security, crisis management planning, training and testing is invaluable
- The law of unintended consequences rules, meaning teams should be able to respond appropriately
- Think before acting
- Never presume the actions of others within the organisation
- Organisational resilience is critical – it will be impossible to 'catch' everything
- Successfully navigating challenges needs leadership
- Prevent a potential crisis by identifying it as an emerging issue, and name a crisis/risk owner to take charge
- Risk management's job is to identify issues, make risk owners aware and support them in dealing with the issue
- Act responsibly and have moral courage
- Get leadership on board
- Crisis is an ideal opportunity for risk managers to demonstrate their value

Terrorism and political violence

CASE STUDY:
InterContinental Hotels Group plc

The InterContinental Hotels Group (IHG) found itself on the front line during the 2013 political upheaval in Egypt when a mob attacked its Semiramis InterContinental Hotel in Cairo and many other assets were affected across the region. Thanks to excellent risk management, no one was killed.

John Ludlow, senior vice-president and head of Global Risk Management at the firm, says: "Political instability is of increasing concern to multinationals in that companies are becoming more and more aware of the potential effects of political instability to the wider business environment – such as business confidence, legal and regulatory constraints, financial conditions and reputation – consequently, geopolitical intelligence is of value to business as a whole, rather than only to risk management."

Geopolitical complexity

IHG has seen geopolitical instability diversifying and becoming increasingly complex, with political and economic uncertainties creating a context in which Ludlow argues that kinetic threats and risks, such as terrorism, insurgency and political violence, can flourish.

"The challenge for IHG was protecting our hotels, guests and employees from the political violence that accompanied these transitions and the heightened ambient security environment borne of the political instability.

"A secondary challenge was continuing to operate safe and secure hotels and resorts, while also being able to pay salaries during extended periods of significantly reduced revenue and securing a constant delivery of essential supplies."

To do this, IHG has developed an intelligence-led, threat-based approach to security underpinning a risk-based approach to protecting IHG's interests, assets, people and reputation. "Intelligence, and the situational awareness that this brings, is a key component of managing these risks," says Ludlow. "IHG is constantly looking for ways to increase the span and effectiveness of its security intelligence capability to assess how current geopolitical situations may evolve and affect its current operations and then predict likely new situations and their likely course."

There has been a significant increase in security resourcing and an increase in staff from two to 17 since 2007.

"IHG also has a formal threat management system that disseminates threat information and provides mitigating action advice," says Ludlow.

"This is underpinned by a 'Hotel Security Categorisation System', which ensures that hotels in high-risk areas are designed and operated appropriately to the ambient threat environment and a 'Hotel Security Alert System' that ensures hotels can respond appropriately to short-term dynamic threats.

"Additionally, IHG has a network of approximately 600 security managers and champions who work as a security community to provide on-the-ground situation reports and information gained from local contacts.

"At the strategic level, the security team liaises with governmental security agencies and other corporate security teams around the globe. Intelligence is also provided by a number of commercial security providers."

Travel risk management

In response to the Cairo events in 2013, IHG reviewed and refreshed its crisis management programme.

"We designed [the programme] in a stage to respond to what is referred to as 'Emerging Issues', seeking to formally respond to issues that have the potential to become crises in order to prevent them," says Ludlow.

"This approach puts IHG on the front foot and enables it to proactively respond to intelligence or situations."

IHG also has in place a well-developed 'Employee Traveller Risk Management Programme' that tracks IHG customers and provides travel-risk support to travellers in both high- and very high-risk countries. **SR**

THOUGHT LEADERSHIP

PIERS GREGORY
Head of terrorism underwriting,
ACE Overseas General

After 9/11, terrorism was thrust onto the corporate risk agenda for businesses across the globe. The main challenge for risk managers currently is how to prepare companies for an increasingly threatening world in which terrorism and political violence are real and changing threats.

Now, clients are moving away from seeking narrow terrorism insurance cover in favour of comprehensive solutions that cover the full range of risks: political instability, perceived injustice, populist politics and economic hardship in parts of Europe, coupled with the spin-off from brutal geopolitical conflict in parts of the Middle East and Eurasia. The range of risks is also growing, from violent attacks that include riots to shootings and arson and to large-scale bombings.

These can potentially affect every area of a business, from security and health and safety to day-to-day operations and even long-term strategy. How should a company adapt if key markets become untenable? What if airlines abandon certain routes or the infrastructure, such as roads, is damaged? What if damage to banks were to affect payroll or supply chains could be disrupted by difficulty in making payments?

Risk managers are increasingly recognised as key business assets. As such, they need to be on top of the insurance solutions available and understand the different types of cover, as well as potential gaps.

Despite the proven inadequacy of standard property damage, business interruption cover and terrorism cover, a worryingly high number of firms still seems unaware of the gaps in their existing policies. In an increasingly politicised world, it may be hard to establish exactly when a riot, for example, moves from being purely criminal to politically motivated, and hence could be excluded from cover. For example, was the damage caused by students protesting tuition cuts in the UK in 2010 political or criminal? The answer depends on the interpretation of terms – strict definitions could leave firms unwittingly exposed.

"It won't happen here" is no longer a tenable reason for not buying terrorism cover or political violence insurance, since the threats in Europe are evolving as many businesses expand their footprint into less- familiar and stable territories. Few countries remain unaffected by terror attacks or politically inspired unrest and hardly any would consider themselves free from the risk of collateral damage.

Therefore, risk managers need to understand exactly what their changing exposures are, what insurance cover they actually have, what the wordings on these policies mean and where the gaps are. Only by doing so can they be sure to have the right protection in place to defend business operations.

REGULATION & LEGAL R

MAKING THE MOST OF INVESTMENT TREATIES

How can businesses with global operations use international investment agreements to manage their political, economic and country risks?

ALL BUSINESSES WITH INTERNATIONAL OPERATIONS are exposed to political, economic and country risks on a daily basis. This is more prevalent than ever owing to currently heightened activity in a large number of politically unstable nation states, such as those in the Middle East, Africa and parts of the former Soviet Union.

Examples of the risks faced include political and civil unrest, discriminatory treatment (with local businesses being treated more favourably than foreign investors) and the imposition of new unfavourable regulations such as harsher tax regimes etc. Businesses may, as a result, experience significant economic slowdown, supply chains being squeezed, a shut down of operations (whether temporary or permanent), damage to business premises and assets, loss of staff and so on.

Although such risks in cross-border investments are unavoidable, some strategies protect and provide avenues of relief against these risks. One such measure of protection, considered here, is the use of international investment agreements (or IIAs).

Types of IIAs available to a foreign investor

IIAs are agreements entered into between states for the express purpose of protecting and promoting foreign investments. Importantly, they set out broad, substantive protections for investments and allow an investor of one country to seek money damages and other relief directly against a government of another country for breaches of those protections in a neutral international arbitration forum. They provide a state with a strong incentive to treat foreign investments fairly.

A network of about 3,000 such IIAs covers many territories worldwide.

They include bilateral investment treaties or "BITs" (between two states), multilateral investment treaties (between several states), regional agreements (between states in the same geographical region) and investment protection provisions contained in free trade agreements between two or more states.

Some examples of key multilateral investment treaties include:

- the ASEAN Comprehensive Investment Agreement (ACIA), which came into effect in 2012 between Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam;
- the North American Free Trade Agreement (NAFTA), which came into effect in 1994 between Canada, Mexico and the US;
- the Energy Charter Treaty (ECT), which entered into force in 1998, with 54 signatories and covering economic activity in the energy sector;
- the Dominican Republic–Central America Free Trade Agreement (CAFTA-DR), which entered into force in 2006 between the US, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic;
- the Comprehensive Trade and Economic Agreement (CETA) between the EU and Canada. Negotiations have been finalised over this agreement but it is not yet in force;
- the EU is currently negotiating a trade and investment deal with the US: the Transatlantic Trade and Investment Partnership or TTIP; and
- at the 16th EU-China Summit on 21 November 2013, both sides announced the launch of negotiations of a comprehensive EU-China Investment Agreement.

