StrategicRISK

FUTURE OF RISK AND INSURANCE

SEPTEMBER 2015

IN ASSOCIATION WITH

ZURICH®

INTRODUCTION

A brief guide to the future of risk

This report highlights the nature of the change confronting the risk and insurance sector. Read on to find out more about the key points and trends outlined below

In these days of unpredictable, technology-driven transformation, the risk and insurance community is required to make fundamental changes to how it operates. In every role within the insurance value chain, fresh skills and a new intellectual dexterity are called for. Here is a quick guide to the top 10 insights and trends for the industry that emerge from this report.

1 Disrupt and innovate. Technology developers in San Francisco, London's Silicone Roundabout, and any number of teenagers' garages and basements around the globe, have their sights trained on the amply proportioned insurance industry, and on many other business sectors besides. Insurers, risk advisers and enterprise risk managers should look to expose the inefficiencies in their own processes and to find innovative solutions – before somebody does it for them (pages 4-6).

2 Embrace change. The velocity of technological transformation is increasing, ushering in new and unexpected risks and opportunities. For those with a head for speed, going with it could be an exhilarating and rewarding ride.

3 Get certified. Risk managers are being called upon to fulfil a new operational risk leader role that has influence over company strategy. It's a big change for some, requiring communication with senior executives at board level. Two new certification schemes provide a potential badge of honour for risk managers, giving them the rigorous professional credentials – and the confidence-booster – they need to take their role up to the next level (pages 12-13 and pages 14-15).

4 Love mobile. A world explosion of mobile device ownership is poised to happen in the next five years. Those who embrace and immerse themselves in the potential of mobile technology will have a big head start when it comes to understanding connectivity risks (pages 4-6).

5 Mentor and promote. Taking steps to develop a new generation of digital native risk professionals is the key to building a sustainable future for the risk and insurance industry. Particularly in the case of technology-driven operational risk, digital literacy and a fresh eye on risk will help to unlock the opportunities, and to anticipate the pitfalls, ahead (pages 14-15).

6 Question class underwriting. There's a new generation of data-savvy commercial insurance buyers who are asking pertinent questions about exactly how their risk is priced. Players on all sides need to be ready to be transparent and get granular with the facts (page 4-6).

7 Say farewell to renewals. The days of the annual renewal may be numbered. This will be a tough nut to crack as so much of the insurance industry's process is built around renewals. But those who move early to sweep away this vintage practice could reap the biggest benefits (page 4-6).

8 Share ideas. With unprecedented amounts of change ahead, now is the time to talk to risk advisers, insurance providers, senior managers and colleagues young and old, to make connections that enable a richer understanding of the new risk landscape. Working in silos is not an option any more.

9 Think global. A word that cropped up over and over again in the making of this report is 'globalisation'. While it may have been a trend in business for many years, the connectivity ushered in by mobile technology is making global business happen more directly and much faster than ever before. Those who think globally about risk will better understand, and protect against, potential loss.

10 To embed or not embed? The debate is raging over whether or not technology security risks are better covered by standalone insurances or by new wording within traditional property casualty and liability policies. There are good arguments both ways and risk professionals should be looking at all the options. SR

CONTENTS

BIBLIOGRAPHY

2015 Global Cyber Impact Report
Aon, Ponemon Institute,
April 2015
www.aon.com

Guide to Corporate Governance Practices of the European Union
ECODA, 2015
www.ecoda.org

Compensation and Market Trends in Risk Management Interim Report 2015,
Barclay Simpson
www.barclaysimpson.com

The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed
World Economic Forum, June 2015
www.weforum.org

UK 2015 Cyber Risk Survey Report
Marsh, June 2015
www.uk.marsh.com

UK Cyber Security: The Role of Insurance In Managing and Mitigating the Risk
Cabinet Office and Marsh, March 2015
www.gov.uk

EMERGING RISK
DISRUPTIVE INNOVATORS

The power of the disruptive innovator

Uber, WhatsApp and 3D printing are just three emerging technologies that ring alarm bells for long established sectors such as insurance. But they only point to one thing: change or be changed

Over the course of the next five years, the number of connected devices globally will rise to 50 billion – up from 12 billion today. In addition, the number of people with internet connections worldwide will grow to 5 billion, up from 1.8 billion, in a world population of 7 billion. This explosion of interconnectedness suggests the current rapid pace of change is already speeding up.

Emerging technologies such as 3D printing, artificial intelligence, digital currencies, the Internet of Everything, robotics, and sensors will disrupt traditional business models – and even economies.

"People need to think seriously about interconnectivity. Every risk is now a global risk," says Aon chief innovation officer Stephen Cross. "Say I have a small manufacturing site in Nottingham; I have a website; my people use iPhones. Now I'm globally exposed to some guy in a basement in Russia hacking into my system, into my clients' data, and closing me down. Digital wildfire is out there, and we need to be cognisant of what can happen."

Cross adds, however: "I disagree with the word disruptive, because it suggests that the disrupter is the bad guy." Instead, risk and insurance professionals should be cultivating their own disruptive thinking, he says.

"Disruptive innovators, as I call them, address inefficiencies in the existing process. Taxi cabs have existed forever, but Uber has put the business on a highly efficient model," he says. "When you get in, the driver presses start on his or her app – that's when the commercial driver insurance starts. When he or she presses stop, it produces a receipt and it stops the insurance. That's usage-based insurance taken to the ultimate."

