EMERGING RISKS

Reactions

INTRODUCTION

What are the major risks that will impact the global re/insurance industry in 2018? That was the question *Reactions* posed to some of the global re/insurance market's senior and well placed figures.

There will be little surprise to read that cyber continues to be a major thorn in the side of the sector, and that is reflected in the number of references made to the peril over the coming pages.

However, other issues surrounding technological innovations also crop up several times. The internet of things is one topic that is causing concern, even though it could also be a help to the industry in the future as it may provide it with a better ability to track risks.

Autonomous vehicles is another technological development that is an emerging risk for the industry, not only in the sense of the new liabilities it creates (as well as the potential business opportunities), but also by the possibility that may completely overhaul the motor insurance market as we currently know it.

It is interesting to note that it is not only these modern perils that are a cause for consternation in the industry however. Even the classic property catastrophe exposure is referred to in the coming pages, and that is a risk the industry has had to deal with since its very beginnings.

CLARE BARLEY

CHIEF RISK OFFICER, ASTA

As the world evolves apace, insurers must grapple with managing emerging risks or face being left in the dust. Key challenges facing our market in 2018 include advancements in technology, climate change, intangible risks, such as cyber and intellectual property, protectionism, ILS and the shifting regulatory environment.

Emerging risks present a unique set of challenges. To meet them, insurers must consider not only the risks themselves but the processes by which they are managed. Looking beyond the underwriting impact is vital, with robust analysis including consideration of how emerging risks may affect customer demand, how they wish to interact with us and how we operate our business.

Listing emerging risks insurers may face is relatively easy. The challenge is getting a handle on them. Balancing breadth of coverage with depth of analysis, and getting the most value from effort expended, is key. Casting the net wide ensures potential risks and opportunities are caught early. Yet detailed analysis of a specific risk provides genuine business value, as the insights gained can be factored into new products and propositions. The right balance will depend on a business' needs and available resources.

"Listing emerging risks insurers may face is relatively easy. The challenge is getting a handle on them"

Prioritising can be based on time horizon, for example by focusing on near-term events such as the impact of the new General Data Protection Requirements legislation. While this ensures a business is fully aware of short-term developments, it is equally important to consider how the environment may change in the long-term. Emerging risks such as blockchain technology will affect how we do business and changing attitudes towards intellectual property risks may influence future insurance products. Focusing on the detail is important, but balancing that with the big picture is key to successfully managing emerging risks.

PAUL BASSETT

MANAGING DIRECTOR – CRISIS MANAGEMENT, ARTHUR J GALLAGHER

The nature of security threats has shifted dramatically over the last decade. Whether it is a malicious ransomware attack or act of terrorism, incidents are more frequent and any organisation, no matter its size, location, or sector, can be impacted. The devastating attacks of 2017 stand testament to this and business interruption is likely to continue in 2018.

Gallagher's research found that, in the last 24 months, 40% of large UK businesses had experienced a security threat, and this number is on the rise.

As businesses become more digitally reliant, cyber extortion could be a major problem. Patterns dictate that anonymous, low-risk, high-reward attacks, like WannaCry, will breed copycat attacks. For example, NotPetya, which followed just two months after, used the same hardware-infecting tricks to extract hundreds of millions of dollars.

Similarly, the advent of marauding terror attacks designed to cause mass casualties rather than property damage has created real and rising BI concerns. With today's typical attack it is the non-damage BI which poses the greatest risk, such as denial of access. Security cordons can remain in place for days, causing significant loss of earnings – just as we saw at London's Borough Market. After all, unless specified, non-damage BI won't be covered following a terrorism incident.

"As businesses become more digitally reliant, cyber extortion could be a major problem"

Amid an unstable geopolitical environment, it is more important than ever for organisations to put protective measures in place.

This presents the market with a new year's resolution for 2018: to help businesses build a culture of crisis resilience. It must go further than insurance, which only really relates to the recovery phase.

JOE CHARCZENKO

PARTNER AT CONSTRUCTION RISK PARTNERS, JLT GROUP

When asked to consider the top risks in 2018, we found ourselves much more concerned with the questions we do not have answers to, rather than the ones we do. The construction industry continues to grow and expand, yet there is little optimism in the business relative to the sustainability of this growth. Maybe we are still recovering from the Great Recession, but in reality there are major risks facing the construction industry and very little clarity to how these risks will be addressed.