How IIAs work and protection they afford investors

Below is a simplified diagram in which states A and B conclude a BIT for the mutual promotion and protection of investments by investors of these states in the territory of the other state party to the treaty.

If an investor from state A makes an investment in state B, that investment then enjoys protection under the BIT and that investor acquires direct rights against state B. The same is true for an investor from state B making an investment in state A.

What is important about these IIAs is that they exist independently and in addition to any contractual rights, or in other words, a direct contract with a government is not necessary to gain protection. They can also enhance existing contractual obligations (such as through the umbrella clause, described below).

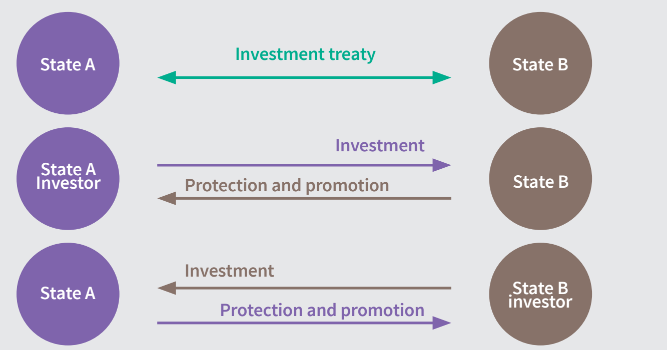
IIAs differ in their scope, wording and structure. The protections that are generally available include: fair and equitable treatment (FET); full protection and security; national treatment; most favoured nation (MFN) treatment; protection from expropriation; freedom of transfers; and an 'umbrella clause' whereby states undertake to observe obligations entered into in respect of investments.

The nature of each of these protections is outlined below, although often the determination of the scope of the protections is complex and fact-specific.

Fair and equitable treatment (FET)

This is the broadest of all protection standards, which may be potentially applied to a variety of situations. It includes: protection of legitimate expectations of investors; prohibition of discriminatory or arbitrary treatment; obligations of consistency and transparency; and protections against bad faith, coercion and harassment. It also includes protection

BIT for mutual protection between two states



against an insufficient level of administration of justice in the local courts of the host state (known as denial of justice).

The importance of the FET standard for the investor lies in its versatility. It is an appropriate standard to invoke against, for example, inconsistent decisions of the local authorities, arbitrary judgments, empty promises of high-level politicians regarding key aspects of an investment, orchestrated actions of local authorities targeted at an investment, as well as measures driven by political, nationalistic or protectionist considerations, which affect the operations of an investment.

Full protection and security

The full protection and security standard protects the investor, its officers, employees and assets from acts of physical violence of the host state and its agents. It also renders the host state internationally liable in case of violence coming from third parties, whenever the state has failed to act with due diligence to prevent or stop the attack, or prosecute the offenders. It has been invoked, for example, where Zairian soldiers destroyed an investor's property during riots.

Some tribunals have accepted that nowadays the obligation extends beyond mere physical protection and also includes components of legal security of an investor in the host state, such as access to legal remedies.

National treatment

This, and the MFN standard below, is intended to provide investors with a level playing-field. This requires states not to discriminate between foreign investors and its own nationals. As an example, this standard was breached in one case where domestic exporting companies were entitled to VAT refunds that foreign investors were not.

Most favoured nation (or MFN) treatment

This requires states not to discriminate between the investments of different foreign nationalities. On the most basic level, it would apply for example if state A passed legislation entitling investors from state B to apply for natural resource concessions in state A, but denying the same right to investors from state C.

(MFN treatment also allows foreign investors that benefit from BIT protection to take advantage of more favourable provisions in other BITs entered into by their host state. So, if the BIT between states A and B does not include an FET (or has only a narrow FET) provision but contains an MFN provision, and there is another BIT between states A and C that does have a broad FET clause, investors from state B can argue that they are entitled to the FET treatment by state A by virtue of the MFN provision contained in the BIT between states A and C.)

Protection from expropriation

Most BITs provide that states must not expropriate – or take a measure equivalent to expropriation of – an investment except where such an act is: (i) for a public purpose; (ii) on a non-discriminatory basis; (iii) carried out in accordance with due process; and (iv) is accompanied by appropriate compensation.

Such a provision covers both "direct" and "indirect" expropriation. The term "direct expropriation" includes the classic forms of expropriation such as the nationalisation of an entire industry; the taking of property during wartime or national emergency; or compulsory acquisitions of property by a state without compensation.

The term "indirect expropriation" covers measures that are not outright acquisitions but that in effect amount or are equivalent to expropriation. In these cases, an investor retains the legal title to its investment, but in effect loses its enjoyment of the investment as a result of the sovereign measures imposed by the state. An example is a failure to renew an environmental permit by the state without which the investor cannot operate.

Transfers

Even the most profitable foreign investment would be of limited use for the investor if transfer of revenues is subject to extensive restrictions. Most IIAs include guarantees that such transfers shall be made in a freely convertible currency, without undue restriction and delay.

Umbrella clause

This provision requires the host state to comply with its undertakings regarding investments. It may be relevant, for example, where a state has entered into a stabilisation clause in an investment agreement (a clause freezing applicable regulations and/or legislation in the host state affecting the business to those in effect as at the date the investment agreement was entered into).

How to structure an investment to take advantage of IIA coverage

IIAs set out expressly which investors and investments they cover. Typically, they cover all companies and persons that are nationals of one of the states that has signed the relevant IIA. The nationality of a person is usually determined by the individual's citizenship and/or residence; the nationality of a company is generally determined by either the company's country of incorporation or primary place of business, although some IIAs require a company to demonstrate that it has economic activity in the country of its alleged nationality.

Most IIAs also define investment broadly using wording such as "every kind of asset" and in effect covering almost anything with monetary value. Thus, IIAs may cover, among other things, titles to money, shares, stocks or other interests in a company, investments in sovereign wealth funds and private equity funds; supply contracts or concession contracts with the government, rights to intellectual property and goodwill.

If an investor or investment does not already fall within the scope of an existing IIA, it is often possible to restructure a business to gain protection. So, a situation may arise where a company from state A wants to develop a project in state D, but there is no treaty between states A and D. State D does, however, have treaties with states B and C:

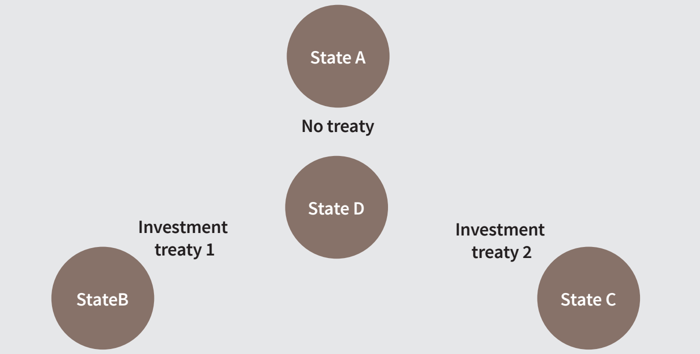
One could restructure and set up a structure like the one below, with one or more intermediary holding companies incorporated in states B and C.

If a dispute arises, holding company (HC) #1 and HC#2 from states B and C will be able to claim as investors with respect to the project in state D. Each will have a separate claim; they may claim in parallel, or the group may choose the more favourable investment treaty. How best to structure will depend on the choice of available treaties, and of course other implications such as tax planning.