Tackling inefficiencies

Innovative technologies that tackle inefficiencies are popping up everywhere. Take 3D printers, which are revolutionising product design and distribution.

"Sales of 3D printers are rocketing. They're a very important part of our product range," says Alex Butt, global head of risk for UK-based distributor Electrocomponents.

The company has a product catalogue comprising half a million lines, from electro-components to test and measurement equipment to engineering tools and consumables. It sells mid-range 3D printers for about £400 (€564) each, generating annual revenues from this product of €1.4m – a figure set to rise to €7m in two years.

Alongside the printers, Electrocomponents offers Design Spark Mechanical, a free-to-download 3D design software package. The software and printer combination is used by engineers and enthusiasts for efficient product prototyping that promises to save them more time and money than with traditional methods. "There is a risk of counterfeiting," explains Butt. "We try to educate customers about what they can and cannot do with 3D printers.

"And there is a risk around customer expectation of the product."

Such risks emerge hand-in-glove with the opportunities afforded by the new technology. A further risk is that digital product designs for 3D printers can be used to circumvent export laws that ban the sale of certain products to countries such as North Korea.

Butt emphasises that 3D printers are particularly ill-suited to manufacturing weaponry, however, because they use plastic and not metal, although he says they can be used for prototyping.

Telecoms challenges

Businesses of all types are feeling the effects of disruptive technology. In the Netherlands, Bert Schijf, director, risk and reporting, at telecoms provider KPN, says: "One of the main risks for KPN is disruptive technology. When WhatsApp came along, it made our revenue shrink dramatically.

"A lot of those app-based technologies are still heading towards us. It's one of the things we have on our radar."

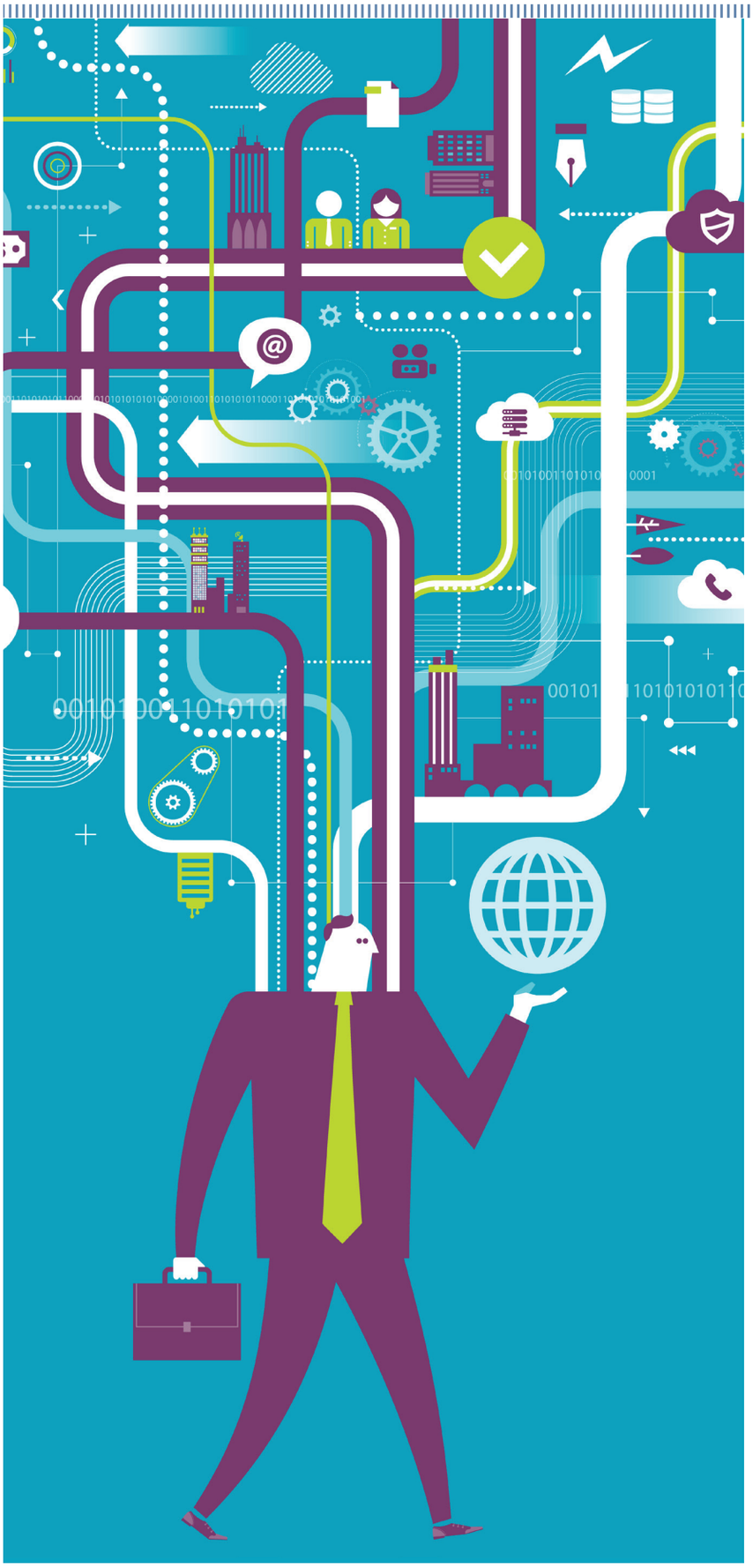
KPN pays for frequencies so that it can deliver a telecoms network to customers, but when developers create new services delivered over the internet to customers' handsets – particularly messaging services such as WhatsApp, Facebook Messenger and Viber, which enables free internet-based calls – the network provider sells less data for texting and calling.

