A recent survey by Allianz Global Corporate & Specialty highlighted the fact that emerging risks present major challenges for risk managers. From large scale risks such as climate change through to power black outs and cybercrime, emerging risks pose many questions for the future of our respective industries.

Technological development has brought a heightened awareness of emerging risks through our ability to monitor and develop trends. However, at the same time, technology has introduced a more systemic risk where our industries are challenged by events that may not have affected us in the past.

We recognise that the increasing complexity of modern life is going to require new and different approaches to managing emerging risks, finding new ways to share the burden between companies and insurers alike. This study of emerging risks has helped us understand ways in which companies perceive risk and manage it in their daily activities.

The insurance industry has a duty to be prepared for and to deal with the complexity of emerging risks. To find solutions by working together, sharing knowledge and taking a more active role in understanding trends in business and its key markets.

I hope you value this information and look forward to finding solutions with you in the future.

Carsten Scheffel, CEO UK

Allianz Global Corporate & Specialty

April 2012
The thought of emerging Risks can keep even the best prepared risk managers awake at night.

This is especially the case when you move into the territory of Donald Rumsfeld’s famous ‘known unknowns and unknown unknowns’.

But while some emerging risks are truly new and unnerving, most others are really just old risks in new clothes.

Either way, they are risks that have to be managed, and in many cases, they are risks that the insurance industry may not be entirely comfortable with because they are difficult to identify and measure and therefore by definition to manage and transfer.

In some cases, as this report reveals, the risks can be devastating. Reputation risk is a good example of this.

As a CEO of a major corporation once said: “If my plant and assets were destroyed, but my reputation was intact, I could start again tomorrow. If my plant and assets survive, but my reputation is destroyed, I am out of business.”

Cyber risk is an example of a risk that companies are very rapidly having to come to terms with.

The speed of change with new technology means that this risk is not only emerging fast, but changing and developing into new threats all the time.

What many of the risks covered in this report have in common is that they are intangible.

And it is this that makes the risks difficult to manage, and difficult for insurers to find solutions that can be used to tackle them.

This is because insurance products in the past have largely dealt with tangible assets.

But the insurance industry is increasingly looking to offer solutions to help mitigate these emerging risks.

It is early days, but it is an opportunity which mustn’t be wasted.

This report, based on a Risk Frontiers Emerging Risks seminar held in London by Commercial Risk Europe and sponsored by Allianz, will hopefully help highlight some of the key challenges and opportunities out there.
TABLE OF CONTENTS

CHAPTER ONE  Risk Frontiers Outlook
   ‘Fortune favours the brave’ ................................................................. 5

CHAPTER TWO  State of the Market
   ‘Insurers—Ready, willing and able?’ .................................................. 7

CHAPTER THREE  Economic Outlook
   ‘Hope for the best, plan for the worst’ .............................................. 10

CHAPTER FOUR  Reputational Risk
   ‘Avoiding the road to ruin’ ................................................................. 12

CHAPTER FIVE  Energy supply and power blackout
   ‘Coping with power blackout risk’ ................................................... 17

CHAPTER SIX  New technology and cyber risk
   ‘Keeping up with the cyber threat’ .................................................. 19

Commercial Risk Europe

CRE EDITORIAL DIRECTOR
Adrian Ladbury
+44 (0) 1202 764 834 [W]
+44 (0) 7818 451 882 [M]
aladbury@commercialriskeurope.com

CRE DEPUTY EDITOR
Ben Norris
+44 (0) 7749 496 612 [M]norris@commercialriskeurope.com

REVIEW EDITOR
Tony Dowding

PUBLISHING DIRECTOR
Hugo Foster
+44 (0) 1580 201 783 [W]
+44 (0) 7894 718 724 [M]
hfoster@commercialriskeurope.com

ART DIRECTOR
Alan Booth
+44 (0) 208 123 3271 [W]
+44 (0) 7817 671 973 [M]
abooth@commercialriskeurope.com

REPORT EDITOR
Tony Dowding

PRINTING
Orchard Press Cheltenham Ltd.

DESIGN & PRODUCTION
www.calixa.biz

MAILING AGENT
A1 Mailings Services Ltd.

Rubicon Media Ltd. © 2012
All rights reserved. Reproduction or transmission of any content is prohibited without prior written agreement of the publisher
For advertising & sponsorship opportunities email hfoster@commercialriskeurope.com
Subscribe @ www.commercialriskeurope.com or email subs@commercialriskeurope.com

Commercial Risk Europe is published monthly, except August and December, by Rubicon Media Ltd.
Registered office 7 Granard Business Centre, Bunns Lane, Mill Hill, London NW7 2QO

Whilst every care has been taken in publishing this report, neither the publisher nor any of the contributors accept responsibility for any errors it may contain or for any losses howsoever arising from or in reliance upon its contents. Editeur Responsable: Adrian Ladbury.
European and international risk managers are struggling to cope with a greater level of risk velocity, and an often cunningly disguised accumulation of risk, than ever before. But almost all are agreed that there are no clusters of truly new risks on their risk radars causing the high levels of stress suffered by corporate managers worldwide. CRE Editor ADRIAN LADBURY reviewed the demands placed on risk managers by the ‘emerging risk’ landscape in his opening remarks of the Risk Frontiers seminar in London and has updated the analysis based on further meetings with risk managers in France, Australia and South Africa.

The consensus among risk managers and the insurance market is that they do not face a panoply of new risks but rather existing risks have been transformed and accelerated in new directions, with different levels of velocity and therefore potential for unexpected damage.

The huge supply chain-related losses suffered as a result of the Japanese earthquake and Thai floods are a classic example of this. The earthquake and the floods are not new phenomena but the impact is because the way companies manage their supply chain has fundamentally changed.

Paolo Rubini, Risk Manager Telecom Italia and Vice President of ANRA, the Italian risk management association, summed it up neatly as he told CRE: “I wouldn’t say we face new risks really. I would rather define them as more severe existing risks. The risks themselves have not really changed much but what has changed is their impact. These risks are tied with terrific opportunities. Technology presents a risk not because of what you can do with it but rather its misuse.”

Mr Rubini also pointed to wider social problems such as the ageing population, disparities of wealth and other problems caused by globalisation. “These are not new risks but are more severe and complex. And this can be made more difficult by the fact that everything is known simultaneously and not necessarily the right information is reaching people,” he said.

Mr Rubini’s final point about communication is an important one.

This was consistently raised across Europe last year as we carried out our annual Risk Frontiers survey but also more recently and further afield at the IRMSA conference in South Africa and at the RMIA conference in Australia in November.

COMMUNICATION AND SOCIAL MEDIA

Communication, and the role of the new and so-called ‘social’ media, was also discussed at length during the AMRAE conference in France at the start of February. It was clearly identified as a fast rising opportunity and headache for major South African companies during roundtables hosted by CRE in Johannesburg and Cape Town at the beginning of March.

It is clear that risk managers are uncomfortable with the power and reach of modern communications because it cannot be as readily controlled as in the past. One of the South African risk managers, who worked for a financial services company, pointed out that risk managers are paid to help their corporations retain control over their operations and ultimately their reputation. When accusations start flying around the web about supposedly dodgy dealings carried out by employees, the impact can be very damaging and impossible to control.

Sabine Prechtl, Head of Risk & Insurance Management at Hugo Boss and DVS board member, summed it up neatly:

“It feels riskier but I am not sure that it is because you only really see the tip of the iceberg. Also there is ever-more information that flows at an ever-faster pace and so the tip effectively becomes bigger and generates the impression that the risk is bigger. But I do question whether the risks really are bigger. Has the underlying risk really changed or just the news agenda? The danger is that, as the perception of risk changes along with the news, one can maybe lose touch with the real problems.”

As the risk managers in South Africa, Australia and Europe all agreed, and the World Economic Forum report stressed again, much of this uncertainty is caused by the interconnected nature of the global economy, supply chain in its broadest sense.

As Ms Prechtl said: “I am not so sure there are so many new risks, but the impact of existing risks could be bigger because of the global interconnectedness of the economy and processes. Companies have tightened processes and shortened lead times. In most cases this is good but it can also lead to problems and make companies more sensitive to risks when they happen.”

The bottom line is surely that risk managers must ensure that lessons from such events are truly learned and digested throughout companies.
“I think it is a riskier world and more complex. Risk management has become more mature, but with that increased sophistication management has become more demanding and now has higher expectations...” JULIA GRAHAM

As ever, companies need to identify, measure and properly manage their business risks.

But it’s no good if the risk and insurance manager is the only one who works out the true implications of such trends and events. The messages need to be digested, understood and above all communicated quickly and loudly, particularly to board members and above all non-executive board members.

Almost all risk managers agree that board members really should be making more of an effort to understand the true nature of the risks their corporations face and not just sign off bland statements in annual reports, happily take their pay cheques and saunter off to the next board meeting. This is particularly important if such events are going to lead to market reactions such as the tightening or even loss of insurance capacity in key growth markets.

If a risk manager is going to have to tell the CFO that they can’t buy any BI cover for the next catastrophe in the key emerging market unless there is a long list of alternative suppliers lined up—best start planning your explanations now. Even worse, if it is D&O cover that is evaporating.

**SUPPLY CHAIN RISK**

Supply chain is obviously the hot topic currently amongst the world’s biggest corporations and the events in Japan and Thailand laid the problem bare for all to see. One of the big conclusions to draw from our Risk Frontiers survey, further discussions with insurers and reinsurers in Monte Carlo and Baden-Baden, plus risk managers at AMRAE and the IRMSA conference, is that these supply chain problems are mainly cost-driven and this causes problems.