The primary issue facing the industry is project finance. A real estate boom helped the industry emerge from recession, but as the real estate supply has begun to catch up with demand, the question of where funding for future projects has become a focus for the industry.

It is well documented that the United States has major infrastructure improvement and development needs, but questions around tax reform and federal funding remain unanswered. While there is a clear consensus that unlocking private investment could provide a solution to these needs, dysfunctional government has not provided support or direction to allow this funding to occur.

"Alternative delivery methods are introducing new, more sophisticated risks"

Outside of the funding challenges, innovation and technology are changing the risk profile of the construction industry. The advancement of alternative delivery methods are introducing new, more sophisticated risks that are proving increasing difficult to mitigate or insure. There is a clear need for creativity in the insurance industry as traditional products are not designed to address these risks.

The above combatted with the emerging issues of changing weather patterns, changing workforces, minority participation requirements, cyber exposure, new equipment/ construction methods and difficult legal environments are making construction projects more difficult (and costly) to complete. There is a clear need to find efficiencies in addressing these issues for the industry to continue to thrive.

JAKE CLARK

MANAGING DIRECTOR AND PUBLIC SECTOR SPECIALTY LEADER, GUY CARPENTER

The recent earthquake in Mexico has demonstrated how two innovative new risk management solutions – public private partnerships and insurance linked securities (ILS) – can be combined to improve national and global resiliency against natural catastrophes.

In August, the Mexican government partnered with the World Bank and GC Securities, a division of MMC Securities, LLC, to place its FONDEN catastrophe bond. The $360m, three-class bond was issued by the World Bank's International Bank for Reconstruction and Development, and represented the first listed property and casualty cat bond issued under its Capital-at-Risk notes program.

On October 10, 2017, the calculation agent, AIR Worldwide, confirmed parameters for the earthquake event and the corresponding full event payment to be paid to FONDEN. The full principal loss payment occurred on November 13, 2017, making it one of the fastest cat bond payouts in ILS history and demonstrating the speed and effectiveness of ILS protection.

"Governments worldwide would be wise to consider the use of public-private partnerships"

Currently providing approximately $80bn of the reinsurance industry's capital base, Guy Carpenter expects the ILS market to continue to generate demand and augment traditional capacity. Mexico, which also received a cat bond payout in 2012 due to Hurricane Patricia, already plans to replace the FONDEN bond, and governments worldwide would be wise to consider the use of public-private partnerships and the capital markets to improve future risk management strategies.

COREY GOOCH

DIRECTOR OF BUSINESS DEVELOPMENT, BROKERSLINK

Emerging markets are home to fast growing, strong companies that are driving rapid growth. In 2016, the GDP in these areas grew around 4.5% compared to 2.25% for developed markets. As businesses grow, so do their risks. However, many companies in high growth markets are underinsured relative to the size of their economies. Additionally, traditional insurance covers only 30% of losses from a disaster. This in effect creates a lag in insurance buying and a widening protection gap for clients. Thus, one of the biggest challenges the insurance industry will face in 2018 will be closing this gap.

Solving the problem of underinsurance in emerging markets is a global and growing challenge which requires commitment, collaboration and innovation. One example of innovative risk financing solutions is parametric insurance which provides a near automatic pay-out once pre-agreed triggers are met. Solutions like this can have a significant role to play in protecting businesses as they mature. However, we still have a long way to go to support growing businesses in developing markets.

"Many companies in high growth markets are underinsured"

Another threat to the industry is having a short-term focus on shareholder return instead of following the client's needs. Just recently, one of the world's most established brokers sold its business in six African countries, with more countries to come. This curbs growth in emerging markets and leaves businesses and people underinsured and vulnerable.

To address this, we must work to reverse these threats by recognising and embracing the opportunities emerging markets can bring, rather than selling our interest in these growth areas. Not only is it important to invest in the globalisation and growth of our industry, but it is also vital for our clients.