"There's not much you can do about it," says Schijf. "Telecoms companies have to adapt to the new realities.

"A few years ago, most telcos were fighting these developments, but increasingly you see sales of data bundles facilitating use of new apps, and that locks in customers for the future. We're not fighting, but joining."

KPN has taken some significant steps towards this. It has set up a 'new innovation' department, which is responsible for disrupting the company from within.

Each new idea is put in front of the Big Data and reputation board, which decides whether



THOUGHT LEADERSHIP

JÉRÔME GOSSÉ
Head of security
and privacy EMEA,
Zurich Global Corporate

A COLLABORATIVE APPROACH TO MANAGING THE INTERNET OF THINGS

Advancement in technology is exacerbating cyber risks for companies globally. A key trend is the emergence of the Internet of Things (IoT).

The business opportunities of IoT are plentiful and appeal to a new tech-savvy generation. Individuals are willing to control everyday items remotely, and companies are responding to this. It is possible to manage house alarm systems, watches, drones or even cookie jars from a smartphone or tablet device. We are living in a hyper-connected world, and this is possible with the development of new technologies.

These technologies create new opportunities, but bring new risks for individuals and companies. Think about connected vehicles: a failure in the navigation device controlling the automobile could result in a life-threatening accident. The question then becomes: who is liable for the accident – the company that developed the IoT software, the car manufacturer or the driver?

Cyber risks now have an impact on real life. Other exposures such as property damage are also likely. Take the utility industry as another example. If IoT is adopted to provide greater efficiency between an electricity provider and the provider of the provider (the third-party company that manufactures the electricity, for example) a new entry point for a cyber attack has been created. A criminal could penetrate the system and, intentionally or not, cause an explosion.

In this scenario, the losses may not only be financial but could arise from bodily injury and property damage. However, at the moment, most cyber policies only cover financial loss.

The challenge for insurers is developing the right cover. With emerging risks such as IoT, insurers cannot work in silos to create policies.

At Zurich, we created standalone business security privacy and cyber liability insurance solutions. Our objective is to work with all lines of business – engineering, property, casualty and financial lines – to form a product that responds to our client's needs.

Aside from risk transfer, we provide a global incident response service to our insureds. Following a security incident or a data breach, Zurich clients can have access to an incident management team, with 24/7 availability to manage the resources needed to recover from a damaging cyber event.

EMERGING RISK
DISRUPTIVE INNOVATORS

or not the new initiative complies with strict company rules on data privacy (see box).

Among the innovations on KPN's risk radar, the Internet of Everything in particular is seen from a business interruption point of view.

"We're looking at smart solutions, connected services. We could provide connectivity services or platform solutions, but if so, we have to be very clear in the terms and conditions about what we are and are not responsible for," says Schijf. "If not, and the service fails, we could be held liable."

Financial services targets

Disruptive innovators have the profitable, but often inefficient, financial services sector in their sights. Insurance, particularly, is ripe for disruption – time is running out for insurers to investigate their inefficiencies and disrupt their own businesses before it is done to them. "Efficiency is an incredibly good thing for our buying customers, so it should be good for risk advisers and for insurers as well," says Cross.

"Anything that improves risk control or enhances the risk profile should be embraced. It leads to improvement, to social good. Anything that can prevent or improve loss is interesting," says Cross.

With driverless cars, which are emerging as safer than traditional vehicles, the risk shifts from the driver to the product. The cars have a black box, like aircrafts do, and if something goes wrong it will be treated as product failure.

"When you look at the insurance industry, and the risk industry, you've got to look at the process or the product and ask: 'What is not efficient to the customer?', and 'Who is going to change this?'," says Cross. "The biggest friend of the insurance industry right now is regulation. The stricter capital environment is probably keeping out some of the companies that track massive amounts of data, like Google or Facebook. It keeps them at bay for now. Insurance is a high-value target to disruptive innovators. Insurance is up there as one of the industries that will be disrupted."

The huge success of price comparison sites is proof that innovations that target inefficiencies from an insurance buyer's perspective can thoroughly disrupt insurance business models. Peer-to-peer insurance is another emerging example, as is real-time insurance, which could sweep away year-long contract-based deals. Arguably, it is long overdue.

Cross says many questions must be tackled. "'Whoever decided that there will be an annual renewal date?' and 'Why can't I purchase insurance until the day I want to cancel it?' . . . You can price and model changes to it, like a variable mortgage. 'Why is insurance so far behind on something that's a dynamic marketplace?', 'How did my risk profile change a minute before renewal date at midnight to a minute after and you come up with a completely different price?'. The reality is that the price of my risk, and the price of the marketplace, adjusted many times over the period of the contract."

Innovators looking to disrupt financial services are targeting the banks as well. Peer-to-peer money platforms are enabling customers to avoid hefty bank charges on overseas transfers and currency exchanges. New digital currencies such as Bitcoin are an attractive option for people in places where the local currency is weak, such as Argentina, where it's used by traders.

In Greece, which endured a week-long bank shutdown during the recent bailout talks, people will inevitably turn to alternative systems, despite the potential risks around their lack of regulation.