Marco Terzago, Risk/Insurance Manager South Europe & Asia for SKF Industrie said: “There is a very strong demand in all companies to reduce costs so they try to source raw materials from low cost countries. This increases the distance and complexity of the supply chain and so the risk is increased overall.”

Supply chain is the big one and to an extent represents the nub of the emerging risks—lack of innovation debate discussed in more depth below. But cyber risk is fast catching up and is surely only one big catastrophe away from securing top slot. The consensus from our survey is that the problem is, as with communications and to an extent reputation, really based upon a perceived loss of control.

Chris Maurice, former Risk Manager of BT, said: “The risk has not changed but our reliance on technology has increased hugely. We have moved from a paper-based economy and paper is not even the backup now. So if it goes wrong then the whole process does not work. This makes all companies vulnerable because you cannot run a business on paper now. That is the big change and we have to really risk manage this. We don’t have the same control over the electronic world that we had over the paper-based world.”

**PROACTIVE RISK MANAGEMENT**

So faced with all this uncertainty and loss of control, what on earth should companies do about it and what should the risk manager do to help regain control or at least anticipate and prepare for disasters?

The key response is to look forward not backward and be more proactive than ever before.

As Julia Graham, Chief Risk Officer, DLA Piper UK and Vice President of Ferma, said: “I think it is a riskier world and more complex. Risk management has become more mature, but with that increased sophistication management has become more demanding and now has higher expectations. Rather than looking in the rear view mirror, risk managers are increasingly trying to gauge what is coming over the horizon. But this is quite a challenge in a recession because people dig in and become short-term in their thinking and will not invest the time and energy to understand the issues.”

The response worldwide to crises has been unfortunately the creation of new regulations of all types and in all industries and this does not help engender a more strategic and forward-looking risk response.

Actually, what it does is to force companies to commit ever more scarce resources to ticking boxes and filling in forms as they are forced to pay consultants ever higher fees. But while this is a big challenge, it also presents opportunities, for insurance managers at least, to broaden their remit.

As Nicholas Bailey, Group Risk Manager at BBA Aviation, said: “The good news is that all this raises the profile of risk and risk management. I am a traditional insurance manager and have happily dealt with insurance for a long time. For strategic risk, the business needs to try and ensure that an executive is dealing with it and thinking about it and whether insurance can at least partly address it. This is why I, as an insurance manager, also need to be involved in the management of risk.”

**GRASPING THE OPPORTUNITY**

Whether risk managers are really ready to grasp this ‘opportunity’ is a big topic that was discussed at length
The second half of the question of whether risk managers themselves are willing and able to cope with the emerging risk landscape is whether or not the insurers are willing and able to help them cope with all this evolving risk and thereby embrace all the new business opportunities that come with it. CRE Editor ADRIAN LADBURY posed this critical question during his opening remarks at the Emerging Risks seminar.

ANY RISK AND INSURANCE MANAGERS in Europe and worldwide are currently demanding that their insurers emerge from their actuarial boxes. They want their core business partners to be bolder and braver to help them cope with the ever more demanding risk environment created by the global interconnected economy.

Daniel San Millán, President of Spanish risk management association IGREA and Corporate Risk Officer at Ferrovial, told CRE: “We are trying to analyse what risks we can transfer, which are not too many, no more than 20% probably. This is more or less the same level as five years ago. The insurance industry is not very innovative. Brokers and insurers are focused on their day-to-day problems. Everything is based on statistics and reports, and nothing is done if a risk does not appear in the reports of insurers and reinsurers.”

Gregor Kohler, Head of Insurance at chemical giant Bayer in Germany, said that even before looking at emerging risks, insurers need to try harder to cover the existing ones: “Some risks are not insured at all and some...”

NICHOLAS BAILEY succinctly put it in Cape Town. Again, more active and positive risk reporting and analysis would help overcome this problem, as well as clear and effective communication of the potential havoc that can be caused by emerging risks and the potential savings and benefits reaped by managing them more effectively.

Third, risk managers themselves are, on the whole, inadequately skilled to deal with the brave new world that faces them, both internally and externally. The biggest challenge appears to be internal as communication skills, above all, are evidently needed to overcome the perception of being the ‘no’ department and more actively and positively sell the benefits of risk management.

So it’s easy really. Work out what this rapidly-changing external risk landscape really means, then work out how to manage it, and then communicate that more effectively to the board and fellow managers.
“Accumulation is not really under the control of the underwriter. It’s like driving in the fog at 200 miles an hour. People need to slow down and put the lights on so that they can understand the risk...” — PHILIPPE JOUVELOT

have insufficient limits...risk transfer for traditional risks is insufficient and this is the more urgent problem rather than finding coverage for so-called new risks.”

Anne-Marie Fournier, Vice-President and Risk Manager at PPR and Vice-President of AMRAE, said that it’s not all that bad. But she did urge insurers not to overreact just when their customers need them to be there to help.

“We purchase much more insurance than five years ago, and we have increased the levels of coverage for a number of events and responsibilities. Insurers and brokers must maintain their appetite for risk and react with their eyes set on the middle and long term, instead of overreacting in the short term and waiting for the next crisis,” she said.

SUPPLY CHAINS AND BI

The supply chain problems that Japan and Thailand thrust in all our faces has reigned this debate. Munich Re told anyone who would listen in Monte Carlo and Baden-Baden that it would pull its coverage within 18 months unless buyers, brokers and insurers could find a way of much more effectively identifying, measuring and managing the risk.

Allianz Global Corporate & Specialty (AGCS) announced at the beginning of March that it was keen to offer customers non damage business interruption (NDBI) coverage but could only do so if customers showed they were on top of their risks and had back up plans in place.

The critical word is transparency and the need for risk managers to show the insurers and reinsurers that the risk is under control.

At AMRAE, AXA Corporate Solutions COO Philippe Jouvelot told CRE that he definitely expects to see a reduction in insurance capacity for CBI this year. The good news is that Mr Jouvelot said that he believes that ‘mature dialogue’ could prevent a withdrawal of capacity altogether.

But, just as Torsten Jeworrek, Head of Reinsurance at Munich Re, said during the debate hosted by Adrian Ladbury at the Monte Carlo Rendez-Vous, this would need the more active involvement of the risk management community. Risk managers would have to increase their supply options and provide insurers with better information on their supply

chain risks, said both the insurer and reinsurer.

“Accumulation is not really under the control of the underwriter. It’s like driving in the fog at 200 miles an hour. People need to slow down and put the lights on so that they can understand the risk,” said Mr Jouvelot at AMRAE. “Today there is too much of a naïve situation where the capacity is granted with unknown and uncontrolled accumulations within the portfolios.”

At the end of January the German insurance industry said the same thing as it strengthened its call for more information to help them deliver more innovative solutions. This followed a broadside from Jurand Honisch of Bertelsmann and DVS who called for a more innovative and imaginative approach from insurers at Mapfre’s annual New Year gathering in Cologne.

Stefan Sigulla, board member of HDI-Gerling Industries, former Risk Manager of Siemens and Chairman of the DVS, replied in much the same way as Mr Jouvelot did in Deauville.

“The risk landscape faced by companies is changing. If the insurance industry is to accompany this development, we will need more information,” he said.

Mr Sigulla conceded that one area where more innovative insurance is needed is when financial damage occurs without a preceding property loss—such as NDBI.

This is also where cyber risk rears its ugly head. Companies that increasingly digitalise processes and use cloud computing will face liability claims because they have lost their client’s data, said Mr Sigulla. “We have to get away from searching for a property loss or a personal claim every time a financial loss occurs,” he said.

But again, the insurer stressed that the key is more data from risk managers. “We need one thing, so we can act, and that is information, information and information,” said Mr Sigulla.

COMMON GROUND

Klaus Greimel, Head of Insurance at energy giant E.ON and current Chairman of DVS, offered the voice of reason in this ongoing spat. He told CRE that common ground has to be somehow found if progress is to be made. “Of course it is not acceptable when I have to answer five thousand questions sent by my insurer. We have to find a way to narrow down risks in a workable manner,” he said. And, Mr Greimel pointed out, this has to happen much quicker than in the past.

As Ms Fournier pointed out in the Risk Frontiers survey—insurers often react to calls for new products with far too sluggish feet.

“At the moment the gap is too large. The industry is being forced to increase speed considerably, but the insurers are lagging behind,” said Mr Greimel.

The good news is that the experts and notably former risk managers within the leading industrial insurers such as...
Mr Sigulla and Thierry van Santen, CEO of AGCS in France, are well aware that new thinking is needed. During the AMRAE conference Mr Van Santen, former Risk Manager with Groupe Danone, President of AMRAE and Ferma, rather bravely suggested that the industrial insurers clearly need to change their model to help rise to the challenges of the global economy and supply chain risks in particular.

Mr Van Santen conceded that insurers must invest in new systems and talent to properly model supply chain risk. He said in an interview with CRE that the old methods of approaching risk transfer by lines of business such as fire is no longer relevant for modern companies that operate in the global environment. He said that the industry needs new dedicated capacity and expertise to deal with previously unmodelled catastrophe risks in new and emerging territories.

New tools and models will clearly help. But it is the dedicated knowledge and capacity provided by the insurers and, of course, more information and better understanding of the risks among the risk managers, that will make a difference, he said.

Mr Van Santen said that AGCS has begun the investment in such a process already. But he stressed that the evolution has only just begun. “There is a long way to go. There is a lot of room for progress. I think that 99% of the industry has not really taken this decision yet. It needs commitment from insurers, brokers and risk managers,” he said.