BRAD GOW

GLOBAL CYBER PRODUCT LEADER, SOMPO INTERNATIONAL

As we look to 2018, there are ominous similarities between today's cyber market and the property market of 25 years ago, when a single event – Hurricane Andrew – wiped out the cumulative profit amassed by property insurers over the previous 150 years. As the frequency and sophistication of cyberattacks increase, we need to consider whether the market is properly estimating potential losses when underwriting and pricing business.

As one of the few commercial P&C lines to experience significant growth over the past decade, the cyber market has attracted significant carrier interest. With generally positive underwriting results following the largely benign 2015 and 2016 underwriting years, a hyper-competitive environment has been created that continues to erode rates and expand coverage grants and claims triggers. Sublimits on the more difficult coverages have faded away, resulting in a considerable disconnect between the total quantum of exposed limits and the corresponding premium collected. A rough estimate has the insurance industry north of $100bn in limits for business interruption and contingent business interruption coverages potentially susceptible to catastrophic aggregation. The Wannacry and NotPetya malware attacks gave cyber insurers an indication of how quickly a game-changer can occur. Many organizations impacted were shut down for weeks, not hours, resulting in hundreds of millions in losses. These 'proof of concept' events demonstrate the potential severity of malicious code attacks and challenge many of the assumptions cyber underwriters make when setting SIRs and pricing primary and excess layers.

"Wannacry and NotPetya gave cyber insurers an indication of how quickly a game-changer can occur"

MARK HAWKSWORTH

GLOBAL TECHNOLOGY SPECIALIST PRACTICE GROUP LEADER, CUNNINGHAM LINDSEY

The nature of cyber risk and exposure has continued to change throughout 2017. From review of claims handled we perceive an increased threat in 2018 to new and developing attack vectors. There will be an increasing exposure to automated attacks using brute force to gain entry to web based services where weak passwords still prevail.

We predict that the use of social engineering in cyber fraud will also increase. In 2017, we have already seen criminals in the supply chain interacting with both parties using compromised email servers to steal both goods and the funds in payment of the goods.

Attack vectors have also changed, in previous years criminal have targeted smaller companies. We believe that in 2018 this trend will continue further along this path leading to increasing cyber-attacks against the general public. To counter this trend, there has been an increase in the number of personal cyber policies being sold within the market, covering threats from cyber bullying to loss of funds though on-line transactions.

The evolution of ransomware was a significant trend in 2017 with the development of Petya hybrid malware incorporating both encryption and worm code. This trend will continue throughout 2018 and business that does not take the initiative and protect its data will be susceptible to these growing malware attacks in 2018.

To cap it all the General Data Protection Regulation comes into force in 2018. It is an EU regulation that applies to every country in the world. Companies not compliant by May 2018 and losing personal identifiable information could face fines of up to 4% of their global annual revenue. Companies must prepare, this should be the number one priority for business owners and company boards as we enter 2018.

"There will be an increasing exposure to automated attacks"

GREG HENDRICK

PRESIDENT, PROPERTY & CASUALTY, XL CATLIN

We believe that closing the protection gap – the disparity between economic and insured losses – represents our most formidable challenge for 2018 and beyond. It requires a concerted effort by re/insurance industry players, governments, and other private and public organisations.

In 2017, estimates indicate the effects of Hurricane Harvey in Texas will cost $75bn; more economic damage than Hurricane Katrina. But insured losses may only reach $25bn, leaving two thirds of the loss uninsured.

The Insurance Development Forum (IDF) estimates that 70 percent of the economic losses from natural catastrophes remain uninsured; and even higher in middle/low-income countries. Even in developed countries, insurance is unlikely to exceed 50 percent of economic loss.

We have made closing the protection gap a strategic priority to which we dedicate significant time, funding and resources. Given our expertise this is the right thing to do, but it is also a potential source of new risk pools for the industry.

"Closing the protection gap represents our most formidable challenge for 2018"

Our dedicated team of experts from ERM, re/insurance underwriting, regulatory and emerging markets, are involved in numerous projects. We're sponsoring research on the correlation between insurance penetration and the time it takes a country to recover from disasters. We're part of the IDF – a public-private partnership comprising representatives from the UN, World Bank and the re/insurance industry, where we're working to help developing countries create the regulatory frameworks and institutions that are needed to support a viable private insurance market. And as a founding member of Blue Marble Microinsurance, we're working to nurture and grow microinsurance projects globally.