When it comes to exploiting some of the undoubted inefficiencies in insurance, risk managers are leading the way by questioning how things are done. "The next generation of risk managers, the buyers of commercial insurance, are very data-savvy, very technology-savvy. They are looking for different types of information, and different types of solution," says Cross.

"The profile of the buyer of today is not the same as the profile of the buyer of tomorrow. A question we get all the time is: 'How do you pick the markets that best suit my specific risk? I'm different; I don't want to be class underwritten. Tell me how best to align my risks'. We are working towards trying to show customers how we pick markets. And it's not anecdote, which is the broking of the past, it is fact-based and provable, coupled with the sentiment of how people see things. That's where we are going." **SR**

Insurance, particularly, is ripe for disruption – time is running out for insurers to investigate their inefficiencies and disrupt their own businesses before it is done to them

KPN'S GOLDEN RULES FOR PROCESSING CUSTOMER DATA

1. Everything you do with customer data could affect customer privacy
2. Anonymised data is not personal data and can be freely used
3. Do not collect more data or store data longer than needed
4. Use traffic data for marketing or analytics only with the explicit approval of customer
5. Customer approval must be based on detailed information, given explicitly, in advance

EMERGING RISK
CYBER CHALLENGES

Search for the key to cyber cover continues

With the enormity of the risk still holding back insurers and a lack of clarity among buyers, debate is still raging about how to handle cyber risk

In July, a Jeep Cherokee was hacked by cyber experts as part of a stunt set up with *Wired* magazine. They took remote control of its radio, air conditioning, windshield and transmission system through the vehicle's internet-enabled entertainment system. The incident led Fiat Chrysler to recall 1.4 million Jeeps.

Could damage to the Jeep Cherokee or Fiat Chrysler brands have been covered by a cyber policy for this security breach? Or perhaps a product liability policy would have covered the cost of the recall? These are typical of the questions vexing risk managers and insurers on how to handle emerging technology risks, including data security and reputation risks.

"The whole issue of cyber risk, the technology- and digital-driven transformation of every part of the economy, means that you cannot separate cyber [risk as a standalone threat]" says Sarah Stephens, JLT Speciality's head of cyber, technology, and media errors and omissions. "There are so many loss scenarios that could be triggered by a technology failure, a security failure, a cyber or quasi-cyber incident, that could be, or should be, covered in a property or casualty policy. That is a massive challenge for insurers and for the industry right now."

In some cases, organisations are taking matters into their own hands and finding their own ways to mitigate cyber exposures. In response to risks around its customer data,

EMERGING RISK CYBER CHALLENGES

KPN, the largest mobile, text, and TV subscriptions provider in the Netherlands, set up a new data security department and embedded a strong ethos on customer privacy and business continuity throughout its operations.

KPN privacy officer Rence Damming highlights the discoveries it made by researching its customers. "It matters what kind of company you are. Google processes a lot of data, and users expect that – they give away their location information in return for a service. But they don't expect it from a telecoms operator or an energy provider. Expectations differ. Customers want to trust their telecoms operator, because we deliver all their communications from A to B. We build trust by telling customers what we do and don't do with their data."

Notification of breaches

KPN's stance on data security and business continuity reflects the substance of a new law passed by the Dutch parliament in May. This will require organisations to notify the authorities about data breaches or face fines of up to €810,000 or 10% of annual turnover. The rules anticipate the European General Data Protection Regulation (GDPR), due in 2015 or early 2016, which will include security breach notification obligations from 2017 or 2018.

Bert Schijf, KPN director risk and reporting, says that while he is interested in cyber insurances, he believes that notification requirements could introduce a degree of caginess into conversations with insurers.

"It could be hundreds of thousands of people who are affected by a data breach. Is this something insurers are willing to provide policies on? On the other hand, maybe organisations will not want to notify the authorities if they think that the insurer won't pay out," explains Schijf.

"It could make the conversation difficult, like trying to purchase medical insurance if you have been unwell in the past."

Cyber brokers emphasise that insurers are very willing to do deals on data breach risks. "It's a competitive, hungry market, with new entrants coming in every quarter. It's a market very willing to take on IT and security-based exposure, and to adapt to clients' requirements," says Stephen Wares, Marsh cyber risk practice EMEA leader. "If we can define the triggering event, and closely define the loss, there's no reason why we can't pitch that into the market and find a solution. The insurance markets are doing a good job at addressing cyber exposures."

Marsh is "pumping out proposals" for consulting services to organisations that want to understand their cyber risk profile.

"They need to start thinking 'What if it happens?', 'Who is responsible for defining that risk profile?', and 'What does that project look like?'," says Wares. "Some clients want a professional consultant, whereas others may have the skills and resources internally to do this for themselves."

JLT's Stephens agrees that data breach and business interruption liabilities can be quantified and underwritten as a standalone risk, and thinks this could develop as a specialist policy, similar to kidnap and ransom, where the service element is a big part of the reason to purchase.

"Many insurers have put together panels to help organisations respond to cyber incidents," says Stephens. "The real questions are whether property damage or bodily injury or non-damage business interruption, triggered by a cyber attack, are covered by property casualty policies, by a cyber policy or even some new specialist insurance."

Communication gap

Meanwhile, on the buyer side, a gap in communication between risk managers and their board directors is continuing to hold organisations back. This is resulting in senior management often being unaware as to which of their cyber risks are covered by insurance and which are not.

"It was a big surprise to us that board-level ownership of cyber risk did not change much year-on-year," says Wares. He is referring to Marsh's Cyber Risk Survey of clients, released in June, which shows that board directors are responsible for cyber risk in 19.4% of companies, compared with 55% where it's owned by the IT department.