THE VIEW OF THE INSURANCE INDUSTRY

It is great to see the debate properly underway in public at leading events such as AMRAE and at events in Germany. But, just as the risk message needs to be outwards and critically upwards within the corporations that are taking the risk in the first place, for real progress to be made, this message has to be understood and accepted at the top level within the insurers, reinsurers and brokers too.

During the AMRAE conference we had a chance to find out what the big cheeses thought in the main insurance panel debate. This included Evan Greenberg, CEO of ACE, Dennis Kessler, CEO of SCOR, Greg Case, CEO of Aon, Christian Hinsch, CEO of HDI Gerling, Jean-Laurent Granier of AXA and Axel Theis, CEO of AGCS.

The message from the top was actually not that encouraging. It provided a stark reminder that the industrial insurance market cannot operate in a vacuum. It also suggested that there is plenty of room for more argument and persuasion before real progress can be made.

The bosses at AMRAE said that they are worried about pressures on capital and the parallel rising demand from customers for more innovation. The CEOs were quick to remind French risk managers that regulatory changes such as Solvency II can only lead to a higher cost of capital.

The CEOs reminded the audience that they have to deliver consistently decent returns to investors if they are to maintain a healthy flow of capital. Only by doing this can insurers offer the capital to help customers deal with emerging risks and provide innovative solutions and meaningful capacity.

“That all sounded like a ‘bit of a chicken and egg’ situation.” And just in case the risk managers in the audience were not listening properly, Mr Greenberg spelled it out in simple terms. “The industry [historically] has a lousy return on capital. We want capital that is more fungible, that can come in and out. But it needs to be attracted by the returns that we can offer, otherwise capital will be allocated to some other business,” he said. “Innovation can only go as far as clients are willing to actually pay for it,” he added.

Mr Greenberg was backed up by the others. SCOR’s Mr Kessler reckons that the ‘capital intensity’ of the business has doubled over the last 20 years. “When you needed one euro of capital for each amount of premium then, you need two euros today. It is a fact that, to carry new risks, we need more capital,” he said.

Axel Theis of AGCS conceded that the industry has perhaps not been innovative enough in the past. But he pointed out how difficult it is to benefit from innovation in this business because the products are so easily copied. And he also pointed out that the word ‘innovation’ can be abused.

“Sometimes innovation is just another word for more coverage for the same price,” Mr Theis said.

Aon’s Greg Case was perhaps obliged to be a little more conciliatory as the man in the middle. He said that, in the current market, the industry cannot afford the luxury of not coming up with creative ideas. “The onus on us—the brokers and insurers—is to be ahead on innovation,” Mr Case said. “We have to be ahead on understanding risk.”

Christian Hinsch, of HDI Gerling, agreed with Mr Case. But he pointed out that innovation becomes ever more challenging because insurance buyers have the temerity to increasingly demand tailor-made solutions. “The most important thing for us, insurers and reinsurers, is to increasingly individualise our services. Companies are becoming more and more differentiated, and we have to specialise in certain industries and services, according to their needs,” he said.

INNOVATION CANNOT BE IGNORED

So it is not an easy nut to crack, this innovation thing. But, no matter how difficult it may be, it cannot be ignored. The world appears to be wedded to a globalisation process that is based on ever changing and faster new technologies and a demand for ever more efficiency.

That means that, by definition, risk will continue to accelerate, and rise in severity and diversity. What is interesting is that the risks themselves are being taken and embraced by investment risk capital in the first place.

So how that risk capital can continue to flow in at the
back end but not be found in sufficient quantity to play at the front end is surely a conundrum to which a solution must be found.

If it is simply a question of price then that means that risk and insurance managers with larger corporations will ultimately be forced to retain more and spend more time playing with their retentions and captives. If that occurs then the insurers will presumably have to focus on the higher priced fat tail…and inevitably consolidate.

This is a result no one wants to see, except perhaps for captive managers.

If more risk capital can be released for these ‘new’ risks through greater partnership and transparency between risk managers, brokers and insurers then it must happen sooner rather than later.

If it does not occur then the whole adaption process will slow down, a capacity crunch will occur in those areas where coverage is most needed, and risk managers will again have to work out new ways of retaining more. Whichever way it goes it smells like more cost because more modelling and bespoke solutions inevitably come at a price.

**CHAPTER THREE — ECONOMIC OUTLOOK**

Hope for the best, plan for the worst

Richard Hewitt, Allianz economist gave a cautiously upbeat outlook for the global and European economies at Commercial Risk Europe’s Risk Frontiers Emerging Risks seminar. While he warned that Europe still faces a longer path back to financial health from the financial crisis, he flagged up recent signs of recovery in advanced economies, particularly the US, and the strong growth among emerging economies.

There has been a material uptick in global growth rates since the aftermath of the financial crisis. This is fundamentally the result of continued strong growth in emerging markets and of decisions in advanced economies to loosen monetary policy and give impetus to growth, said Richard Hewitt, Allianz SE Economic Research & Corporate Development.

Better than expected manufacturing figures at the start of this year, improved investor confidence, increased merger and acquisitions (M&A) and positive growth rates in certain key economies, including the US, are all positive developments.

There has been a shift in investor sentiment from defensive stocks, in sectors like healthcare, utilities and telecoms, into growth stocks ranging from basic materials to a recovery in financials. “This shows that investors are becoming more confident about economic recovery. They recognise that it might be rather meagre in certain areas but that there are export markets to shoot for, so confidence is slowly growing,” explained the Allianz strategist.

But, addressing the audience gathered in London, Mr Hewitt explained that growth is still being held back in Europe and further afield by deleveraging of the debt mountain and deep rooted structural issues.

Policymakers are heading us in the right direction and there are signs that the real economy has picked up again, but the crisis in the eurozone and its knock-on effects for European financial markets remains the biggest threat to global economic growth, Mr Hewitt told the audience of risk managers and insurance professionals.

He also warned that companies, particularly in the UK, will have to self fund future growth as, for the time being, the clogged up banking system and financial markets are not going to supply much of the monetary fuel to drive investment and growth.

And Mr Hewitt added that a number of elections planned for this year, notably in Greece and France, could have far reaching consequences on the future shape of the European and global response to the financial crisis and eurozone troubles.

“I see a balanced picture, perhaps a little more on the more optimistic side, but there are reasons still to be very concerned and the fact is that Europe, in particular, has a long way to go in terms of building a robust economic recovery. So, it’s about hoping for the best but preparing for the worst, because I don’t think we are entirely out of the woods yet,” Mr Hewitt explained.

**US GROWTH RISING**

“Overall there is a mixed picture in the world economy. The US is doing quite well, compared to Europe, but really it is the emerging markets that are driving global growth,” he added.

According to Mr Hewitt the US economy is now bouncing back quite strongly. It saw GDP growth of 1.7% in 2011 and Allianz expects this to increase to 2.1% in 2012. It produced stronger than expected manufacturing figures in the fourth quarter showing 4% growth in the sector.

“US growth will be a bit erratic, but overall it is going pretty well and we are starting to see the effects of growth on unemployment which is falling,” said Mr Hewitt.
Unemployment remains high at above 8% but there is a downward pattern. The European Union saw growth in Gross Domestic Product (GDP) of 1.5% in 2011. But, Allianz predicts this will fall to 0.6% in 2012.

“This year Europe is going to be driven very much by fiscal contraction, what is happening in the financial markets and weak confidence generally,” said Mr Hewitt.

There is also a sharp division between the economies of southern and northern Europe. The north is benefitting from export markets and relatively benign unemployment, whilst the south is struggling with fiscal austerity, lack of available credit and very high unemployment. Worryingly overall unemployment in Europe is at a 13 year high of 10.4%.

“The real danger to global economic growth is Europe and what happens with the current crisis in the euro and its financial markets. Will this have contagion for the rest of the world’s growth prospects? This is the big unknown in terms of the economy at the moment,” he warned.

“We don’t know where a Greek exit from the euro would lead, its knock-on effects and where all global financial interconnections are. During the crisis of 2007 to 2009, as a consequence of some financial institutions seizing up, confidence evaporated immediately and credit dried up. Global trade froze and the world’s GDP probably dropped by around 5%. In the UK, it was by about 7%, and a similar amount in Germany. I am not saying the same would happen if Greece left the euro today, but there is a not insignificant risk of contagion that could be quite frightening. So, I am not a fan of dissolution, let’s keep Greece in the euro,” he said.

Focusing on the UK, Mr Hewitt said that the growth outlook for this year is ‘pretty meagre’. Its GDP dropped 0.2% in the fourth quarter of 2011. Allianz predicts overall UK growth of just 0.8% in 2012 with probable stagnation in the first half of the year because of sluggish domestic demand and a contraction of credit markets. But the insurer’s economists do not foresee a double dip recession because companies’ balance sheets are generally in ‘pretty good shape’.

Japan’s economy is expected to bounce back in 2012 and record growth rates of 2.1% after last year’s earthquake and tsunami tipped it into recession.

**EMERGING MARKETS AND EXPORTS TO THE RESCUE?**

The only signs of significant growth though are in emerging markets. This is aiding global financial recovery. These markets offer companies in developed economies an ever expanding customer base, which in these times is crucial.

China is still showing spectacular growth rates despite the fiscal problems in other economies. It grew 9.3% in 2011. Allianz expects this to fall to 8.5% this year because of a cooling of the housing market and subsequent forecasts from the Chinese government confirmed this outlook.