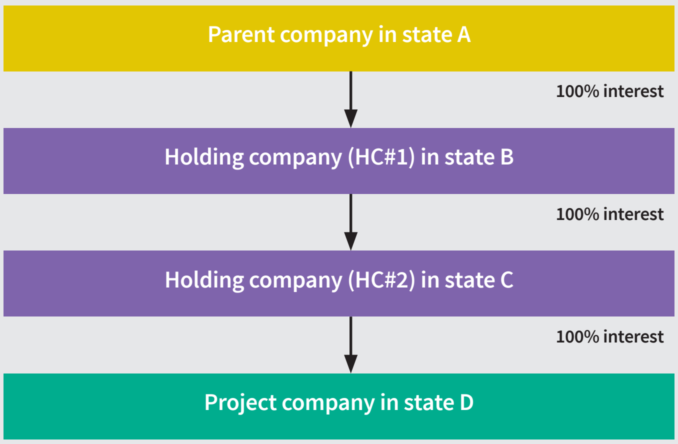
Examples of successful structuring are: involving a subsidiary (because the parent is not eligible for protection); inserting a (say, Dutch) holding company to gain standing for the local investment vehicle; or investing through a tax-efficient jurisdiction that has a BIT with the host country. Arbitral tribunals have expressly recognised that such structuring works "The language of the definition of national in many BITs evidences that such national routing of investment is in keeping with the purposes of the instruments and the motivations of the state parties": see *Aguas del Tunari SA v Bolivia*, 21 October 2005.

Importantly, the restructuring must be carried out before the dispute with the host state arises; restructuring an investment only in order to gain IIA protection constitutes an "abuse of treaty" and in such circumstances protection is likely to be denied. »

No relevant IIA in place



Restructure with one or more intermediaries



Modes of dispute resolution and organisations designated to hear them

Most IIAs provide investors with direct access to international arbitration. This guarantees investors recourse to a neutral forum, independent from the local courts of the host state. Moreover, it ensures that where a state breaches its obligations under the IIA, the state's conduct is assessed against international law standards.

Most IIAs provide the investor with a choice of dispute resolution mechanisms. The choice usually includes one or more types of arbitration (and possibly also litigation before the local courts).

The type of arbitration most commonly referred to in IIAs is ICSID (The International Centre for Settlement of Investment Disputes) arbitration. ICSID was set up by the Convention on the Settlement of Investment Disputes between States and Nationals of Other States, which was entered into force on 14 October 1966 under the auspices of the World Bank. ICSID handles the vast majority of investment treaty cases. ICSID arbitration will be available only where both state parties to the IIA are signatories of the ICSID Convention. (Where only one state is a signatory, the ICSID Additional Facility Rules may be available as an option, if provided for in the IIA.)

An advantage of ICSID arbitration over domestic court proceedings is that a contracting state is prevented from invoking sovereign immunity from suit.

Although the ICSID Convention leaves the law on state immunity from execution of an award intact, a contracting state that invokes immunity from execution to frustrate the enforcement of an ICSID award would be in violation of its duty to comply with that award. It should be stressed at this point that historic rates of compliance with ICSID awards are encouraging from the private investor's perspective. To date, member states have, with few exceptions, co-operated fully in the arbitration process and judgments have been paid. ICSID arbitral awards are moreover equivalent to a final judgment of a court in member states, and accordingly are directly executable. Out of all the cases registered, only four appear to have been challenged at the enforcement stage.

Two other forms of "institutional" arbitration often offered are ICC (International Chamber of Commerce) arbitration and SCC (Stockholm Chamber of Commerce) arbitration.

Some IIAs may require the investor to first exhaust local remedies, in other words to take their dispute to the local courts, and only if unsuccessful before the local courts allow the investor to resort to arbitration or to embark on a 'cooling off' period attempting to settle the dispute amicably before initiating arbitration.

Points a state may try to challenge

It is typical for states to raise certain objections to the jurisdiction of the arbitral tribunal that is constituted. Sometimes, this is a strategy to delay proceedings. A state might employ various arguments, for example, that:

- the company is not a "real investor" and does not conduct substantial business activities in the territory of the host state;
- the investment is not made in accordance with the local laws of the host states or is tainted by some irregularity such as bribery or the submission of fraudulent documents; or
- there has been a failure to comply with the exhaustion of local remedies or cooling-off period requirements.

Where the dispute concerns a BIT between two EU states, the state party may make arguments to the effect that obligations in the IIAs are inconsistent with EU law. For example, in relation to one recent case in which two brothers (the Micula brothers) were awarded compensation against Romania in an ICSID arbitration, the European Commission concluded that the compensation was paid in breach of EU state aid rules and should be repaid. Enforcement of the award is currently being sought by the brothers in the US courts.

Investor state arbitration has recently come under public attack, as part of the discussions surrounding the TTIP. Those criticising the system cite concern that arbitration proceedings undermine democratic structures and there is potential for rulings to obstruct a government's rights to regulate. This is a debate for another article and should not detract from the key message: IIA protections exist and businesses should consider how to avail themselves of those protections when investing abroad. This may be in conjunction with consideration of other mechanisms that may be more familiar to the reader, such as political risk insurance.

Ania Farren is a special counsel, specialising in international arbitration, at K&L Gates LLP

EXAMPLES OF FAMOUS RECENT DISPUTES

The United Nations Conference On Trade And Development update on IIAs dated April 2014 reports that, in 2013, the overall number of concluded investor-state cases pursuant to IIAs reached 274. In 2013 alone, investors initiated at least 57 such cases. Investors challenged a broad range of government measures, including changes related to investment incentive schemes, alleged breaches of contracts, alleged direct or indirect expropriation, revocation of licenses or permits, regulation of energy tariffs, allegedly wrongful criminal prosecution, land-zoning decisions, invalidation of patents and others.
Three examples of famous recent disputes:

- **Argentina:** In October 2013, it was reported that Argentina had agreed a settlement relating to five investment treaty arbitration awards made between 2005 and 2008 for more than \$450m (€395m) plus interest. Although each case concerned a different set of facts, all the claims arose out of Argentina's financial crisis and the privatisation of various industries. The cases concerned forced tariff reductions relating to water and sewage concessions and gas transport services; a devaluation of an investment in the electricity sector; and losses resulting from the devaluation of the peso and related measures taken by Argentina.
- **Russia:** On 18 July 2014, former shareholders in Yukos were awarded \$50bn in a dispute against the Russian Federation under the ECT for the expropriation of Yukos. This is the largest damages award to date in an investor-state arbitration. In 2002, Yukos was Russia's largest oil and gas company. The claim was that Russia took a series of measures (including the imposition of taxes) leading to Yukos being declared bankrupt in August 2006 and Russian state-owned companies Gazprom and Rosneft acquiring Yukos' assets at a discount.
- **Libya:** In the aftermath of Arab Spring, foreign investors initiated a string of claims against states in the MENA region. In March 2013, the Kuwaiti Conglomerate, Al Kharafi & Sons, was awarded \$935m in a dispute against Libya for its obstruction of the construction and operation of a tourism complex. This was the second largest known award.

Getting to grips with international sanctions

Q: With talk of sanctions always in the news, what do risk managers need to know and should they be concerned?

A: The threat of adverse publicity, investigations, high fines, criminal liability and consequential reputational damage has brought sanctions to the top of agenda for many risk managers.

In May, the US Department of Justice sentenced a financial institution headquartered in Paris for violations of US economic sanctions targeting Sudan, Iran and Cuba. The sentencing made headlines because it was the first time that a financial institution has been convicted and sentenced for breaches of US financial sanctions and it was the largest ever fine imposed in a criminal case. The sentencing included a five-year term of probation, an order to forfeit $8,84bn (€7.9bn) to the US and a fine of $140m.

Financial sanctions involve restrictions on trade and financial activity to address a foreign and security policy objective. Modern sanctions take various forms, such as travel bans, arms embargoes and freezing the assets of listed individuals or entities. Financial sanctions can also be comprehensive, imposing restrictions on the international trade and economic activity of an entire country.

For risk managers trying to better understand sanctions compliance, several issues should be explored as a starting point.

Which programmes apply?

Many countries operate autonomous sanctions programmes and risk managers should therefore ensure that their firms and businesses are compliant with the national sanctions laws in the country in which they are based. The EU implements UN sanctions into EU regulations that directly apply to all EU countries. EU sanctions apply to EU nationals wherever they are located, entities incorporated within the EU and any person or business in respect of any business done in whole or part within the EU.