"Most cyber risk management is done by the IT team," he says, "and IT is driving the conversation. We need to emphasise that this is a risk conversation, not a technical one."

'Maybe organisations will not want to notify the authorities if they think that the insurer won't pay out. The GDPR could make the conversation difficult'

Bert Schijf, KPN

An analysis by Marsh of premium flow into the market suggests that cyber insurance penetration is 2%. This compares with UK government figures showing that 52% of board directors think that they have cyber cover.

"We asked insurance buyers if they had bought cover, whereas the government asked senior executives. We think our figures are likely to be nearer the truth, so there is a big communication gap between the insurance buyer and the board about what is insured and what is not," Wares explains.

This lack of clarity about coverage on the buyer side is mirrored by a degree of uncertainty in insurance markets about how best to underwrite these emerging risks.

"It is happening in property, professional liability and product liability, where there is no cyber exclusion but there is no cyber underwriting happening either," says Stephens. "In a market cycle that is relatively competitive, it is tough to be the insurer who puts the exclusion on, because they lose that deal. So a lot of insurers are struggling."

A property policy for an industrial site, for example, if it has no exclusion, presumably covers damage triggered by hackers breaching the site's control systems, as it would cover damage caused by a fire, or windstorm.

Property underwriters using metrics such as historic weather risks, location, construction materials and whether the building has sprinklers do not traditionally underwrite these new cyber risks. Now that internet-connected controls and remote monitoring systems are becoming commonplace, insurers will begin looking at internet security systems, whether default passwords have been changed and if back doors installed by equipment suppliers are properly disabled.

"They should ask 'What did you do in terms of managing all that connected cyber risk in your control system, which now has remote monitoring, and all sorts of capabilities it didn't used to have?'," says Stephens.

"That's a risk that could trigger a property loss, but insurers aren't asking the right questions, either because they don't know which questions to ask or because it's not on their radar that it could trigger that policy."

Dedicated teams

Inside insurance companies, underwriters who have cyber expertise are often part of a professional liability or cyber team, where their knowledge is kept separate from the wider property casualty business.

"Some insurers are starting to deploy cyber and technology underwriters across different lines, so that they can transfer expertise, but generally there is a knowledge gap and a training gap," says Stephens.

The rise in cyber-related risks will change the underwriting experience for risk managers as well, adds Stephens.

"In addition to providing building engineering information for a property policy, buyers will be asked about system firewalls, original equipment manufacturers and what data they put in the cloud," she says.

"They have to start providing a different level of detail. In some cases, that will mean talking to people internally who they've never met before, and compiling information they may feel uncomfortable with, including lots of technical jargon."

While the debate continues about the extent to which emerging cyber risks should be embedded into traditional insurance lines or covered by standalone policies, the clinching factor is likely to be a big loss.

"We are at a crossroads and definitely don't have a consensus," says Stephens. "There's this thing called cyber and it has grown and changed a lot over the past decade. We know of examples of cyber attacks on oil pipelines and energy generation plants, but no big losses. If we have a big loss, then that changes behaviour pretty quickly." **SR**

RISK MANAGERS' VIEW

Shift in emphasis

The role of today's risk manager is very different to that of a decade ago. Four leading risk managers give their views on how the role has evolved over the past 10 years and how it is set to change

Patrick Smith, chief risk officer at The Warranty Group and chairman at UK risk management association Airmic

Four main trends have changed the risk manager's role:
1. Globalisation The world is rapidly changing, with shifts in economic power and stability. There is also an increasing ability among businesses to harness worldwide capabilities to deliver services, manufacturing or securing natural resources. This creates complex supply chain dependencies and highlights the conflicts between differing regulatory requirements, cultures and business ethics.
2. Regulation Highlighted by the economic changes over the past five to 10 years, regulation across most industries has developed in focus and willingness to act. This places risk management processes at the heart of effective corporate governance and compliance systems, both in terms of monitoring current and emerging risk profiles but also in mitigating the impact of breaches, which can be increasingly damaging.
3. Reputation Heightened by the impact of social media and the attitudes of the younger generations, corporate reputations can be enhanced or diminished rapidly. The risk around conduct and ethics are increasingly relevant to corporate reputation and I only see this increasing in significance.
4. Accountability Following a number of corporate failures and events, it is evident that the effective management of risk is a board responsibility. Corporate negligence is increasingly penalised and personal accountability is reinforced by increasing powers to penalise directors and senior management. Thus, creating risk maturity and enterprise-wide understanding of the strength of an effective risk management framework is increasingly important.

The risk and insurance industry can do several things to help risk managers prepare for a more complex risk environment. It can assist risk managers in thinking beyond insurance and support risk mitigation efforts, knowledge and techniques. Insurers can position solutions in the context of overall risk exposure, risk managers can take an entrepreneurial approach to assessment. Additionally, certainty and clarity in terms of wordings, claims outcomes, process and delivery is vital and can help the industry adopt a 'no surprises' ethos that encourages partnership between risk manager (and advisers), broker and insurer.

Sabrina Hartusch, global head of insurance at lingerie manufacturer Triumph and president of Swiss association SIRM

Our role was always complex and needed a fair amount of thought. What has further complicated the risk manager's role is the speed at which the new business world moves, globalisation, advancement in technology, the lack of boundaries and certainty in many fields. These factors can make risk managers feel insecure and drowned in 'risks'.