Russia saw growth of 4% in 2011 and Allianz predicts 3.7% in 2012. Brazil is expected to record 3.2% growth this year.
CHAPTER THREE — ECONOMIC OUTLOOK

But this policy is having varied success in different economies and although policymakers are in general headed in the right direction there is still a long way to go, in Europe in particular, and more needs to be done to reform and support growth, Mr Hewitt explained.

“For recovery to take hold, credit and liquidity are going to be vital, they are the fuel that companies are going to need to support their growth trajectories,” he said. “I expect a lot of that will come from internal resources. I think that a lot of companies have done, by and large, a pretty good job at strengthening their balance sheets to support that. It is still very hard to see, in the UK in particular, that the banking system and the financial markets are really providing a lot of fuel to support growth,” he added.

CHAPTER FOUR — REPUTATIONAL RISK

Avoiding the road to ruin

Reputation is perhaps the most crucial element of an organisation’s success, and it is certainly the ultimate asset of any company. Reputational risk is a difficult risk to define, measure and analyse, but it has been moving up the corporate agenda in recent years, driven by various crises that have hit major corporations, resulting in damage to their reputation or brand.

Professor Alan Punter discussed the findings of latest research on the topic familiar. The study investigated 18 high profile corporate crises from 1999 to 2009, including companies such as AIG, Arthur Andersen, BP, Cadbury Schweppes, Enron, Firestone, Northern Rock, and Société Générale.

Mr Punter explained that the cases were from the decade 1999–2009, not more recent. “They were chosen such that they were at least a couple of years old, so there was a degree of maturity, so you could see what the events were, and begin to monitor what the impacts were,” he said.

He added that there were plenty of candidates that have appeared in the last few years that could be used if the study were to be repeated—UBS, Soc Gen’s rogue trader, Toyota’s product recall, Allen Stanford, Olympus in Japan, News Corporation, and so on.

The report looked at the key consequences of the case studies:

- In seven cases out of the 18 cases studies, the company collapsed and/or faced a government rescue (AIG, Arthur Andersen, Enron, Independent Insurance, Land of Leather, Northern Rock and Network Rail)
- In 11 cases, the chairman or CEO lost their job
- In 16 cases, the company and/or senior executives were fined
- In 4 cases, senior management or board members were jailed.

Clearly, said Mr Punter, the consequences were fairly severe, and that’s just the measurable ones. Others could be much more severe, and much more difficult to measure,
such as loss of market capitalisation and damage to the reputation of the company.

He pointed out in many of the cases, some of the outside agencies were culpable including auditors, regulators, and credit rating agencies, who failed to take action, or significant action, in many of these cases.

THE KEY LESSONS
The first lesson was to do with board skills and dysfunctional boards, where the boards or non-executive directors appear not to be in control of the business or did not understand the fatal flaw in the business model, or did not stand up to dominant CEOs.

A major problem was that even if questions were asked, and concerns were raised, in quite a few of the companies, the CEO was very dominant and didn’t brook any arguments, and had their executives and boards under the thumb, said Mr Punter.

“The leaders were lacking the skills necessary to exercise oversight of the business,” he said. He was particularly scathing about non-executive directors, or as he put it, “NEDs or Non-Effective Directors.” These non-executive directors often appeared to not have the skills and experience they might need to supervise or advise on a business. The problem was that they were too often political appointees, academics, or city grandees. He described them as “a trophy board not a board of business people.” For example, he said the board of Independent Insurance included bankers and city grandees, none of whom had any discernible insurance expertise according to their biographies. “So, maybe they weren’t aware of the sort of games you can play with setting reserves, long tail reserves on business and the games that were being played by the senior executives,” said Mr Punter.

Another key lesson was what Mr Punter called “board risk blindness.” He described this as not focusing on what is important to the company, what could put the company out of business, what could damage its reputation and what could lead to it losing its license to operate.

A third key lesson was a failure of board leadership and implementation on ethos and culture. He said this included the board not setting and universally applying an adequate and coherent business and moral compass, and the board failing to create and embed throughout the organisation a coherent strategy on safety matters.

And the final lesson was the defective flow of risk information, both across the organisation and from bottom to top. Mr Punter pointed to a “risk glass ceiling” with an inability and unwillingness of risk management and internal audit to report on risks up to the C-suite or the non-executive directors, particularly risks arising from strategy or behaviour or culture as opposed to operations.

“Risks that the risk manager maybe thinks he doesn’t have the brief to report on. To say there’s some fraud going on here, or the treatment of expenses in this department isn’t right, and it might be a signal that the ethics and the culture in this department are wrong in other ways. So there were warning signs in many of these companies,” said Mr Punter.

So what needs to be done? According to Mr Punter, it is vital that risk professionals extend their skills to be able to, and to feel competent to, identify and analyse risks emerging from their company’s ethos, culture and strategy, and their leaders’ activities and behaviour. He said that risk professionals need a raised status so they can report and discuss all they find on these matters at all levels, including board level.

“These are the emerging risks, the sort of behavioural risks that aren’t on anyone’s clipboard, but in many of these cases lead to the company being brought down,” said Mr Punter.

He said there needed to be a rethink from the board level down of the scope, purpose and practicalities of risk management to capture emerging risks not identified by current techniques. And above all, he said, boards, particularly the chairman and non-executive directors, need to recognise the importance of these emerging risks.

THE CASE STUDIES
CORPORATE MISCONDUCT—
FRAUDULENT ACCOUNTING AND OTHER
- AIG and AIG Financial Products (2005 & 2007)
- Arthur Andersen (2001)
- Enron (2001)
- Independent Insurance (2001)—insurance company under-reserving
- Northern Rock (2007)—UK bank failure
- Shell (2001 to 2004)—over-statement of oil and gas reserves
- Société Générale (2008)—Jérôme Kerviel rogue trading

EXPLOSION AND FIRE
- BP Texas City Refinery (2005)
- Buncefield: Hertfordshire Oil Storage Ltd (2005)

IT-RELATED
- EADS Airbus A380 (2004 onwards)—launch delay
- UK Passport Agency (1998/9)—new IT system
- HSBC/Zurich/Nationwide (2006–2008)—data loss

PRODUCT-RELATED
- Cadbury Schweppes (2006)—salmonella
- Coca-Cola (2004)—Dasani mineral water UK launch
- Firestone (1978 and 2000 onwards) tyre recalls
- Land of Leather (2007 onwards)—product liability and recall
- Maclaren (2009) US and UK pushchairs recall

TRANSPORT
- Great Heck, Hatfield and Potters Bar (2000–2002)—UK rail crashes
CASE STUDY—BP, TEXAS CITY REFINERY

BP had been through a spate of growth, with a number of takeovers and mergers in 1998–2000. Within three years it had more or less doubled its size by three large US acquisitions.

BP America was its largest division with headquarters in Houston, Texas and the Texas city refinery was BPs largest refinery worldwide. It had a poor record of maintenance under Omoco’s previous ownership. It continued that poor history of maintenance and incidence under BP’s ownership from 1998 onwards until the defining event in 2005. This saw an explosion that killed 15 people and injured many hundreds both within the site and close to it.

The employees on the site had commissioned a report by consulting firms in 2005, which stated: “We have never seen a site where the notion ‘I could die today’ was so real.” That was in January 2005, and the explosion happened in March 2005.

BP’s immediate response was very good. Senior management flew overnight to the refinery and stood up the next day and said that BP was responsible for all that happened on its sites and this was no exception. It provided support to all the victims and their families, provided full resources dedicated to the investigation, the cause and preventing any reoccurrence, full cooperation with governments and any other official investigations, and release of findings. So immediate crisis management followed the textbook.

The impact on BP’s share price and reputation is difficult to measure. It didn’t impact BP’s reputation as measured by share price. But there was a financial cost for the next couple of years—criminal fines, health and safety fines, compensation claims and so on—involving hundreds of millions of dollars. And with Alaskan oil spills, and Deep Water Horizon, it was part of a series of events that went wrong for BP.

RISK MANAGEMENT LESSONS

Rapid growth resulting in organisation complexity: The management structure and the health and safety procedures in the refinery hadn’t been consolidated and rationalised. Management commitment—not walking the walk: The board talked health and safety and then cut costs. Management did not take accountability of safety, said one report.

Take notice of early warning signals: There had been 23 earlier fatalities at the Texas city refinery, some under Omoco’s watch but some under BP’s watch. Learning from your own experience: BP was heavily criticised by the regulators in some of the official reports for having had very similar events at the Grangemouth refinery a few years earlier and having not learnt and transferred the knowledge from Grangemouth in Scotland over to their operations in Texas city which was, after all, the larger refinery.

Compliance should be more proactive: BP’s internal audit in compliance seemed to be pure box ticking. And where there were recommendations, they weren’t followed up.

Challenge or opportunity

Reputation risk is a challenge for risk managers, not helped by the fact that it is largely uninsurable at the moment. But according to Phil Ellis, CEO of Willis Structured Risk Solutions, reputation risk represents an enormous opportunity for the insurance industry, despite some big hurdles that will have to be overcome, not least dealing with the industry’s own culture, mind-set and business models.

WILLIS’ OWN RESEARCH, BASED on a survey of 600 publicaly-held companies, suggests that 95% of major corporations in the last twenty years have suffered at least one serious reputation-damaging event. Just about every major corporation goes through a crisis of one sort or another that affects its reputation in a very serious way and on average, this happens about once every seven years, according to Willis’ research. The research showed that these 600 publicly-held companies had faced 1,853 crisis events, of which 50% were due to a failure of the company’s strategy or business model.