ANDREW JOHNSTON

GLOBAL INSURTECH OUTREACH AND RESEARCH LEAD, WILLIS RE

In North America and Europe, an increasing number of InsurTechs are shifting focus away from alternative distribution and front-of-house activity, concentrating more of their attention to supporting insurers with improved back-end solutions. These processes embrace claims handling, underwriting, pricing, optimising available data and integration of artificial intelligence to automating high volume low complexity tasks to reduce internal costs and improve services. Why? Because they now understand that originating customers is complex and expensive and the clichéd battle-cry to reduce distribution costs is easier to say than to achieve given the complexity of the insurance model in developed economies.

Over the last 24 months, the InsurTech ecosystem has been an experiment for start-ups and incumbents alike. At the beginning of 2017, approximately 80% of all self-identifying InsurTechs worked on front-end solutions, either as a standalone entity, or in collaboration. Fast-forward 12 months, and a realisation that focusing on front-end processes, products and systems is difficult and navigating regulation, scaling nuanced products, financing risk, customer acquisition, and building a brand; the sine qua non for disrupting the current value chain, is prohibitive for many.

"InsurTechs are shifting focus away from alternative distribution"

Where significant gains have been made is in integrating innovative technology into the current Insurer model. One such success story is UK-based 'RightIndem', an InsurTech who originally developed a front-facing solution for insureds to take photographs of damage, but have pivoted by developing and integrating claims handling software into the back-end systems of many carriers writing motor policies also. The cost savings associated with their software, and the improved consumer experience provides the carriers with an opportunity to reduce frictional costs thereby enhancing returns.

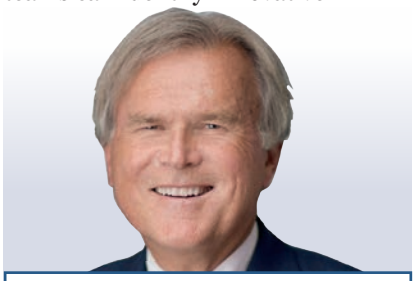
KEVIN KELLEY

CHIEF EXECUTIVE, IRONSHORE INC

Education, education, education is what will be needed to prepare underwriting professionals in a dynamically changing environment and the key challenge industry executives will need to address in 2018. Underwriting is a learning profession. Executive leadership who embolden their front line underwriting teams to anticipate, adjust and adapt, will position them to meet demand in a new multifaceted risk world.

Profiles of risk are being dramatically altered at a breath-taking pace. Technology disruption, alternative capital, and industry consolidation are just a few notable drivers of the global economy that are specifically impacting risk factors in specialty property casualty markets. A record year of natural and man-made catastrophic events worldwide adds even further complexities.

Specialty property casualty commercial insurance represents a $75bn to $100bn global industry. The US is the largest segment and, generally, the first to see and implement rate change when needed. Well-informed underwriting teams can identify innovative solutions in response to insurance coverage implications brought on by inevitable market shifts. Preparation should include data and analytics, meaningful historical lessons, and market-specific underwriting conditions. Underwriting selection, rating to exposure and appropriate contract language all need to be revisited to confront rapid market transformation. We are seeing rates moving upwards and expect that to continue through the next several quarters of 2018.



"Profiles of risk are being dramatically altered at a breath-taking pace"

Leaders who get it right will be early to market with educated staff confident in their abilities to meet client demands. A disciplined approach to underwriting will likely ensue as staf are sufficiently armed with the tools and insight to effectively uncover opportunity triggered by new market realities.

FRIEDER KNÜPLING

CHIEF RISK OFFICER, SCOR

Climate change is posing unprecedented threats to the re/insurance industry and society at large. The scale of the global risks associated with extreme weather events and longer-term changes to climate patterns is a source of alarm, especially given the staggering complexity of our climate systems and the slowly developing scientific knowledge about them.