I see this in my daily role, as well as when I speak and interact with fellow risk managers. I see this also within the company I work for, both from what stakeholders speak to me about and from the topics they have on their agenda. The key here is to stay focused and to identify what is relevant for the company and filter out what isn't, then bring this up to top management.

The insurance industry can help risk managers better prepare for a more complex environment. The sector is rich in data, information, research, papers, studies, and so on. Day to day, this may go unseen. There needs to be more focus on tomorrow's risks but the insurance industry has to work more closely with its clients to achieve this. It should be the industry's primary focus, so that it stays relevant.

Attracting new and fresh talent is also key in tackling tomorrow's risks. We have to make clear that risk management is a profession, just like medicine is a profession. This will help people to understand what risk managers do and what risk management is about. The role is not yet understood widely. Once international recognition is achieved, risk management will have a true identity. This will help attract new risk managers to the profession who choose risk management as a career.

The industry then needs to develop a professional framework, which risk managers can follow to fulfil their role. Naturally the role will be one that from the outset requires common sense, open-mindedness and great judgement capabilities – character traits a risk manager should bring with them. In a complex risk landscape, these traits and continuous self-development will help.

Carl Leeman, chief risk officer at Luxembourg-based international logistics and transportation firm Katoen Natie

Three important elements help explain how and why the risk manager's role has changed over time: speed, complexity, and a more risk averse society. Everything – from business operations to new technology – works and operates faster than ever before. Additionally, societal demands are more complex.

As such, there are a lot more unknowns today than in the business world of the past. But businesses do not want to take risks and are afraid of the unknown. So helping companies cope with the unknown is a great role for the risk manager of tomorrow.

Risk managers of tomorrow must be lean and able to react/adapt to new situations. As the saying goes, 'it is not the big that eats the small but the fast that eats the slow' – and big means often (very) slow.

Additionally, it is important that the industry attracts new blood to risk management. This has been a challenge. Indeed, very few talented young people step into our industry.

Risk and insurance is still perceived as dull and old-fashioned. The image of a successful stock trader making big money, as seen in the movies, is much more attractive to young people. The fact that the risk manager's role is carried out differently from one organisation to another, or one country or other, doesn't help in giving a clear and defined image or standard description of what a risk manager does, which is part of the 'image' problem.

A more structured and uniform risk management education and also certification will certainly be part of the solution.

'Today's risk manager also has to think about wider implications, such as social media and reputation, crisis management, business continuity and alternative ways of working'

Colin Barker, Bayer

Colin Barker, group risk manager at chemical and pharmaceuticals company Bayer

Historically, the risk manager would concentrate his/her efforts on current operational risks – the known risks – creating risk registers and the like, then look for risk avoidance, mitigation or transfer strategies to address those risks. Today, the risk manager still has those responsibilities but is a lot more proactive and creative – 'what if?' is considered, along with 'what might that lead to?'. Today's risk manager also has to think about wider implications, such as social media and reputation, crisis management, business continuity and alternative ways of working.

Combined with raising awareness, so that everyone in the enterprise becomes a true risk manager in their own right, the emphasis is more on resilience – 'if anything happens, could we cope and, if not, how do we change things so we can cope with any risk thrown at us, no matter how unexpected?'. Good risk managers will stress test this using scenario-playing exercises and unannounced simulation exercises.

Many risk managers have greater involvement in incident management, crisis response and business continuity (I oversee incident response and crisis management until the crisis team can take over). More and more risk managers are also working alongside developers prior to product and marketing launches or as part of the strategic management of the organisation in developing low-risk/acceptable-risk commercial initiatives. Previously, they would have been left out of this and only involved post-implementation in minimising the resultant risks. Risk managers are now, more often than not, part of the business team and less of a restrictor of business activity.

Things have also changed in the split of responsibilities between risk management and insurance. By spending more time on risk at the project development stage and in raising staff awareness to address risks themselves, greater risk management has resulted in a lower risk of claims. The business has, rightly, seen investment in risk management as giving a better return than simply putting money into insurance. This has meant risk managers spend more time managing the risk in the business and less on the residual risk via insurance – particularly as risks such as social media and reputation cannot be adequately addressed through insurance but via proactive risk management.

FUTURE OF RISK MANGEMENT
MODERN RISK LEADERS

Gearing up for the strategy journey

Risk managers are increasingly expected to share their expertise and knowledge at board level and their professional bodies are helping them meet the new challenge

Dutch company ASML makes machines that produce computer chips. It strives to develop machines that make ever tinier chips for use in high-end smart phones. But in 10 years' time, ASML expects its business model to be very different. Today it generates 95% of revenues by selling litho machines – lithography is the patterning technology that simplifies the manufacture of advanced chips. But by 2025, 80% of its revenues will come from machine servicing.

The rapid business transformation that ASML expects is typical of the risks that organisations face during this period of fast-paced technology-driven change.

"The changing business model, complexity and globalisation are all reasons why people are taking a greater interest in risk management," says Paul Hopkin, technical director of the UK's Institute of Risk Management (IRM).

"Enterprise risk management encourages a broader perspective by asking what we depend on to be successful and which risks could undermine those dependencies."

In 2013, ASML ran a materiality assessment to better understand its risks.

"We wanted to know what things we needed to do now to make sure that 20 years down the line we still have a successful business," says ASML vice-president, risk and assurance, Martin Reinecke.