Mr Ellis pointed to the Lloyd’s Risk Index, a review of the leading risks according to a survey of 500 C-suite board level executives. In the latest Risk Index, 2011, the top five risks were:

- Loss of customers
- Talent and skills shortages
- Reputational risk
- Currency fluctuation
- Changing legislation.

Mr Ellis pointed out that these risks are, by and large, uninsurable at the moment. “So now this is another opportunity for us because the C-Suite is worried about these kind of issues and we are not addressing them. There is a huge space for us to move into.” He added that in the Lloyd’s Risk Index 2009, reputation was ninth on the list. “So reputation is right in the thick of things, currently,” he said.

One of the problems with reputation risk, said Mr Ellis, is that owners, investors, suppliers, partners and customers all think of reputation risk, and measure it, in very different ways. “Each group measures reputation differently and some of these measures are in conflict with one another,” he said. Investors typically are concerned about
quarter to quarter results, whereas employees have a much longer-term horizon. And customers measure reputation in different ways, from the highly emotional to the highly pragmatic.

"The point is, reputation means different things to different stakeholders and that is one of our challenges," said Mr Ellis. "The other challenge is that reputation risk is not really a risk at all. Reputation is an outcome, it’s a consequence of a lot of different decisions, a lot of different factors. As Benjamin Franklin once said, good reputation is a result of many good decisions and this, in fact, means the measurement of transfer of reputation risk is certainly not straightforward."

He explained that the insurance industry deals, by and large, with protecting against major perils. Reputation risk is the result of many different factors, and so the insurance industry’s standard products are not fit for purpose to solve reputation issues, he said. "We’re going to change that, but this means changing our mind-set and changing our business laws which is no small challenge," he added.

Mr Ellis said there was one measure of reputation that just about every stakeholder would recognise and acknowledge, and that is market capitalisation or share price. "And if a company suffers a significant and sustained reversal on what it’s worth then all stakeholders would be concerned," he said.

The crises covered in the Willis research included everything from 9/11 repercussions, to rumours of product contamination. Crises resulting in a reversal of market capitalisation can happen for all kinds of reasons, he said, and that is one of the challenges for the insurance industry, because you cannot predict what’s going to cause a reputation crisis.

About 50% of the events had to do with problems with the company’s business strategy model, about 15% were lawsuits, and 10% were M&A related issues. And notably, until 2011, natural catastrophes didn’t figure—the one area where the insurance industry has huge expertise, and a lot of products to offer, he said.

He stressed that these reversals happen to the best companies, they are difficult to predict, and the result can often be liquidity issues and executive job loss. He explained that in many cases, a classic pattern starts to emerge. Almost always there is a liquidity issue, some more severe than others, and the stock price slides. Lines of credit dry up, he explained, and new lines of credit are only available at unfavourable rates.

Is there a role for insurance in all of this? The answer, according to Mr Ellis, is that there should be a role for insurers, and it represents a big opportunity for the industry, but at the moment, the risk is not transferable, though he stressed that the insurance industry is working on solutions.

What do clients want and need from a reputation protection product? They need immediate payment. And they want no, or few, exclusions. “These crises happen for a limitless number of reasons. There are often a multitude of perils behind them. We cannot design a product that is peril related, to treat this position. Products need to be priced significantly below the cost of capital in order to be rational and economical from a risk financing perspective. And they require very high levels," he said.

He said it was possible to meet these specifications, but it was hard, very hard, and would require a change of mind-set. It would also probably involve the capital markets. Mr Ellis said, “There are discussions with capital markets, and they are interested. One of the biggest challenges with the capital markets is that they look at the upside, they are optimists, while the insurance industry looks at the downside. So we talk a different language…Capital markets are comfortable with parametrics, and with providing capital quickly, but they are uncomfortable in providing capital when there is a crisis.”

He summed up:

- Attacks on reputation happen every seven years for major corporations
- When they happen, credit and management are threatened
- It’s not possible to predict what will cause these attacks
- Traditional insurance products and recent attempts don’t offer much help
- However, he concluded on an optimistic note: “Help may be on its way.”

"The crises covered in the Willis research included everything from 9/11 repercussions, to rumours of product contamination. Crises resulting in a reversal of market capitalisation can happen for all kinds of reasons..."  PHIL ELLIS
CHAPTER FOUR — REPUTATIONAL RISK

Reputational Risk Q&A

QUESTION: The capital markets are interested. What is your sense that this needs a completely different model, maybe a parametric structure rather than a contract-based structure?

PHIL ELLIS: Parametrics are definitely involved in the solution, they have to be. One of the biggest challenges we have in the capital markets is speaking different languages—we do see it differently and capital markets traditionally focus on financing the upside. It has been a long process. They are comfortable with parametrics and with providing capital quickly, but their discomfort is with providing capital when there is a crisis, and this is something we've had to solve with them.

QUESTION: If you were to go to a public affairs conference, you would be having exactly the same type of conversation and a parallel concern within the same enterprise structure. How would you foresee, or even advise, on a closer tactical strategic integration with public affairs and risk management teams within an organisation?

ALAN PUNTER: When boards hear Enterprise Risk Management (ERM) they think about outcomes rather than just think about the perils, because making a list of perils can be infinite. So in terms of outcomes, for example, for Network Rail, it might be ‘what could lead to us losing our license’, and then work back from that. Working back from significant outcomes and looking at what are some of the risks that might cause that outcome to come about, and try and manage some of those risks.

PHIL ELLIS: That's exactly what we try to do—instead of starting with the risk register, we say ‘what's the crisis to you?’ and then work back from that crisis we invented for ourselves’, so that when the real one happens they are in a better position and better prepared.

ALAN PUNTER: For example, for years Shell had conducted scenario analyses, three or four major scenarios each year. And that prepares you, not because one of those scenarios actually happens but because they have the mind-set of ‘how do we tackle this crisis we invented for ourselves’, so that when the real one happens they are in a better position and better prepared.

QUESTION: Isn't part of a solution here ensuring that companies revisit integrated, enterprise risk management and ensure that they're getting information coming up through the organisation?

PHIL ELLIS: It's perhaps a question of terminology and language. When boards hear Enterprise Risk Management (ERM) they think quite often middle management compliance, huge processes, all that sort of thing. There is a front end to ERM which has to engage the board around what the risk strategy is, what is your appetite, what is a crisis to you, what are your leading risks? Because boards will give you ten minutes or maybe half an hour if you're lucky on a particular topic, and you have to grab them and engage them. The typical ERM response doesn’t engage boards very well.

ALAN PUNTER: If the risk managers don't get the board's full attention on a regular or consistent basis, then the people that should be asking the question ‘what can go wrong?’ should be the non-executive directors.

QUESTION: Reputation is an outcome not a risk so therefore you should manage the risk and make sure the issue doesn’t occur in the first place. So isn't it, therefore, Darwinism? No matter what happens, the wrong ones don’t survive?

PHIL ELLIS: I think part of the answer would be for companies to think about outcomes rather than just think about the perils, because making a list of perils can be infinite. So in terms of outcomes, for example, for Network Rail, it might be ‘what could lead to us losing our license’, and then work back from that. Working back from significant outcomes and looking at what are some of the risks that might cause that outcome to come about, and try and manage some of those risks.

ALAN PUNTER: For example, for years Shell had conducted scenario analyses, three or four major scenarios each year. And that prepares you, not because one of those scenarios actually happens but because they have the mind-set of ‘how do we tackle this crisis we invented for ourselves’, so that when the real one happens they are in a better position and better prepared.

QUESTION: Isn't part of a solution here ensuring that companies revisit integrated, enterprise risk management and ensure that they're getting information coming up through the organisation?

PHIL ELLIS: It's perhaps a question of terminology and language. When boards hear Enterprise Risk Management (ERM) they think quite often middle management compliance, huge processes, all that sort of thing. There is a front end to ERM which has to engage the board around what the risk strategy is, what is your appetite, what is a crisis to you, what are your leading risks? Because boards will give you ten minutes or maybe half an hour if you're lucky on a particular topic, and you have to grab them and engage them. The typical ERM response doesn’t engage boards very well.

ALAN PUNTER: If the risk managers don't get the board's full attention on a regular or consistent basis, then the people that should be asking the question ‘what can go wrong?’ should be the non-executive directors.

ALAN PUNTER: I think part of the answer would be for companies to think about outcomes rather than just think about the perils, because making a list of perils can be infinite. So in terms of outcomes, for example, for Network Rail, it might be ‘what could lead to us losing our license’, and then work back from that. Working back from significant outcomes and looking at what are some of the risks that might cause that outcome to come about, and try and manage some of those risks.

ALAN PUNTER: For example, for years Shell had conducted scenario analyses, three or four major scenarios each year. And that prepares you, not because one of those scenarios actually happens but because they have the mind-set of ‘how do we tackle this crisis we invented for ourselves’, so that when the real one happens they are in a better position and better prepared.

QUESTION: Isn't part of a solution here ensuring that companies revisit integrated, enterprise risk management and ensure that they’re getting information coming up through the organisation?

PHIL ELLIS: It’s perhaps a question of terminology and language. When boards hear Enterprise Risk Management (ERM) they think quite often middle management compliance, huge processes, all that sort of thing. There is a front end to ERM which has to engage the board around what the risk strategy is, what is your appetite, what is a crisis to you, what are your leading risks? Because boards will give you ten minutes or maybe half an hour if you’re lucky on a particular topic, and you have to grab them and engage them. The typical ERM response doesn’t engage boards very well.