A further layer of complexity arises in circumstances where an organisation may be affected not only by domestic and EU regulations but also by foreign sanctions programmes. For example, an insurer based in an EU member state might be affected by US sanctions because its business is owned and controlled by a US parent. US citizens might be employed in an European business that might engage in activities that are prohibited by US sanctions.

Greatest risk of exposure and prohibited activities

Risk managers need to conduct a risk assessment of the potential areas where their businesses might be exposed to sanctions. This could be influenced by the countries in which their firms do business or the nationality of the clients or those supplying services to their business.

Typically, sanctions will prohibit making funds or economic resources available to, or dealing with funds or economic resources belonging to or controlled by, sanctioned companies and individuals. Recent sectoral sanctions have restricted activities in specific areas such as oil and gas, access to capital markets. Sanctions have also restricted the provision of (re)insurance services to persons, entities and governments on sanctions lists.

Preventing breaches

It is good practice to identify when you are dealing with a listed individual or entity, either by implementing bulk screening or manually screening individuals or entities against the applicable sanctions lists, (which are generally available online). Registering to receive automated alerts is an effective way to keep on top of frequent updates to sanctions lists and legislation.

It is vital to be aware of when employees are about to engage in business that involves a sanctioned country. Communications highlighting countries subject to sanctions can be effective in raising awareness and this should be supported by a process for notifying potential sanctions matters to a central point within the organisation. Notifications provide an opportunity to review the potential risk that your organisation might conduct a prohibited activity and to advise on the best course of action.

When assessing sanctions risk, relevant factors include the nationality of all parties to the transaction, the place of incorporation and ownership of your business, the involvement of US interests (US dollars, goods of US origin). It is a good idea to standardise how this information is obtained through a paper questionnaire or electronic form.

If you have identified that you are dealing with a sanctioned party and/or your transaction or services are likely to involve a prohibited activity, withdrawing from the transaction or supply of services is not the only option. It is possible to apply for a licence from the national competent authority responsible for the administration of sanctions in the country in which you are based. If a licence is granted, it will authorise you to undertake an activity that is otherwise prohibited.

One last important area to note is that circumventing financial sanctions or enabling or facilitating an action that has the effect of circumventing sanctions is generally prohibited.

What next?

Sanctions are becoming more complex and governments are producing new ways to fashion 'smart' sanctions that address specific policy goals. This trend can be witnessed in the sectoral sanctions against Russia by the US, EU and other countries and the US president Barack Obama's recent Executive Order establishing a new sanctions regime for "significant malicious cyber-enabled activities." These co-called cyber sanctions target hackers and those complicit in cyber attacks on the US or who benefit from trade secrets, knowing that they are derived from illegal cyber activity. This recent activity points to the conclusion that this is an ever-burgeoning area of interest for risk managers, particularly those based in multinational businesses or who do business internationally.

Che Odlum is the compliance manager – financial crime and sanctions at DLA Piper UK LLP

REGULATION & LEGAL

NEW EU PRODUCT SAFETY RULES: ARE YOU READY?

With new legislation forthcoming harmonising consumer product safety and market surveillance, organisations need to start preparing now and ensure they and their supply chain understand compliance requirements

PRODUCT SAFETY IS A MAJOR CONCERN, WITH THE INFLUX of cheaper imports into the European markets. This necessitates a constant survey of markets and scrutinising of products for the risks they might pose to consumers.

In a bid to survive and remain competitive, EU industries are trying to enhance the quality of their products. However, they are beleaguered by different legislations and market surveillance systems.

To do away with the individual national regulations, the European Commission (EC) is proposing a homogeneous set of directives to simplify and harmonise consumer product safety and market surveillance in the EU. Although this legislation has not been finalised yet, organisations need to gear up for upcoming regulatory changes and start preparing now.

Current legislation and rules

- **Directive 2001/95/EC on General Product Safety** maintains the basic safety provisions with which all consumer products must comply (except for food and medical devices). Member states (MS) should ensure that: (i) products meet the applicable safety requirements; (ii) steps are taken to make products compliant; and (iii) sanctions are applied where necessary.
- **The new Approach Directive** deals with specific categories of products. Its terms are wider and incorporate technical standards to specify details for each product that falls within its framework. It includes safeguard clauses for products that may be liable to compromise the health and safety of persons, specifying that it must then be recalled from the market.
- **Regulation (EC) 765/2008 on accreditation and market surveillance** is related to the marketing of products and sets the procedures required to "establish, implement, and update national market surveillance programmes". It is important to distinguish between the harmonised and non-harmonised products. The former comprise products, such as lawn mowers, lifts and pressure equipment regulated by EU legislations.
- **Regulation 764/2008** deals with non-harmonised products, such as handbags, wooden articles and wood or toothbrushes, for instance, for which the rules have not been uniformly adopted in the EU and may vary from one MS to another. The regulation ensures that these non-harmonised products can be freely sold in all MSs on the basis of the mutual recognition procedure principle.
- **The Rapid Alert Information System** (RAPEX) enables the "rapid exchange of information between MSs and the EC on measures taken to prevent or restrict the marketing or use of products posing serious risks to the health and safety of consumers (with the exception of food and medical devices which are covered by other mechanisms)".

Proposed changes

In 2013, the EC adopted a Product Safety and Market Surveillance Package. This proposes a new regulation on: (i) consumer product safety to merge all safety rules for consumer products into a single legislation (not applicable to food and medicinal products); (ii) market surveillance for products; (iii) and a multi-annual action plan to improve market surveillance rules in the next three years. If approved, the Draft Regulation on Consumer Product Safety would create a new framework for the market surveillance of products.

Although the scope of the proposed regulation is expected to be the same, it will, however, be further clarified. It will not apply to medical devices and building materials and will apply to the harmonised and non-harmonised categories of products.

These changes are expected to simplify and make uniform the legislative and non-legislative measures, with regard to safety guidelines for non-food products distributed in the EU. In addition, these will also bring about common standards in market surveillance procedures, their co-ordination and monitoring, consumer product identification and tracking, enforcement of product safety rules, while placing additional responsibilities on stakeholders, manufacturers, importers and distributors whose products are sold in the EU.

- **Safety assessments by product categories:** under the proposed changes, safety assessments will differ according to the category of the product. For those products covered by the harmonised legislation, risk assessments will be made on the basis of the EU harmonised legislation or the national laws of the MSs or European standards. For those products not covered by harmonised legislation, risk assessments will be based on the existing national legislations, if any, or on the basis of criteria included in Directive 2001/95 (GPSD).

These proposed changes also set the responsibilities of the various stakeholders – the economic operators – which will need to guarantee the safety of the product via comprehensive documentation, list the risks posed and adopt effective solutions to mitigate these.

In addition to setting the different levels of obligations between the different economic operators, these changes may apply exceptionally to commercial products, online sales and confirm the application of the precautionary principle.

- **EU safety tested (CE plus):** a new provision called the CE Plus has been included by the European Parliament (EP) by which there should be a difference in marking for those products testified by certified labs (CE Plus), as opposed to those tested by companies internally (CE). Although some MSs rejected this, it may be reintroduced in the future.
- **Indication of origin:** although supported by the EP, this provision is a point of contention between northern and southern MSs. While the indication of a country of origin of a product has been considerably debated following pressure by Italy and France, the EC had to introduce this aspect. Under this principle, manufacturers and importers would have to include the name of the country of origin on their products. However, if the size and nature of the product did not allow for the name to be included, this would have to be inserted on all documents accompanying

the product. This provision is essential because it compliments traceability and enables consumers to easily access information on the product chain.

- **Traceability:** the EC may require economic operators to establish or adhere to a system of traceability for certain products, categories or groups of products that could bear a serious risk to health and safety of consumers owing to characteristics or conditions of usage and distribution.
- **Emerging risk:** a product about which scientific evidence shows that it presents a new or a known risk if used in new or unusual conditions that cannot be reasonably foreseen by the manufacturer is defined as emerging risk. Here, the EC can set out uniform conditions to conduct checks by reference to particular product categories or sectors.
- **Streamlined corrective actions:** the six hypothetical types of measures the economic operators are required to undertake under the GPSD have been reduced to four: (i) non-compliant product; (ii) product liable to present a risk only in certain conditions or only to certain persons; (iii) product that may present a serious risk; and (iv) product that presents a serious risk.
- **RAPEX** is extended to the notification of products presenting a risk (not only those products that bear a "serious" risk). Punitive action may be taken against those not conforming to the set of rules spans the application of sanctions, blacklisting and imposition of fines.