Are we factoring climate change into our medium- to long-term strategic plans? Are we taking sufficient action to make our business models sustainable? Is there a close enough dialogue between our risk experts, who often need to focus on the shorter perspective, and the academic community researching the medium- to long-term changes in climate patterns? Are climate-related risks properly factored into pricing, underwriting and investment decisions? Do we sufficiently understand the secondary impacts of climate change on human health, disease spread, famines and climate-related mortality? Are we sufficiently conscious of how political uncertainties, populism, economic instability and climate change may influence each other, and are we doing enough to ensure that we influence these factors for the better? Are the impacts of climate change on the affordability of insurance cover, the global protection gap and catastrophe resilience adequately understood and anticipated?

"Are climate-related risks properly factored into pricing, underwriting and investment decisions?"

Over the past few years, SCOR has continuously invested in climate-related research, actively fostering the dialogue between industry and science, and has adapted its underwriting and investment process, incorporating strengthened sustainability criteria. re/insurers need to make sure that they constantly improve their understanding of these risks, and that they have the appropriate models and data in place to do so, thereby assuming their global responsibility.

ANTHONY KUCZINSKI

PRESIDENT AND CEO, MUNICH REINSURANCE AMERICA, INC.

The catastrophic events of the last several months are a stark reminder of why our industry exists: to help ensure that communities, businesses, and families can rebuild and thrive. As we at Munich Re look back on not just the last year, but the last 40 years, one thing is clear: extreme events are the new normal.

This is not just about the hurricanes, flooding, and wildfires we've experienced in the US in 2017, but also the heatwaves, droughts, tornadoes and severe storms we've experienced around the world. Global economic losses caused by natural catastrophes worldwide are a serious problem, since less than one-third are insured. Even here in the US, half – or even more – of total losses from natural catastrophes are not covered.

The re/insurance industry must understand and evaluate the risk posed by the current and future environment we face.

While we can look backward to historical events, we must also support research and data analytics approaches that look forward to understand the risk we face now and into the future.

"One thing is clear: extreme events are the new normal"

Munich Re has been a pioneer in researching changes in the frequency of these kinds of loss events, and we have made use of this knowledge to better understand weather and climate risks and to develop solutions for them.

I believe that in 2018 re/insurance can and will understand and cover more losses, and also collaborate with public and private partners do more to foster resilience and promote sustainability. As a result, we will help our society and economy cope with the consequences of extreme events and respond to the new normal.

ANDREAS KULL

CHIEF RISK OFFICER, TOKIO MILLENNIUM RE

Over the past two to three years, threats to the global economy and society have not changed significantly. Key drivers of risk remain climate change, cyber risk, political and economic instability, terror and unanticipated impact of chemical agents on humans and ecosystems. Recent events such as large-scale cyber-attacks, major hurricanes and heightened political uncertainty related to Brexit and the US have only helped highlight more clearly existing exposures, loss potentials and the interdependency of risks.

Given recent events, risk functions should be concerned first and foremost with backtesting their models, by understanding how past risk assessments differ from the actual impact of events. Second, risk functions should continue to refine their understanding of known and emerging risks, considering how innovation including predictive analytics, big data and partnering with technology firms can provide new insight into the nature of risks. Third, risk functions together with senior management teams should consider threats to business models themselves arising from factors such as overregulation, disruptive technology or erosion of profitability due to abundant capital. Beyond focusing on risk as a threat, risk agendas should refocus on partnering with business functions to enable the identification of new opportunities and, where possible, push the boundaries of insurability benefiting not only the own company and customers but ultimately also society.

"Given recent events, risk functions should be concerned first and foremost with backtesting their models"

In summary, it remains of fundamental importance to foster a sound risk culture by embedding risk management systematically into all businesses processes. This will enable risk-taking functions to identify business opportunities early on and to deploy risk capacity efficiently in line with risk constraints.

PAUL MANG

GLOBAL CEO OF ANALYTICS AT AON

Our recently launched Global Insurance Market Opportunities report focused on the key risks and opportunities for insurers, and one of the highlights was the sharing economy, which is a business model that has wide-ranging implications for how the economic landscape might be organised in the future.

Such platforms generate a number of risk-related opportunities which warrant close attention from us, and as an industry we need to be flexible and innovative in order to maintain our relevance in this new environment. We should remember that when products or services are transferred to an Uber-type platform for example, it doesn't mean the risks go away; they just get shifted around. For instance, at Uber there are two million drivers with certain risks that might have been solved by workers' compensation cover.