ALAN PUNTER: If the risk managers don't get the board's full attention on a regular or consistent basis, then the people that should be asking the question ‘what can go wrong?’ should be the non-executive directors.
History shows that power blackouts are nothing new, but they have been in the headlines in recent years because of the severe impact that they can have on organisations and people. Power blackouts are a systemic failure and blackout costs are significant and increasing. But, according to Michael Bruch, Emerging Risks, Allianz, the insurance industry is working hard to come up with risk transfer solutions.

**From a Historical Perspective, There**

are three main causes of power blackouts, Mr Bruch told the seminar. The first is a lack of maintenance, human error or equipment failure, as seen in the New York State blackout in 2003. The second is ineffective communication and emergency response, as in the blackouts across Italy and Switzerland in 2003, or Germany in 2006. And finally there are space weather events such as solar flares and eruptions. He added that now, of course, there is also the worst-case nightmare scenario: power generators destroyed by cyber-attack.

Based on historical blackouts, said Mr Bruch, it is clear that there often isn’t a single trigger, it is a combination of different failures which are interconnected and interlinked with each other. For example, he said, climate change leads to more heatwaves, which means that you start running out of cooling water in the rivers, or the temperature of the rivers is too high that you are not able to cool power plants.

He explained that as far as power supply security is concerned, central Europe is in a good position—for example, in Germany the system average interruption duration (SAID) is around 17 minutes per customer in each year, compared to around 100–200 minutes in Scandinavia or eastern Europe. Interestingly, the US grid is five to ten times less reliable than in major European countries, and it is estimated that each power blackout per year in the US results in economic losses of between $80 bn and $188 bn.

So why is blackout risk on an increase? According to Mr Bruch, it is not so much in terms of the number of blackouts, but because the impact of blackouts is more significant, especially for industrialised countries, than in the past. He said the reasons are to do with insufficient investment in power supply infrastructure, and the focus on renewable energies, where there are longer distances to consumers and higher source volatility. And there is also the issue of greater interconnectivity and a higher dependency of all industrial sectors.

Mr Bruch particularly highlighted the issue of everything being interconnected. “If there is a power blackout, this easily has a domino and cascading effect into the banking and finance sector, government services, and especially the emergency services.”

**The Growing Cost of Blackout**

As a result, blackout costs are significant. For example, the cost for the financial trading sector of a blackout is estimated to be around €6 million per hour. For the telecommunications sector, the cost is €30,000 per minute. For semiconductor production, a blackout event costs around €3.8 million. A blackout event costs a steel works around €350,000, or a computer centre around €750,000.

Mr Bruch pointed out that there are a number of business interruption trends causing concern, not least the increasing ‘just-in-time’ production tendencies, but also the fact that there are smaller groups of critical suppliers concentrated in specific regions. And major suppliers may be located in countries with a low quality of electricity supply, such as Southeast Asia.

Mr Bruch emphasised the importance of testing. He said that many vulnerable companies in the steel, aluminium, and data computing industries have diesel generators or backup power supplies, but often when the power blackout hits the company, it can find that the diesel generator doesn’t work because they hadn’t done any testing in the past.

As far as the power supply industry is concerned, there are a number of issues, said Mr Bruch. One of the significant trends, he said, is a very broad decentralisation in the electricity market with different flows of electricity, and the current infrastructure is not designed to cope with these issues. He said that to balance renewable energies with demand, the industry needs to have smarter grids which can cope with the challenges.

Two other important issues for the power supply
THE UK: GAS SUPPLY CONCERNS

The specific issue of the UK gas security policy might not be directly relevant to what risk managers deal with on a daily basis. But it is relevant to business, and as Dr Pierre Noël, Director of Energy Policy Forum, Judge Business School, University of Cambridge, pointed out during his speech at the emerging risks seminar: “It’s taking place upstream, perhaps, of your businesses, and it is managed as a risk by government, by public policy.”

Dr Noël said that the UK gas security policy is now an issue because the UK is transforming rapidly from self-sufficiency in natural gas to being a large importer, and there are growing calls for government intervention.

“There are concerns that have been arising for a number of years now, since about 2005/6 when the big price spike happened, and those concerns are about access to gas and price volatility, and those concerns drive calls for the government to intervene in this market and to address directly the gas supply security risk.”

He maintained that the access to gas problem was probably overdone. “The UK market is increasingly integrated into the European market which itself is increasingly integrating into a global market,” he said. “This market will attract gas, but it will attract it at a price that is determined increasingly by a global supply and demand, and not UK supply and demand, and not even European supply and demand.”

He pointed to a study from an energy consultancy which had concluded that there was enough capacity, both storage and import capacity, to meet peak demand in various scenarios of supply disruption in the UK.

However, Dr Noël warned: “It’s true to say that there might be enough capacity to meet peak demand in any conceivable scenario, but capacity is not gas. Capacity is the ability to go to the market and pay the price you have to pay to get the commodity. So this market might be secure in that sense but it is exposed to price spikes. So if some of your businesses are concerned about the price of gas there is nothing the government can do about that,” he told the seminar. “If some of your businesses are concerned about the volatility of gas prices as well, to the extent that this is a public policy problem, then perhaps the government can do something, but these are two separate issues.”

He said that elected politicians and the government have to realise that no level of intervention will bring back the ‘good old days’ of cheap gas. “The opportunity cost of gas in the UK is now determined by a global market and there’s no level of intervention here that is going to change that, so the price level, which I believe is the subtext of all this discourse on gas supply security, is completely beyond governments’ reach.”

He added, “If the problem is that energy intensive industries are finding it hard to be competitive when they operate in this country, well, I understand the political problem but I don’t see how they can seriously address that. This country used to be a cheap gas island but there’s no way that’s going to come back, and in that respect government and everybody else will have to adapt.”

However, he ended on a more positive note, pointing out that the discoveries of shale gas in the UK could make a difference. “It is possible that the UK could be the first country to produce shale gas, but how much it will produce, nobody knows,” he said.

industry are simulation training and recruitment. “You need a kind of simulation training and I’ve read that in the UK one power utility has installed a kind of simulation training room so that they can simulate different actions in the grid, including interconnections to France, for example, to cope with communication issues and operational behaviours, in case of a significant event,” he said.

And on the issue of recruitment and training, Mr Bruch added: “When you look at the grid infrastructure that was mainly designed fifty years ago, most of the components are at the end of their lifespan. And so it can be difficult to find the right personnel and staff that are able to understand the techniques and cope with failures in this infrastructure.”

RISK TRANSFER SOLUTIONS

Mr Bruch then turned to the risk mitigation solutions available from the insurance industry. “Generally, when we are talking about power blackouts, property damage/business interruption for utilities is a common coverage in the market. There are some BI extensions around for specific failure of power supply and special coverages for electricity producers and distributors.”

He also pointed to parametric covers, where, for example, if you are operating a hydro-power plant and you have a weather parametric cover for that plant, then there is a payment where the weather conditions are so bad that the hydro power plant has to be stopped and cannot produce the expected output.

And he added that there are some special BI extensions in the market concerning data corruption, malfunction, operating errors, and hacker attacks.

But he also highlighted the fact that if no physical damage occurs at the location, or at the supplier, and you have contingent business interruption cover (CBI), then this loss is currently not covered. “That’s the reason why we have a new product within our company which especially deals with those non-damaged BI coverages like service interruptions and blackout power supplies.”

But, he explained, “We have to take into account that these new coverages are definitely an unknown territory for the insurance industry, and that means for us that we are doing a very customised risk assessment and offering a very customised product into the market.”

The key messages, he said, are that power blackouts are definitely on the rise and the worse-case blackout scenarios, like space weather events, or cyber terrorist attacks, could mean companies facing huge uninsured losses. “This has to be changed and therefore we are working on new products and new services,” said Mr Bruch. He concluded that the industry is working towards adequate risk transfer solutions, but at the same time there is a need to raise awareness of blackout risk and a need for organisations to strengthen their preparedness for blackout events.
CHAPTER FIVE — ENERGY SUPPLY AND POWER BLACKOUT

Energy Supply and Blackout Risk Q&A

QUESTION: What is the level of awareness of blackout risk?
MICHAEL BRUCH: Especially the industries, like the high level industries, telecommunication providers, or the finance industry, or data computing centres, I think they are really aware because they have to deal not only with those blackouts, but also with the frequency fluctuations, and so they are quite well prepared on this. But what I see is also that there is a gap between this awareness for the industrial customers and the activities of the governmental authorities. There was, for example, in Germany just some months ago, a so-called emergency letter from an aluminium industry company. They said they were already facing losses due to the fluctuation of the frequency, and they pointed out that they need more and more reliable power grids in the future.

QUESTION: So it is the hardware, the infrastructure itself that is a big problem? Is that a critical problem?
MICHAEL BRUCH: I think when we are talking about the power grid infrastructure in Europe, it is definitely the issue of the ageing infrastructure, but it is also the issue of coordination of those different companies. So what the countries have installed in the past was actually a lot of interconnections to facilitate electricity trading across the borders in Europe, but what they neglected was the hardware such as the grids and also the communication side—how do we connect those grids to each other?

QUESTION: And is the European Commission on top of this? Is it playing a role?
MICHAEL BRUCH: It is playing a role but my impression is that the interests of each individual country, and the state and quality of the infrastructure, is so different in each country that this is really difficult to coordinate.