How to ensure compliance

The EU product safety requirements have not been finalised yet, but firms need to start preparing, keeping the many sanctions and principles in mind. Since compliance, product safety and surveillance go beyond the individual companies and extend to relationships with third parties, technology will become an enabling part of all compliance-related activities.

The first step is to understand compliance requirements and draft compliance-related rules affecting the organisation and those parts of its supply chain. It then becomes easier to adapt technology to the organisation's compliance needs. Technology can then become the backbone of all organisational and compliance-related tasks.

Below are a few key areas where technology can help:

- **Information management:** information management systems can help capture and map relevant suppliers, sub-suppliers, products, and third-party lab information in a centralised repository. A robust information management system can help manage relationships between supplier, product, material, attribute and compliance. It will provide complete visibility across the supply chain and ensure traceability.
- **Policy management:** companies can leverage technology to create, communicate and manage policies across the organisation and supply chain. Industry best policy management systems are equipped with sophisticated collaboration and workflow tools that can be used to access, create, modify, review and approve policy and procedure documents globally in a controlled manner. A centralised, web-based repository helps store and organise policy and procedure documents, map policies to compliance requirements, and provides easy search and access capabilities.
- **Risk management:** an advanced risk management tool enables organisations to design and conduct risk assessments to identify and mitigate product quality risks. Powerful risk heat maps and risk calculators will help assess, rate and prioritise risks such as non-compliance risks and consumer safety hazard risks.
- **Product testing:** technology systems can provide a single framework to create product test plans and manage each stage of testing. These systems can also facilitate integration with testing labs to import findings and results across the entire testing lifecycle. A centralised database makes it easy to manage testing information on product properties, specifications, attributes and regulatory compliance.
- **Inspection management:** technology can be adopted to automate inspection planning, sampling plans and inspection criteria. These solutions provide flexible means to manage inspection information, sample information, inspections criteria, scheduling of inspections, templates, questionnaires and workflows to manage inspections.

Probability of damage during the forseeable lifetime of the project		Severity of Injury			
		1	2	3	4
High	>50%	H	S	S	S
	>1/10	M	S	S	S
	>1/100	M	S	S	S
	>1/1 000	L	H	S	S
	>1/10 000	L	M	H	S
	>1/10 000	L	L	M	H
	>1/100 000 M	L	L	L	M
Low	<1/1 000 00	L	L	L	L

S	Serious Risk
H	High Risk
M	Medium risk
L	Low risk

- **Audit management:** audit management systems can be used to manage internal quality audits, supplier audits and external or third-party audits and inspections to determine if quality and compliance requirements are being followed. Advanced inbuilt capabilities can help plan and schedule the audits, conduct fieldwork based on audit checklists, review and analyse audit findings and initiate follow-up activities.
- **NCM & CAPA:** a sophisticated NCM & CAPA management system can be adopted to ensure centralised management and tracking of all issues and corrective/preventive actions as well as product recalls. Through automatic rule-based routing, non-conformance issues can be sent to the appropriate teams for review and disposition. These solutions have inbuilt capabilities to support issue investigation, root cause analysis, assignment of follow-up actions and initiation of corrective and preventive action.

By leveraging these areas, it is possible to streamline, integrate and automate many product safety and compliance processes spanning audits, inspections, risk assessments, product testing and preventive and curative actions. Such systems enable real-time communication and training while improving quality and safety compliance across the enterprise and supply chain, thereby offering better visibility leading to building better brands.

Further, these solutions bring all the stakeholders together on a common platform, streamlines compliance with regulations pertinent to a company's upstream and downstream processes, while tracking the product through its lifecycle for compliance with high standards of quality.

Organisations can also strengthen their compliance efforts by systematically developing reporting capabilities, filtering, storing, retrieving data when required, data crunching, appropriate data usage, and backing up and archiving current data.

Preparing for compliance

To guarantee product safety and effective market surveillance and to enable their seamless functioning across global markets, organisations need to be prepared for new and evolving compliance requirements. This also requires that management assumes greater ownership over risks, especially as stakeholders become more vocal about organisations failures and mis-steps. It is vital to understand all the proposed regulatory changes, design effective product safety compliance programmes and leverage technology to strengthen these programmes.

***Jean-Luc Laffineur** is a partner at Laffineur Law Firm and **Cédric Merahi** is a risk management specialist at MetricStream*

A POWERFUL TOOL IN AID OF ENFORCEMENT

Freezing orders are effective devices for parties seeking to protect assets fraudulently misappropriated particularly as the English courts are willing to be flexible to ensure the injunctions are effective

ENGLAND HAS LONG BEEN A FAVOURED ANCHOR jurisdiction for claimants seeking to protect assets fraudulently misappropriated from them being hidden or otherwise moved out of reach before a judgment can be secured to compel their return. The past few years and, in particular, the first half of 2015 have seen further cases clarifying how the English courts will apply their far-reaching powers. This article discusses how the English courts appear to be increasingly willing to adopt a flexible approach to ensure that freezing injunctions are properly effective, while remaining true to the principles that underpin the jurisdiction to grant freezing orders, including that:

- there must be an underlying right to protect (that is, a strong *prima facie* case of fraud);
- the order will preserve the status quo by freezing assets, not place the applicant in the position of a secured creditor; and
- the order must be easily understandable by those against whom it is to be enforced.

No direct connection with England: the wide reach of the English courts

There have been a number of recent cases where a freezing order has been granted where there is no direct connection with England. In October 2014, in *U&M Mining Zambia Ltd v Konkola* [2014] EWHC 3250 (Comm), the court continued a worldwide freezing order in support of sums awarded by a tribunal in a London-seated arbitration, where the respondent had no assets in the UK. The court accepted that the seat of the arbitration being in London (which affords supervisory powers to the English courts) provided a sufficient connection.

Making the application

An applicant must prove that: there is an underlying legal or equitable right giving rise to a cause of action; the applicant has a good arguable case; there are assets existing within the jurisdiction of the English courts (or some other connection, as discussed above); and there is a real risk of the respondent's assets being dissipated.

When applying for a freezing order (whether with worldwide effect or restricted to England and Wales) an applicant is under a strict duty to make full and frank disclosure, which includes providing information to the court that may be detrimental to the applicant's position.

> These recent cases emphasise that the English Courts will adopt a flexible, pragmatic approach when granting and enforcing freezing orders

The importance of this duty (as well as the general duty not to mislead the court) was upheld in the March decision of *Boreh v Republic of Djibouti* [2015] EWHC 769 (Comm). In *Boreh*, the court set aside a freezing injunction on the ground that a solicitor from the firm representing the applicants deliberately misled the court at the injunction application. The application relied on a conviction of terrorism against the respondent, even though, before the hearing, the applicant's solicitor had become aware of an error that rendered the conviction unsafe. This is hopefully a rare example, but illustrates the importance of the duty of full and frank disclosure and the consequences of failing to discharge that duty.

Assets covered

Freezing orders granted by the English courts operate *in personam* and will include a prohibition on the respondent(s) removing assets from England and Wales up to a total value of the claim and a prohibition or in any way disposing of, dealing with or diminishing the value of their assets wherever they are up to the same value (if the order sought is to have extra-territorial effect). The prohibition applies irrespective of whether the assets are held in the respondents' names and whether they are solely or jointly owned. The freezing injunction also extends to any assets that the respondent has the power, directly or indirectly, to dispose of or deal with as though they were their own, which specifically includes circumstances where a third party holds or controls the assets in accordance with the respondent's direct or indirect instructions. Any variation from the standard form of order sought must be specifically brought to the attention of the court.