While we do need to invent different sets of products to manage within this changing risk context, the theme of change is allowing our industry to achieve net new growth.

"Cyber risk doesn't respect organisational boundaries"

Cyber risk is another evolving area we address in the report. Identifying and quantifying cyber risk has proved a challenge for insurers, but new models are being created. In fact, we are currently working on the aggregation models that insurers need to make progress in the cyber risk space. Cyber security risk has special challenges, not least of which is that those perpetrating the cyber breaches are also highly innovative.

We are committed to cutting across all the traditional boundaries that have existed within intermediaries and carriers. Cyber risk doesn't respect organisational boundaries; it's not just a technical issue. It's an enterprise risk that includes compliance, operations and reputation among others. It requires a holistic approach from us.

WILLIAM MCDONNELL

CHIEF RISK OFFICER, RSA AND CHAIRMAN OF THE EMERGING RISKS INITIATIVE OF THE CRO FORUM

Autonomous machines increasingly feature in business's and people's everyday lives. With exponential advances expected in the next few years in artificial intelligence, robotics and data-supporting infrastructure, autonomous machines are set to become even more prevalent in the public space.

Autonomous machines encompass self-driving cars, robots and autonomous equipment used for manufacturing, mining, farming, transport, medical care and assistance, lethal autonomous weapons and many other applications. They represent important examples of technological developments that are occurring quickly, affecting almost all sectors of the economy, and leading to important new legal, regulatory, societal and ethical considerations.

In particular, autonomous machines may have profound implications for re/insurance. As human error is the main cause of accidents, a wider use of autonomous machines might lead to a transition from loss frequency to severity, and losses may accumulate in new ways. Autonomous machines also have the potential to significantly improve risk management, prevention and disaster investigation.

"Autonomous machines may have profound implications for re/insurance"

These developments will create a societal demand for a new framework of safeguards and insurance will be one of these. By managing risks, insurance allows individuals and companies to take risks and to innovate.

The full extent of impacts from autonomous machines on the re/insurance industry is still difficult to assess. Whilst some of the vulnerabilities are already apparent, it is clear that the opportunities offered by these new technologies are immense, as highlighted in a recent publication by the CRO Forum's Emerging Risks Initiative.

NIGEL MORTIMER

PRESIDENT, ARGO INSURANCE

Three words come to mind.

Catastrophes: Predictive climatology suggests that hurricanes, earthquakes, droughts, fires and floods will increase in both frequency and magnitude. As claims mount following catastrophes, rates will rise and coverage will contract.

Capital: It's been surprising to see how quickly the capital markets reloaded after 2017, despite the $100bn-plus losses in the wake of hurricanes Harvey, Irma and Maria, the earthquake in Mexico and the fires in California. As capital persists, the pressure on pricing will too, especially in reinsurance markets and even as London reinvents itself. In 2018, we'll see some capital investors swing away at last, as the size, latency and longevity of the risks propel them to seek more predictable profits elsewhere. Rates may then rise to reflect the true risk prudently.

Cyber: Cyber is unique in that the risks are both unlimited and perpetual. Digital attack and defense are opposing forces in a war of escalation, with solutions such as blockchain in turn becoming prestige targets for hackers eager to make their mark. While we can sense the scale of the problem by examining assaults, such as those against Merck, we have no idea of the possible impact of new hacking technologies against multiple, smaller entities. Imagine the losses following concurrent attacks against one million small businesses, the shut down of every self-driving car, or perhaps just the bricking of every digital door lock. The payouts could be massive, and yet today's premiums for those small-scale customers in no way reflect the scope of the risk, precisely because we don't know what that scope is. On the other hand, because the digital arms race will be perpetual, cyber offers our industry the best opportunity we've seen since the advent of shipping.

"As capital persists, the pressure on pricing will too"

JONATHAN PRINN

GROUP HEAD OF BROKING, ED

The largest emerging risk is that 'hardening' reinsurance and direct markets mask the underlying issues within our industry related to distribution costs.

2017 has been filled with talk of blockchain and insurtech. Exotically named outfits have claimed wins over our traditional industry in terms of client experience and speed of claims payment.

However, their secret sauce has always been to cut distribution costs.