QUESTION: Is this a business continuity and risk management question rather than an insurance question?
MICHAEL BRUCH: It’s both I would say. What we are seeing right now is that 25% of real economic losses are not connected to any physical damage. That means our customers are looking for new solutions, and that is the reason why we’re going to make new products available for those issues.

CHAPTER SIX — NEW TECHNOLOGY AND CYBER RISK

Keeping up with the cyber threat

If there was an award for the most terrifying presentation at the seminar, Paul Dwyer, Security GRC and Cyber Threat Advisor for The Cyber Threat Task Force, would head the list of nominees.

Mr Dwyer outlined the ever increasing array of cyber threats—from politically motivated ‘hactivism’ to government-sponsored cyber warfare; the network of organised and professional hackers trading data and expertise on an underground stock exchange; the difficulty in drafting legislation that can keep pace with the technology; and the problems these all cause for risk managers and insurance buyers.

Mr Dwyer began his presentation with one of the many grey areas in the whole cyber risk area—the terminology. “Cybercrime is essentially any crime that takes place using computers or the internet—everything from credit card fraud, to hacking to cyber warfare and terrorism. But there are a lot of grey areas between these different categories and this is where the difficulty arises in trying to insure against these different threats. You need to know if cyber warfare is covered under your insurance policy or is it considered an act of war? What defines an act of terrorism? Is an anonymous hacking group ‘real’ terrorism?”

In the US, Barack Obama has said that a cyber attack on certain aspects of the national critical infrastructure would be considered an act of war. And various countries are establishing cyber command units to defend against these sort of attacks, with some even going so far as to bring in conscription to create these units, said Mr Dwyer. “So you
Paul Dwyer used a fictional case study, dubbed ‘When Harry Met Sally’, to highlight both the ease with which cybercrimes can be perpetrated and the difficulty involved in bringing the criminals to justice. “I want to emphasise the amount of jurisdictions involved, how few people are involved, how much money is involved and how hard it would be to prosecute anyone involved,” said Dwyer.

Sally works in a data centre in Ireland. Harry lives in Germany. They meet on Facebook (which is based in America) and start a relationship that becomes increasingly close. Alas, Sally is an unwitting victim of a romance scam. “There are guys in Nigeria that fill warehouses with the files they keep on the different romances they are running. It’s incredibly well organised,” said Dwyer. “They have pictures of American Army officers and other false identities they use in their relationships as they gradually drain money from their carefully chosen victims.”

Sally and Harry fall in love online and eventually Harry gets round to asking Sally about the fact that she works in a data centre and has access to credit card payments. Sally says she would never give that information out. Harry says he just wants to be with her and they could use the money to finance a romantic liaison. Sally says she couldn’t help even if she wanted to. The systems are all locked down and there's data leakage prevention technology everywhere. Even if she had a spreadsheet full of credit card information, it would be traced. There is nothing she can do.

Well, there is, says Harry. He suggests going to a website called Rapidshare (based in Switzerland)—one of hundreds of websites that act as an online safe deposit box where users can create publicly accessible links for other users and have these links expire after a set time, leaving no trace, no trail and no log files. So Sally posts a link to a spreadsheet full of credit card information that will expire after an hour.

Meanwhile Harry contacts his friend in Russia who will sell the information for him for £20,000. The money arrives back with Harry and he then decides to send it to his money mule—often students with clean bank accounts who have been enticed to act as overseas money laundering agents for these cyber-criminals. Harry’s money mule is in the UK. He uses PayPal (based in Luxembourg) to send the money to Harry’s account in Thailand using Western Union.

Throughout the case, a number of legitimate companies based in different jurisdictions have been used making it difficult to pinpoint any illegal activity. Sally for her part may have contravened company policy but has not broken any Irish law unless she receives any money.

“It is another example of the law failing to keep up with technology,” says Dwyer. “And this is the difference between cyber threats and other threats. It’s not somebody breaking into a store. These attacks can be done from anywhere in the world and at any time of day. And there is no one criminal doing things on their own. They all work together, propagating ideas until they find a way into a company’s account and then trade that information on the ‘dark’ market.”

**THE UNDERGROUND ECONOMY FOR CYBERCRIME**

It has been estimated that cybercrime costs the UK around £27bn annually and it has surpassed drug trafficking as the number one crime, said Mr Dwyer. But perhaps more worrying than the size of the cybercrime industry is the level of organisation involved. “There is a complete underground economy for cybercrime with its own stock exchange where people buy and sell stolen information, computer viruses and their expertise. And like any stock exchange, the price goes up and down depending on supply and demand, the quality of the data, how many people have used it. These exchanges, such as the notorious DarkMarket founded by cybercrime broker Alberto Gonzalez, also have their own rules and procedures concerning the addition of new members and the verification of data or products offered for sale.

More recently though, said Mr Dwyer, cyber criminals are targeting the mass market. “You no longer have to be a computer expert to be able to engage in cybercrime. You can simply buy what’s known as crimeware—tools to commit computer crime. So whether you want to read your boss’s emails, whether you want to hack into a competitor and read their proposals or whatever it happens to be, a couple of hundred dollars will get you the tool set and you are unlikely to get caught.”

A further threat is the rising popularity of so-called ‘hactivism’—politically motivated cyber attacks led by high profile groups such as Anonymous and Lulzsec. The average

have land, sea, air and space and now cyber space as the fifth domain in national defence.”

And this can be related back to the business world because businesses can be seen as targets for cyber warfare, especially systematically important financial institutions or companies such as Google.

Terminology is also important for legislation as lawmakers struggle to keep up with the pace of technology. And given the global nature of cyber space, there is also the problem of jurisdiction, said Mr Dwyer.

“What is illegal in one country may not be illegal in another. The lack of a common playing field is a problem in bringing people before the courts or even proving something has actually happened.”

Despite the limitations of legislation, it should not be ignored, said Mr Dwyer. Firstly there are legal obligations that companies must live up to, and secondly it acts as a safeguard when dealing with counterparties to know that they too are complying with legislation. In Europe there is the European Convention on Cybercrime. “This is the closest thing there is to an international law on cybercrime,” said Mr Dwyer.

“A lot of countries including the UK and the US have signed up to it. Furthermore, it offers some common ground in terms of the definitions given to the crimes it relates to and it makes company directors responsible if they have not done everything possible to prevent their systems being used as a part of a cybercrime. And action has been taken. In 2010 three directors of Google Italy were convicted over a bullying video posted on their site.”
‘hactivist’ is a disaffected youth aged between 15 and 25 and their targets vary—from scientology to financial institutions to life sciences to anti-piracy groups—meaning that the risk to businesses can be hard to predict. “There is no real rhyme or reason to many of their targets,” said Mr Dwyer.

There is, however, a clearer intention behind the type of attacks that could be classified as cyber warfare—cyber attacks sponsored by national governments. Mr Dwyer highlighted the case of a computer worm virus called Stuxnet that was used to derail Iran’s nuclear programme in 2011 by disabling Siemens’ computer systems. The suggestion is that the Israeli and US defence forces were in some way involved. Aside from the worry of a World War III that begins in cyber space, the Stuxnet case also raises a new form of cyber liability for corporate risk managers that insurance may not be able to cover—the possibility of becoming collateral damage in international cyber warfare or terrorism, as in the case of Siemens and its corporate clients.

Evolving technology is not only helping to create more malicious tools, it is also creating new vulnerabilities for companies, said Mr Dwyer.

“Cloud computing and social media are two of the biggest catalysts that business people will experience in their lifetime. They are also the biggest cyber threats of 2012 so companies have to embrace this technology with a cyber strategy in mind. Cyber criminals are using social media to identify people within organisations to socially engineer information from people (see case study below: ‘When Harry Met Sally’).

The other cyber threat is the increasing number of people using their own devices at work and using instant messaging rather than the company email. That is a big challenge from an IT security and risk management perspective and that is the challenge. Companies should be able to get the return on investment from new technology like cloud computing but they have to deal with the risks at the same time.”

Ensuring information security

The term cybercrime is unhelpful in many ways, said Mark Fishleigh, Head of Insurance, BAE Systems Detica. “If you put the ‘cyber’ tag in front of anything, people often think that it no longer applies to them. Really what we are talking about is old fashioned information security—the information you have in your business and the best way to keep that information protected.”

Mark Fishleigh began by focusing on the vulnerabilities that exist in most companies. In many organisations there is an assumption that information security is predominantly an IT issue. The risk manager will periodically ask the head of IT about IT security and will be told that there are firewalls, patches and protection software in place. But this only deals with one part of the problem.

Aside from the fact hacking groups like Anonymous are regularly demonstrating the limitations of most technology defences, many information security breaches are not always a technical issue. “Sometimes it is a people issue, especially when people do not understand the value of the information that they hold.” This is of crucial importance when a company is outsourcing and their data is being handled by multiple third parties. “Not only do companies have to understand the value of that data but so do their suppliers and their suppliers’ suppliers. They also have to have control over their supply chain—to know where their data is and to ensure there are adequate controls in place.”

The importance of protecting customers’ personal data is well understood in the US where legislation makes it mandatory for companies to inform their customers in the event of an information breach. Consequently there have been several instances of customer notifications and this has helped companies to get a better understanding of the impact of an information security breach, said Mr Fishleigh. A relatively standard process for notifying customers has developed and this has made it possible to make more reasonable estimates of the average cost of a security breach, as seen in the annual study released by the US-based Ponemon Institute.