Under the standard form freezing order, a respondent not only has to stop any dealing with the assets, but also give full disclosure as to what assets they have, on oath, at short notice. This can be a powerful tool to help uncover and protect further assets.

In June 2014, the Court of Appeal considered in *Lakatamia Shipping Company Ltd v Nobu Su* [2014] EWCA Civ 636 whether a freezing injunction could apply to underlying assets of non-defendant companies, where the non-defendant companies were directly or indirectly 100% owned by the defendant company. At first instance, the court held that the assets of the non-defendant company were subject to the freezing order, primarily because if the respondent had disposed of the assets of

the non-defendant company, his shareholding in those companies would diminish in value. The assets were covered by the freezing injunction, with a notice requirement included in the order that the company was required to give 14 days' notice before disposing of those assets. The Court of Appeal refused to vary the freezing order to remove the notice provisions, finding that, although the assets were not assets of the respondent, they were "indirectly affected" by the order as their disposal would diminish the value of the shares subject to the freezing order.

Lakatamia broadens the relief available for claimants in appropriate cases and evidences the potential willingness of the courts properly to protect assets subject to the order, irrespective of whether they are legally owned by the respondent.

The Court of Appeal had previously considered what qualifies as an asset in 2013 in *JSC BTA Bankv Ablyazov (No 10)* [2013] EWCA Civ 928. Here, the applicant sought to argue that a contractual right to draw down under an unsecured loan facility qualified as an "asset" and so was subject to a freezing injunction. The Court of Appeal held that such a right did not qualify as an asset. The purpose of a freezing injunction is to preserve assets that could ultimately be subject to enforcement, although the jurisdiction to grant a freezing order should be able to adapt to new situations, and so operate in a flexible manner. In addition, as breach of a freezing injunction has penal consequences (including, in extreme cases, the potential for imprisonment), the court held that a strict interpretation of the terms of the freezing injunction must be adopted.

In February, the Court of Appeal in *SC Mezhdunarodniy Promyshlenniy Bank v Pugachev* [2015] EWCA Civ 139 applied *Ablyazov No 10*. This decision concerned whether trust assets were subject to disclosure obligations in the freezing order. The respondent, Mr Pugachev, had disclosed that he was one of a number of beneficiaries under a trust based in New Zealand, and at first instance the court ordered him to swear an affidavit identifying details of assets subject to the trusts, and the name of the trustees and beneficiaries of the trusts. Mr Pugachev sought to overturn this order in the Court of Appeal. The court noted that assets in a discretionary trust would potentially be available for enforcement, but that this was at the discretion of the trustees. Again, the court noted that these assets were not strictly the assets of Mr Pugachev. However, the Court of Appeal, upholding the order, noted that it had jurisdiction to make freezing orders and to make whatever ancillary orders are necessary to make the freezing order truly effective. In the circumstances, providing this information would serve to make the order effective and required only information, so was unobtrusive.

How long will it last?

A freezing injunction will be granted only in aid of proceedings in support of a real cause of action. It is an aid to enforcement, rather than an end itself. In January, the Court of Appeal considered in *JSC Ukrsibbank v Polyakov* [2015] EWCA 67 when a freezing order must come to an end. The claimant, a Ukrainian bank, had commenced proceedings in Ukraine relating to personal guarantees Mr Polyakov had made with respect to certain loans. The bank obtained a worldwide freezing order in support of the Ukrainian proceedings.

The claim in Ukraine was dismissed at the final appeal stage on the ground that the guarantee given by Mr Polyakov was unenforceable. The freezing order had been maintained during the various appeal stages but now there were no live proceedings in the Ukraine. However, a third party to the claim in the Ukrainian proceedings was due to appeal the decision given in favour of Mr Polyakov, and the bank requested that the freezing injunction be maintained until that appeal was heard. The Court of Appeal held that the bank had failed to demonstrate that it had a good arguable case that the third-party appeal in Ukraine would lead to the bank obtaining a judgment against Mr Polyakov. In particular, the third-party appeal was out of time, and it was questionable that the third party was independent from the bank in bringing the claim. The court held that the applicant bank had failed to establish a good arguable case, and the injunction was discharged.

Where judgment is successfully obtained, a freezing order will usually be continued to aid enforcement. However, an application for its continuance must be specifically made to protect against dissipation post-judgment.

Conclusion

These recent cases emphasise that the English Courts will adopt a flexible, pragmatic approach when granting and enforcing freezing orders. Parties considering applying for a freezing order can take comfort in the fact that the courts will adopt measures to ensure that freezing orders are effective, and capture assets, potentially even when they are not legally owned by the respondent, so long as the order contains clear wording to this effect, amendments being made to the standard form order where necessary. The jurisdiction to make freezing orders is, however, an aid to enforcement, not a freestanding right and the courts will not grant freezing injunctions where they are not supported by a good arguable case.

***Jamie Curle** is a partner, **Sarah Ellington** is a senior associate and **Sean McGuiness** is an associate at DLA Piper UK LLP*

INVESTMENT IN RUSSIA AFTER SANCTIONS

As sanctions were imposed on Russia for its role in the Ukraine crisis, capital has flown out of the country and M&As have dwindled. With sanctions likely to remain in place for a while, should businesses stay away or will ignoring Russia as an investment destination prove a short-sighted strategy?

SANCTIONS AGAINST RUSSIA ARE LIKELY TO remain in place for the foreseeable future. A significant diplomatic breakthrough between Kiev and Moscow – and the rebuilding of trust between the Kremlin, the White House and Brussels – is needed before EU and US sanctions are lifted entirely.

Although the EU has tied the sunset of sanctions to the fulfilment of the Minsk accords – which include devolved power to rebel regions in the east of Ukraine, the withdrawal of foreign militias from the country and the restoration of Ukrainian control over its border with Russia – internal divisions between EU member states could see a progressive lifting of so-called 'sectoral sanctions' in July, which have primarily affected the banking, defence and energy sectors in Russia. The EU has called for the settlement of the peace accords by December 2015, but full compliance with the terms is unlikely since some of the measures – such as the devolution of power to the breakaway regions in the east of the country – face strong opposition in the Ukrainian parliament.

The US appears more resolute in its stance on Ukraine's territorial integrity – demanding the return of Crimea to Ukraine – and US sanctions are likely to remain in place longer.

Is investing in Russia possible in the current climate?

Since sectoral sanctions were first introduced in July 2014 – curtailing Russian access to western financial markets and placing restrictions on activities in the oil and gas sector – we have witnessed substantial capital flight and a grinding halt to M&A activity in Russia.

Many western firms have shown a reluctance to invest, compounded by the economic uncertainty created by depressed oil prices and Russian currency uncertainty, while others have been prohibited from continuing their operations. ExxonMobil, Shell and Total have all suspended joint shale oil and Arctic projects in Russia owing to bans on the provision of technology and services for exploration in these areas.

Nevertheless, a number of investors remain that take an overall positive view on investing in Russia and believe that, despite the risks, ignoring Russia as an investment destination could be short-sighted.

Where has there been investment?

Sanctions have not prevented new investments in Russia. Some of these deals include:

- The acquisition in March 2014 by Russian state oil major Rosneft of a 13% stake in Pirelli. Rosneft's chief executive, Igor Sechin, also took a seat on the board of the Italian tyre manufacturer. Rosneft is under EU and US sanctions and is prevented from accessing capital markets and certain oil field technologies, while Sechin is subject to a US visa restriction and asset freeze. Although the deal was agreed before sanctions were introduced, Pirelli maintains that it remains in compliance.
- The December 2014 acquisition by US pharmaceutical company Abbott of Veropharm – one of the leaders on the Russian pharmaceutical market.
- A December 2014 deal between Italy's Finmeccanica and Russian Helicopters – a unit of the US-sanctioned public holding company Rostec – to build 160 helicopters for Rosneft.
- The acquisition by Phoenix Mecano – the Swiss producer of industrial components – to acquire control of Electroshield-K, a Russian supplier of components for the nuclear industry, controlling approximately 15% of the market.