"We did it from a sustainability perspective and to be responsible for our corporate behaviour. We are a market leader, we are multi-national and the people who do business with us presume we have zero risk appetite for non-compliance."

Embedding lessons

After investigating its risk landscape, ASML's next move was to embed its new understanding into company strategy. "Now, a lot of our risk activity is business-focused and is aligned to our strategic business objectives," says Reinecke. "We intertwined risk activity with our corporate performance management process, which links to long-term bonus incentives for our top managers."

The steps taken by ASML reflect increasing pressure from investors and regulators, against a backdrop of fast-paced change in business, for board directors to take more direct responsibility for risk. Operational risk managers are now expected to talk to board directors about risk and demonstrate how, by introducing risk into strategy, the business can better meet its performance objectives.

Setting the agenda

A report from ECODA (European Confederation of Directors Associations) and IFC (International Finance Corporation, the private sector arm of World Bank Group), entitled *Guide to Corporate Governance Practices of the European Union,* states: "The board is responsible for ensuring all business risks are identified, evaluated and suitably managed. In a world of increasing complexity and uncertainty, directors must manage risk more assiduously than ever before."

This view is crystallising across Europe. The Organisation for Economic Co-operation and Development (OECD) is reviewing its corporate governance principles and if it toughens up, many countries are likely to follow. The Netherlands has already passed a new law on data privacy, in anticipation of the forthcoming EU Data Protection Directive.

As risk managers begin to contribute to strategy, professional bodies are bringing forward certification schemes to support their members in this new role. About 70% of risk managers in Europe today have a background in buying insurance. Certification is seen as a way for these individuals to demonstrate to the board that, as well as having skills in insurance buying, risk management, and enterprise risk, they can step up to a strategic risk role.

"An evolutionary process has happened, from people buying insurance to people managing risk to people managing enterprise

'It is shaping up that there are two leaders, one on the board and one on the operational team. The risk manager ought to be stepping up to that operational risk leader role'
Julia Graham, FERMA

risk," says Julia Graham, president of the UK's Federation of European Risk Management Associations (FERMA). "Enterprise risk is evolving into risk as part of strategy. There is discussion about the role of risk leaders – and it is shaping up that there are two leaders, one on the board and one on the operational team. The risk manager ought to be stepping up to that operational risk leader role."

This view is shared by ECODA/IFC in their guide: "The execution of the risk management system should be entrusted to the management, which is in charge of daily risk."

Certification schemes

Both the IRM and FERMA have developed professional certification schemes that ask risk managers to demonstrate their knowledge and experience, to participate in continuing professional development (CPD) and to sign up to an ethical code.

The IRM scheme began earlier this year, when it published professional standards (see page 15), and FERMA is planning to share full details of its upcoming certification scheme at its Forum in Venice in October.

"It's important that behind our new certification scheme there is credibility and efficacy. We want people to know that certified risk managers go through a structured, consistent and independent process. We're not just handing out freebies," says Graham, who has led on the FERMA certification project, with the steering committee and committee chairman and FERMA Board member, Michel Dennery.

There will be two levels of its certification: Advance Professional, which will be available from early 2016, and Professional, which will be brought in the following year. Applicants must first demonstrate their qualifications and experience and, if eligible, they will then take an exam to determine "whether they are up to the mark", says Graham. They are also required to sign up for CPD and to a code of ethics.

"When your business model becomes more fragmented, there are greater risks embedded in the way you do business," explains Hopkin. "If manufacturing is overseas, perhaps in China, India or Bangladesh, operational risks such as health and safety need to be considered on a broader basis. It becomes a reputation or ethical issue and you need to look at things in a more holistic way."

"We'd like to see risk managers at the strategy table, encouraging the consideration of risk as strategy is formed," Hopkin says. "Certification helps with that. It says: 'I'm at the top of my business.'" **SR**

FUTURE OF RISK MANGEMENT
TALENT MANAGEMENT

This way for an exciting career

It's been a struggle to fill the talent gap in risk management left by the financial crisis, but efforts are being made to raise awareness among the younger generation about a rewarding career choice

Why is risk management facing such a dearth of young talent? A tight squeeze on graduate recruitment from 2008 to 2013, following the financial crisis, means organisations are experiencing an acute shortage of junior and mid-level candidates with three to five years' experience.

"As a recruitment company, we're sensitive to the fact that organisations didn't recruit graduates into their risk functions for about five years following the credit crisis," says Matt Brown, divisional director, risk, at corporate governance recruitment firm Barclay Simpson. "So now, when a company goes out to recruit a mid-level risk manager with five years' experience, there are hardly any there. There are just not enough candidates with that length of experience."

This is particularly true for financial services companies, where skilled credit risk and market risk candidates are in high demand, but it's also the case that graduate recruitment into all types of job role was put on ice during the downturn. Across the spectrum of risk management, from credit risk to market risk to operational risk, there are further reasons why young talent is in such short supply, and why attracting the best candidates into risk roles is a huge challenge.

"My friends probably think I'm an actuary or an accountant, that I sit at my desk all day and crunch numbers or analyse things. It seems like a dry type of job," says Judit Harangozó, Aegon UK senior risk relationship manager, and winner of this year's International Certificate Student of the Year Award at the Institute of Risk Management Global Risk Awards.

> **'Many young people think about the credit crunch, that the numbers and models didn't work well and risk managers were not good enough, so probably the role has a negative connotation'**
> Judit Harangozó, Aegon UK

In reality, says Harangozó, who studied international relations, including diplomacy and politics, in her native Hungary before entering risk management "almost by accident", her operational risk role is varied and people-focused.