Such research, however, is limited to the direct costs
resulting from a security breach (such as the cost of contacting customers) and can do little to quantify the indirect impacts, such as reputational damage and long-term loss of business. This is best demonstrated by the recent case involving Sony when a security breach compromised the personal data of more than one million customers. “Hundreds of millions of dollars have been spent on clearing up the mess but no one has attempted to quantify the indirect costs that could result,” said Mr Fishleigh.

Rather than extrapolating from the figures contained in industry surveys, companies would be better served by conducting an impact assessment of the various potential threats that exist. “It should be scenario-based and made relevant to the business. The costs can vary according to the type of attack that has taken place so the assessment should look at the type of attack, the scale of the damage, the best response and the potential liability facing the company.”

In order to build an accurate risk profile, companies need to bring the views of IT and the business together,” said Mr Fishleigh. “This way you can accurately assess what information you have, the value of it and the relative vulnerability. Then you can work out what best to do with it—whether to ignore the risk, mitigate the risk or indemnify it.”

**MANAGING THE RISKS**

There are, of course, some risks that are unavoidable and cannot be transferred to third parties, in which case Mr Fishleigh laid out five practical steps to help manage such risks. The first of these relates to the business case and how much a company is willing to invest in protecting against certain risks. Secondly, organisations should classify their information according to its value. “This is something that government is usually very good at in that different documents are granted different confidentiality levels according to their importance but very few commercial organisations do this.”

Thirdly organisations should look at who is responsible for IT security, where they sit in the organisation (if it is in IT then perhaps they should think again) and how much influence they have. The fourth step is IT security. “IT is not secure. It just isn’t. But there are some tools and techniques that you can employ to build a secure IT infrastructure for your most valuable data. If you segregate the more valuable data from the sources of threat then you make it much harder for individuals to get to that information.”

Lastly, organisations must maintain constant monitoring and develop relevant responses. “With the best will in the world you’re never going to make yourself entirely secure. So, it’s important to monitor the activity on your network and to respond at the first sign of a threat.”

The insurance market is still evolving when it comes to cyber risk and Detica is working with a number of insurers to help them deal with the challenges of limited loss data and rapidly developing exposures. But, said Mr Fishleigh, there are some positive developments that could help create a better insurance market for cyber risk. Step number one is a greater understanding at board level. “If the insured knows what information it wants to insure, it can get the right policy.” This will in turn create a greater demand and a better supply for cyber insurance. “If you’re asking for the right policy and you know how much you’re prepared to pay for it a market will fall around that.”

Step two is the creation of effective standards. ISO 27001 already exists for certain means of cyber defence but a similar effort should be put into looking at cyber attacks and how best to define them. Greater information sharing would also help. There are various government-sponsored initiatives that exist, such as the UK’s hub and node project announced in late 2011, however there still needs to be more work done in terms of creating incentives for firms to take part.

The final step is regulation. Governments are clearly taking cyber risk seriously, said Mr Fishleigh. The UK has made it a tier one risk, the US has made similar commitments and EU data protection legislation should help to drive change in continental Europe. We may even see more exotic proposals in the future such as the establishment of a Cyber Re fund similar to the Pool Re fund that was established for addressing massive systemic risks.

Cyber risk Q&A

**QUESTION:** Because some of these events happen out of the public view and are effectively covered up, this can create a false belief that these things aren’t going to happen to me, they’re going to happen to somebody else. Do you have any particular strategy you think would be effective in changing that situation?

**MIKE FISHEIGH:** We use scenarios—humanised descriptions of things that could happen to your business and individuals’ roles within that business when the threat happens. The scenarios are supported by the work we’ve done around the specific vulnerabilities of the company and by examples of other organisations where this has happened. So that’s the most effective technique that we have used with boards that haven’t had an incident. I could also talk to you about the example of an organisation that I went in to see last year. “This is all very interesting,” they said “But no one is going to be interested in us are they?” And all I can say is we are now midway through the response to a major incident at that company. So it does happen.

**PAUL DWYER:** Education is the key. The problem we see a lot of the time is that when there is a high profile incident in the media, a board member will phone the IT director and will hear what they want to hear—we have firewalls, it couldn’t happen to us’. But it’s not just an IT issue. It’s about processes and it’s about people before it’s about technology. Board members have to ask more intelligent and pertinent questions so they can see through the standard answers. For example, if they ask their ISP whether they have mitigation...
tools against DDOS attacks, the answer will be ‘yes’. But then they need to ask what type of mitigation tools they have. Without getting into a technical argument about it, board members need to understand the true level of mitigation and cover they’re getting in relation to each aspect. It is a combination of getting the board level to understand the complexities of these issues and then aligning IT strategy with business objectives and dealing with all of that in a risk environment so that they can take the pertinent course of action when an event happens.

MIKE FISHLEIGH: There is clearly a perception gap. Governments around the world are spending a lot of time looking at these issues. In a time of general austerity, the UK government has chosen to invest slightly over half a billion pounds in cyber security. Now they wouldn’t be doing that unless there was a reason. There is a lot of fear and uncertainty around cyber risk but I think there is one very small change that’s happened in the US recently which is going to be extremely helpful and a similar change in the UK or a similar change of attitude in the UK would help. In October last year the Securities and Exchanges Commission (SEC) released guidance for all listed US companies stating that cyber risk should be considered when completing the risk section on your form 10K. If all that does is make the CRO question the extent of the company’s exposure to cyber risk, that’s a very good start.

QUESTION: We are advising companies that might be perceived to be at a high risk of some sort of attack. Do you have personal experience of, or any thoughts on, the extent to which advisors, like accountancy firms or law firms, have been targeted in order to get to their clients’ data?

PAUL DWYER: Yes there are lots of cases. When we talk about the ‘stocks’ that are sold on this underground stock exchange it is generally what’s known as Personally Identifiable Information. As with any other stock exchange, there are different categories of PII that determine its value. Industrial related or commercial sensitive information is extremely valuable. I was recently working with a large law firm in London. The staff were very proud of their network security and telling me that their firewalls had a top rating but using some quite mundane methods I was able to show how someone could breach this security.

There are lots of cases especially in relation to merger deals, everything from sweeping rooms for bugs right through to who’s hacking into who, who’s following who. There was a very high profile case involving a billionaire in Ireland who was being followed by private detectives and the solicitors and the accountants. Everything was being monitored to try and get as much information as they could.

One of the techniques we use when we’re auditing an organisation, and there is a legal aspect involved, is to go and hang out in the coffee shops near the courts. The solicitors will often meet in there and you will hear them talking about cases and leaking information. It’s that human element. People will talk. So whether they target the physical network or the organisation itself, it is that human element that is the ultimate vulnerability.

MIKE FISHLEIGH: It’s true that the people who are after this information are very ingenious and very motivated and when they are after the information, they will find the weakest link in the chain to get it, so there’s one particular client we work with where we saw an organisation was trying to attack them to get certain information out of that organisation and failed because it was protected well within their organisation. However the attackers went down the road to their insurer. As far as their insurer was concerned, this was just more policy information, we just store it the same way as everything else and it walked out of the door. So yes this does happen.

THE CYBER INSURANCE MARKET

The challenge in developing insurance products for any emerging risk is that there is so much unknown territory. As Mr Dwyer said: “When clients ask me about cyber insurance policies, it is the one cyber question I cannot answer.” Cyber risk is itself such a broad area that any insurance policy has to be based on the specific risks facing each organisation. Consequently the few insurance products first to market have tended to be heavily customised.

The insurance market is evolving, said Mr Fishleigh. “It is a fragmented market, there’s not much clarity on coverage, some of the bigger risks aren’t touched at all and there’s a lack of risk data to support that underwriting process both in terms of the likelihood and in terms of the impact of events.”

And, the evolution is coming from two different directions. On one side are liability underwriters looking to extend their technology liability to cover emerging cyber risks. On the other side are the property insurers that have finally realised that losses can occur without there being any physical damage.

The loss of customer data is the most obvious example of insurable cyber risk and the US market for such policies is the most mature thanks mainly to legislation that makes it mandatory for corporates to notify their customers in the case of a data breach. There are roughly 30 insurers in the US market offering policies designed to cover the cost of customer notification and any related liabilities—both first party (loss of business) and third party (legal cases). There is less of a market in the UK, where the number of insurers is around 10, and even fewer in continental Europe. However, with EU data protection legislation likely to make customer notification mandatory at some point, this market can be expected to mature.

There are, however, big gaps in coverage around new and exotic areas such as cyber terrorism and cyber warfare and this may be the case for some time, said Mr Fishleigh, not least because no one is quite sure what constitutes an act of cyber terrorism or cyber warfare. There are also large differences between policies because there are no standard wordings.

The biggest challenge for risk managers though, said Mr Fishleigh, is the fact that what cyber-related insurance products are out there have evolved from the supply side. “Insurers like cyber risk. It is a new area with potential for price improvement but the demand is not at the same level.”

One reason for the imbalance between supply and demand is that many corporates have not properly assessed and quantified their information security risk, said Fishleigh. “This makes it very hard to work out how much you are prepared to insure it for. How can you tell if an insurance policy is good value for money if you cannot quantify your exposures? I am often asked if cyber insurance is too expensive and when premiums might come down to a more reasonable level. I genuinely don’t know because I don’t think the risks are well enough understood yet.”

23
Know more. Achieve more.

Creating the world’s largest cruise ship requires a trusted partner. That’s why Royal Caribbean International® trusts in the expertise of Allianz Global Corporate & Specialty – covering the most complex business risks worldwide.

www.agcs.allianz.com

Jason Liberty, Vice President
Royal Caribbean International®
Corporate and Revenue Planning & Insurance