Even in the strategically sensitive oil and gas sector – which has borne the brunt of economic sanctions against Russia – investment activity has continued. Sanctions have not derailed the agreement between Norwegian offshore drilling company North Atlantic Drilling (NAD) and Rosneft, which would see NAD purchasing rigs from Rosneft in exchange for a 30% stake in the company. However, the closing date of the deal was recently postponed to 2017 primarily owing to the collapse in the oil price and the limited access of Rosneft to capital markets.

Russian counter-sanctions

In response to western sanctions Russia has introduced its own restrictive measures, notably prohibitions on food imports from the EU, US and others. Beyond formal sanctions, the greatest concern for investors is the sense of increased Russian isolationism and growing hostility towards western investment, which manifests itself less overtly – most often in the form of a harsher regulatory

> The biggest hidden risk lies in dealing with a counter-party that is acting on behalf of a sanctioned entity that is attempting to circumvent sanctions

environment and arbitrary refusals to grant licenses or approvals to invest.

Nevertheless – despite fears that Russia would close for business when western sanctions were introduced – there are plenty of examples where the Russian government has allowed investors to enter the market – often after some initial hesitation – as outlined above.

The case of Schlumberger

A key litmus test for foreign investment was the recent provisional approval of the Russian government's foreign investment committee – which oversees investments in strategic sectors – to allow Franco-American oilfield services company Schlumberger to purchase a 46% stake in Eurasia Drilling Company (with the option to acquire the entire company) – the largest Russian drilling contractor.

The deal looked set to collapse when Russia's Federal Antimonopoly Service (FAS) intervened on the eve of its completion, despite claims from the parties involved that the deal was not anticompetitive. It was eventually agreed that the deal could be allowed to proceed on the condition that Schlumberger sells its Eurasia Drilling assets to a Russian investor, if the company is required to suspend its operations in future owing to sanctions.

In a similar vein – the FAS announced in April that it had extended its examination of an application from Halliburton and Baker Hughes – two major US oilfield services companies – to merge their assets in Russia. Approval is ultimately expected, but the merger will likely require approval by the foreign investment committee.

The foreign investment committee will also weigh in on Glencore's decision in March 2015 to acquire 49% of Russian oil company Russneft. It is likely that the committee will rule in Glencore's favour given the Russian government's need to attract foreign investment – particularly in the hard-hit energy sector.

How to avoid sanctions exposure

Thorough due diligence is key to avoiding exposure to a sanctioned entity. When considering an investment in Russia, it is also worth considering the likely trajectory of sanctions to understand if a counter-party, which is not sanctioned today, may be sanctioned tomorrow.

Predicting the likelihood of sanctions is not an exact science, but ongoing monitoring of the political landscape, following the situation on the ground in Ukraine, and understanding where a company and its owners sit within Russian structures of power and influence, has so far proved a useful indicator of new targets, as sanctions have been deployed progressively. Understanding the political landscape is particularly important now because the atmosphere of increased adversity between Russia and the West has led to a less stable and more unpredictable business environment.

Thorough due diligence on a counter-party must include a review of its formal ownership structure and assessment of its owners' links to political elites. Investors should bear in mind that Russian individuals and companies may have sold assets or changed their ownership structure to hedge themselves against the possible fallout of sanctions. Following the imposition of US sanctions on Gennady Timchenko, co-founder of the oil trader Gunvor, Timchenko sold his 43% stake to co-founder Torbjorn Tornqvist.

In addition to understanding a counter-party's ownership structure, it is necessary to look into its directors, who may exert control over the company. 'Control' over a company is a term used by the EU in its sanctions compliance requirements and does not necessarily mean that an individual or entity owns more than 50% of a given entity.

The biggest hidden risk lies in dealing with a counter-party that is acting on behalf of a sanctioned entity that is attempting to circumvent sanctions. In addition to due diligence, lawyers advise obtaining representations and warranties from the counter-party attesting that they are not acting as intermediaries for a sanctioned entity and including an option to terminate a contract if it transpires that the counter-party is acting on behalf of a sanctioned entity.

Lawyers also note the importance of checking a company's compliance with the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010 when investing in Russia because – in the atmosphere of heightened scrutiny – there will likely be increased inspection of adherence to these regulations.

***Adam Lewis** is a political risk analyst at GPW Ltd*

Sanctions check-list

- Review the public record about your counter-party
- Review all information received from your potential counter-party
- Assess the extent of sanctions in the sector
- In addition to assessing formal ownership conduct due diligence on the company's directors
- Look for links to defence, dual-use technology and the oil and gas sector
- Check whether your counter-party operates in Crimea

THEORY & PRACTICE

Companies that embed risk management into their decision-making processes have much to gain. However, this is easier said than done

Is the concept of a corporate risk culture doomed to fail?

FINANCIAL INSTITUTIONS ARE BEING STRONGLY ENCOURAGED BY stakeholders to integrate rigorous risk management processes into their business. The aim is to assist businesses with mitigating risks.

To successfully integrate risk management into the business decision process, it is necessary to have the concept and the importance of risk management understood by all employees and strongly endorsed and monitored by senior management and the board.

This integration of risk management into the business decision process requires the establishment of a risk culture for the business. The risk culture can be thought of as the explicit and implicit understanding by all employees of what risks are acceptable and what risks are not, how to identify risks, and the need to communicate changes in risks across the business. A risk culture typically evolves from the integration of a risk statement endorsed by the board into the business decision processes and more likely to be implicit rather than explicit. Each company will have a different risk appetite and hence employees need to be very clear about what is expected.

However, the creation of this risk culture is not straightforward. As Simon Ashby, Tommaso Palermo and Michael Power reported in their paper *Risk Culture in Financial Organisations: An Interim Report* (London School of Economics and Political Science, 2012):

- "First, in contrast to public debates which emphasise values and the need to change mindsets, we learned of risk culture work streams with more of an emphasis on improving oversight structures and information flows, including performance metrics for risk and good compliance.
- "Second, from our discussions it also appeared that critical issues in risk culture were being played out in the space between what are called first and second lines of defence, suggesting that this distinction, which many take for granted, may not be helpful in advancing the debate about risk culture.
- "Third, improving risk culture was also seen by chief risk officers as a matter of improving the organisational footprint of the risk management function. This was more than just rolling out ERM systems but involved expanding the reach of informal risk processes, information sharing and escalation, and representation on key committees.
- "Fourth, we also heard concerns about a familiar issue – the role of documentation. The argument was that some documentary and evidentiary demands were creating the wrong kind of risk culture."

The first observation would seem to indicate that businesses involved in the survey were more concerned with information flows than "values", which we would argue is the appropriate process in the evolution and embedding of a risk culture in a business. Creating a risk culture will require significant communication and co-operation across all business units in order to identify risks inherent in the business and ensure they stay within agreed limits. "Values" is a different issue to risk culture, although we accept that values can affect the risks that might be taken on by a business.

A good example of this need is the management of operational risk, which is a highly complex process requiring estimations of the effectiveness of operational controls and consequent losses when operational risk events occur. This estimation process must reflect the dynamism of operational risks as the risks move to and from the 'known' state to the 'unknown' state. To ensure the overall operational risk exposure remains as close as possible to the businesses' intended maximum exposure requires effective communication across business units as operational processes change or external threats are recognised.

However, the creation of an effective risk culture across the business then flies in the face of the bureaucratic structure in place in most institutions to allow growth through isolating tasks into small, manageable and seemingly independent functions. To quote an early researcher of bureaucracies (American sociologist Peter Blau, who in 1956 wrote Bureaucracy in Modern Society): "The type of organisation designed to accomplish large-scale administrative tasks by systematically co-ordinating the work of many individuals is called a bureaucracy. The basic characteristics of bureaucratic organisation are specialisation, a hierarchy of authority, a system of rules, and impersonality".