"It comes with getting to know a lot of people and engaging at high levels of the company," she says. "So you build up your knowledge and your networks very quickly."

Lack of awareness

Lack of understanding about risk management roles among young job seekers is a big barrier to recruiting fresh talent. "There is a general lack of knowledge that these jobs in risk exist, and that they can be challenging and interesting and also well paid," says Carolyn Williams, director of corporate relations at the UK's Institute of Risk Managers (IRM).

One of the reasons for this is simply that risk management as a profession is a relatively recent development. "The problem that risk management has as a discipline is that there is no easily recognised industry standard," says Brown. "If you look at law or accountancy,

they have recognised qualifications, and if you talk to an American public accountant, they will know what a British chartered accountant is. It's much more established.

"There is not that commonality in risk management at this point in time. But then, it is very much a fledgeling profession – operational risk is not very old compared with law or accounting."

The idea of risk as a profession developed during the mid-1980s, but it competes for talent with the far more established career paths such as law, accounting and insurance. Candidates tend to fall into risk roles, as Harangozó says she did, or move across from other functions.

"The industry has to find a way to cope with the lack of supply of candidates," says Brown. "In the past, it has borrowed people with relevant skill sets and moved them into risk functions – certainly that's how operational risk as a discipline grew."

"Depending on their sector, different professionals will pick up the risk role," says Williams. "Lots of people come into risk from insurance, health and safety or project management."

The reputation of risk management as a profession, and particularly for roles within banking and financial services, may also be discouraging young applicants.

"Many young people think about the credit crunch, that the numbers and models didn't work well and risk managers were not good enough, so probably the role has a slight negative connotation," says Harangozó. "People relate to that and don't see what else the role could be."

As a recruiter, Brown notes similar sentiments among the top graduates. "My experience is that really bright people who graduated 10 years ago wanted to work in the banks, at the cutting edge of financial services," he says.

"Now it's tech – they're interested in digital, they want to work for Google. That's more appealing, more exciting, and the banks have a tarnished reputation."

The IRM has a programme of outreach activity at the main UK universities that offer risk management degrees. It gives presentations and maintains an "information-rich" website to help guide interested young people into the profession.

"IRM has students and members in more than 100 countries worldwide, but we don't market in those countries; they find us," says Williams. "We make sure that there is lots of information available online for people who want to find out more."

Clearer career path

The real game changer for the risk profession may be the move towards defining a clearer career path by introducing certification.

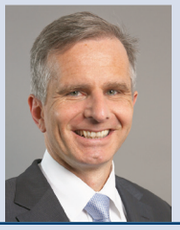
The IRM has this year published new professional standards in risk management, which set out the behaviour, knowledge and skills that risk managers should demonstrate across four key areas of risk and at four levels of seniority, from entry level right up to chief risk officer.

These standards combine with IRM's qualifications, code of ethics and continuing professional development programme, to create the new IRM certification scheme that has started this year.

"It gives risk professionals a badge, to demonstrate what they know, what they have done and how they behave," says Williams. "This is a much clearer career path through risk management than the industry has had before. It gives employers and recruiters an idea, if somebody says they're a risk professional, what to look for and what they will be able to do when in post.

"And it gives young people coming into the industry something exciting to aim for." SR

THOUGHT LEADERSHIP



JEAN-PIERRE KRAUSE
Chief risk engineering officer EMEA, Zurich Insurance Group

COVERING INTANGIBLE ASSETS? BACK TO DRAWING BOARD, PLEASE

Risks to intangible assets such as brand, goodwill, intellectual property or reputation present a big challenge for all of us in insurance. The fundamental question for companies, their brokers and insurers is the insurability of these non-traditional assets, which are difficult to understand, quantify and price. On top of that, as these assets are a consequence of how well a business is run, they are also open to moral hazard.

A host of risks could threaten intangible assets, but the triggers and the consequences are not well understood and a lack of historical underwriting data makes pricing difficult. All in all, this does not provide a recipe to generate a huge risk appetite.

The mechanism of risk transfer may not always be the first, best solution for such complex risk. Nevertheless, to remain a relevant business partner in an ever-evolving, globalised and interconnected environment, insurers must look at alternative ways to help their clients. Hence, back to the drawing board to engineer solutions.

To help businesses keep track of their risk exposures, Zurich has compiled a set of its most effective analytics services – its Risk Panorama. Based on an app, the Risk Panorama maps out a drawing board to a better understanding of a business's risk profile through a series of tailored, interactive and dynamic analyses around emerging political, economic and regulatory risks, claims history and risk benchmarking relevant to a client's industry. It is a first step to helping risk managers make more informed decisions.

Based on that Risk Panorama, the drawing board exercise continues by applying structured approaches to risk analysis – total risk profiling services, supply chain risk analysis or business interruption modelling.

These analytical tools will help the client better understand the underlying risks that threaten their intangible assets. Quite often, such analyses show that it is the underlying and well known 'hard' risks – lack of quality management, security, natural hazards – that threaten intangible assets as one of their consequences.

This drawing board exercise will guide the way to solving that insurability question, be it through new products or extending existing products, innovative self-retention using captives or even parametric insurance products. Nevertheless, any well engineered solution has it roots at a drawing board. So let's start there, please.

NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

FIND OUT MORE AT
zurich.com/my-zurich

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.

ZURICH®