Traumatic change

All institutions adopt a bureaucratic structure in their business, as this enables employees to be trained in specific functions rather than an entire process, which would be more difficult to train them in and would introduce greater operational risk as well as human capital risks. One of the inherent consequences of a bureaucratic structure is that there is no need for communication between the functions as they are seen as independent. Any communication across the various functions is effectively delegated to a manager responsible for the entire process. An effective risk management culture, however, requires exactly the opposite assumption to that of independence of functions, requiring the various functions to identify and communicate risks being taken on, so that the overall risk tolerance is not exceeded.

The creation of a risk culture in an institution then requires the independence of the functions be broken down, a traumatic change that institutions need to manage carefully.

Although existing parallel management structures already exist in financial institutions related to financial management, these structures relate to very finite reporting, whereas risk management frequently involves less precision as to likely outcomes and especially as to timing of the outcomes. Certainly, the business units already report on a regular basis their financial results and expected future results through some reporting structure – then there is feedback, once these are consolidated and referenced to expected overall results. However, this type of reporting and management is different to that required for risk management.

Whereas financial reporting is both historical and expectational, risk management is solely expectational, with historical risk occurrences being embedded in the historical financial reporting either explicitly, in the case of specific losses or gains, or implicitly, in the case of consequential risks such as reputational risks. Also, whereas financial results do not affect other business units, risks arising in one business unit may well have flow-on effects in other business units, and it is this necessary interaction that makes the creation of a risk culture for the group difficult to achieve.

Mind shift

An even greater challenge is broadening people's conception of risk beyond that of financial risk to encompass, for example, the organisation's profile in the media, which has huge potential for damaging an organisation's reputation, with knock-on effects on sales and recruitment as well as the morale and engagement of existing employees. Similarly high risks are at stake if the organisation is over-reliant on key personnel, with no succession planning or little depth of strength in management. A simple question organisations can ask themselves is: 'If I were a venture capitalist, would I invest in this company?'

For similar reasons, it is wise to separate board risk management committees from finance and audit committees, in order to go beyond financial indicators and ensure that attention is paid to leading indicators such as reputation and customer satisfaction. By the time the effect of such indicators is seen in financial key performance indicators, it may be too late to address. It will certainly take longer and be more costly to address.

The creation of an effective risk culture requires a complete reversal of the independence assumption behind a bureaucracy, and the creation of a view that all business units need to be considerate of the effects of their actions on other business units. Although this may be highly desirable from a shareholder value-creation perspective, it takes a complete mind shift within the organisation. The mind shift cannot be top-down driven, and it needs to be bottom-up accepted, which requires employees to understand and see the benefits of their collegiate behaviour. This is not easy to achieve. Financial services organisations typically have people who are highly competent technically but who do not always possess the greatest communication and people skills. This has led to a shift in the hiring of chief financial officers, who are now more likely to come from generalist backgrounds than accounting backgrounds, according to a recent KPMG survey of Asia-Pacific chief executives.

This is a welcome shift. However, the survey found that only 12% of chief executives thought that chief financial officers' greatest contribution came from governance, risk and compliance. KPMG Malaysia's managing partner Datuk Johan Idris said: "Chief financial officers should examine decisions through a value lens and challenge strategy from a risk perspective so that they are not bogged down in compliance and regulatory issues."

Creating a culture where everyone understands the nature of risk, and sees it as part of their role to identify emerging risks and monitor existing risks, is a complex task. It requires organisations to be willing to listen to their employees and for employees not to be afraid of highlighting potential risks. Yet, the higher people go in an organisation, the less likely it is that people will give them negative feedback. This is particularly so in high-power distance countries such as China or Malaysia. Even where leaders are given warnings from within their companies, they may ignore them, believing in their own omniscience and infallibility. Leaders can thus be blindsided by unexpected negative events. Furthermore, it is well established that whistleblowers generally suffer from their actions, even if their actions benefit their company. To make this shift will require a considerable mind shift on the part of the company's leadership. Some may be unable or unwilling to do so.

The nature of the organisational structure of financial institutions and the leadership skills of those who lead them will be the Achilles' heel of attempts to create meaningful risk cultures. Those who do address the changes outlined above will reap the benefits not only of an effective risk culture, but also an engaged workforce, with the concomitant benefits of improved productivity and innovation. A risk worth taking.

John Evans and Grace McCarthy are associate professors at the University of Wollongong's Faculty of Business

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

15-17 June
Airmic exhibition
The ACC, Liverpool
The programme comprises 34 risk- and insurance-related workshops, high-profile keynote speakers, networking opportunities and a large exhibition hall with a showcase of products and services
bit.ly/1JBB1rO

18 June
Belrim general assembly
Katoen Natie, Antwerp
bit.ly/1Fcm77y

2 July
IRM Reputation Risk seminar
Willis Building, London
This free morning seminar, held in conjunction with Willis, aims to provide the latest thinking from practitioners, legal experts and consultants who deploy Big Data techniques to bring the science to reputational risk
bit.ly/1GG376V

8 September
fastTrack foundation: Insurance Contracts
ACE Building, London
CII/IRM
CDP Points: 3 hrs (Structured)/5
bit.ly/1KrHrdF

9-11 September
DVS Symposium
The Westin Grand München Arabellapark, Munich
bit.ly/1HOdjJ3

23 September
fastTrack foundation: Risk Communications
Zurich offices, London
CII/IRM
CDP Points: 3 hrs (Structured)/5
bit.ly/1Hy3c8w

27 September
MEA Risk & Insurance Excellence Awards
Four Seasons, Dubai
Organised by the publishers of *GR* and *StrategicRISK*, 14 awards will be handed out at a gala dinner in what will be the first in the region to combine risk and insurance professionals as well as the only awards to cover the Middle East and African continent
bit.ly/1DwWPWs

28 September
The Financial Institutions Risk Briefing
Ritz Carlton, Dubai
This event hosted by *StrategicRISK* is an opportunity to share concerns with your peers from the Middle East and to identify solutions
bit.ly/1BqYWFS

4-7 October
FERMA Forum
Palazzo del Cinema di Venezia, Venice
The Forum will build on the discussions and feedback from the 2013 Forum in Maastricht and the 2014 Seminar in Brussels.
bit.ly/1KAM8VO

TOP TWEETS

1 Steve Tunstall (@TunstallAsc): #SRForum2015 @ StrategicRISK @IHG @PARIMAorg Rudi Wertheim on managing brand pic.twitter.com/HtEGRk5BMR

2 Maxwell Davis (@Maxwellcdavis): @TunstallAsc @ StrategicRISK @IHG very interesting talk – wondered if reputation is assessed separately to other risks

3 Steve Tunstall (@TunstallAsc): @maxwellcdavis @StrategicRISK @IHG my view is reputation damage is a consequence of other risks not being handled properly... Deal with specific risk issues that may give rise to brand or rep damage before during & after a crisis

4 Maxwell Davis (@Maxwellcdavis): @TunstallAsc @StrategicRISK @IHG tends to be our view as well it's a consequence just like financial or HSE

WHAT WE ARE DISCUSSING ON LINKEDIN

"Is cyber security at third-party vendors a threat to your business?"

Although organisations know they should take their own cyber security seriously, they often overlook risks at third parties.

COMMENT/ANSWER

JLT Specialty head of cyber, technology and media E&O Sarah Stephens:
"This is a great article with practical tips. Vendor risk management is a hugely important issue that cyber insurers consider when underwriting a company's cyber insurance. For companies with high-quality risk management around this area, remember that it's possible to insure the risk that a vendor cyber security failure may still occur."

CNA Europe European underwriting director technology and cyber Scott Sayce:
"Great point Sarah. All companies, regardless of size, need to put in place the correct controls to aid the prevention of possible points of entry. Once the correct controls are in place, organisations then need to turn to their cyber risk management strategy and obviously insurance is an important aspect."

Have your say here: linkd.in/1FWIfqL

FINAL WORD

"A company's cyber security is only as strong as the cyber security of its third-party vendors"

Benjamin Lawsky, superintendent of the New York State department of financial services

Cyber Sphere

Protecting businesses against Cyber risks

AXA CORPORATE SOLUTIONS

redefining / standards