The 'traditional market' must place greater focus on this – despite the potential of more flattering gross rates in the future.

Disruption is an overly used term, but facts are facts. Look at the intermediary costs of MasterCard, of estate agents, to use Amazon, eBay, Apple Pay – none of those are close to the 30% average that our industry pays to intermediaries.

Sitting in the east side of the square mile, I am acutely aware that the west side was full of stockbrokers. They are all gone. The time and cost to trade stocks is now real time and free.

"'Hardening' reinsurance and direct markets mask the underlying issues within our industry related to distribution costs"

Let's be clear, I am a middle man, not a carrier running a 97.9% combined ratio (pre-Q3 2017) or a client questioning the value they receive for 30% of the premium. The argument is that that we are 'not a commodity' and, as specialty re/insurance is bespoke, the middle man does more. Maybe we do – but not 30% more.

As the market reacts to HIM and other losses, we cannot allow issues that have dogged the market for years to be brushed aside.

Perhaps, if premiums rise, there is even more reason for brokers to reduce the percentage amounts they receive and adjust their cost bases to reflect that the intermediary of the future will earn less.

The threat to our industry in not reacting or ignoring this issue as the tide rises is terminal.

PAT REGAN

INCOMING GROUP CEO OF QBE INSURANCE GROUP

We are in the early innings of the dramatic change that advances in technology will have on both the insurance industry and the world in which our customers operate.

Embracing this change is the biggest challenge faced by the insurance industry. We need to innovate faster than ever before as there's so much opportunity to create new products and services, improve processes across the value chain and capture new market opportunities. Failure to innovate will mean being left behind.

Insurers need to accelerate adoption of the full gamut of emerging technologies – everything from machine learning to data science, text mining, image recognition and the internet of things.

"We need to innovate faster than ever before as there's so much opportunity to create new products and services"

One of our strategies at QBE is to seek out partners who can provide access to differentiated technology. We've established a corporate venture fund with a focus on forming enduring commercial relationships with startups that will enhance our business model, drive efficiencies and develop new avenues of growth.

Establishing QBE as a partner of choice within the startup ecosystem is only part of the solution. In a fast-changing market, a focus on intermediaries and end customers is essential.

We will only succeed if we listen to our customers and match our offering to their needs.

CYBER RISK IN AN INTERCONNECTED WORLD

Innovation and transparency are key factors to better understand the threats of both attritional and systemic cyber risks.

In a digital world, cyber exposure evolves every day, making it one of the most dynamic emerging risks in the industry. Just as the housing boom along the U.S. shoreline accelerated property losses, the technological sophistication and digital connectivity of the global economy have increased the cyber threat for all sectors. As large-scale breaches become more damaging and pervasive, the re/insurance industry needs to continue to innovate to address potential systemic events, aggregations, and modelling capabilities. As such, 2018 will be a year of product growth and new challenges. In order to advance this important market, we must develop a common analytical language, harness advanced modeling technologies and learn lessons from other lines of business.

To diversify the U.S. cyber market beyond confidentiality and data breach, we must continue to expand into other areas, such as operational technology (OT) risk and data integrity. Growing supply chain dependencies both between companies and across operating systems and internet services greatly enhance OT exposure, while over 80 percent of the S&P's value is tied to information-based assets that could be impaired in a systemic cyber-attack. Forty years ago, the opposite was true. To develop solutions for both exposures, re/insurers need a common cyber risk currency that gives underwriters, actuaries, cat modelers, brokers and others a common terminology and set of metrics with which to measure companies' reliance on particular suppliers and systems and the true, sometimes nebulous value of data. As insured cyber loss continues to emerge and transparency around network and operating system supply chain dependencies evolves, Guy Carpenter is helping this become a reality.

While we have made improvements modeling modern interconnections, it remains extremely challenging to accurately model how dependent any one company may be on a given supplier or system, or its level of enterprise risk management and cyber resilience. As seen with WannaCry and Petya earlier this year, reliance on one specific operating system determined the level of exposure many companies faced, and those with less rigorous risk mitigation strategies often fared the worst. But it is difficult to quantify that dependence and resilience to develop an accurate picture of potential risk. And with growth in automation, cyber-physical systems, the Internet of Things, cloud computing and cognitive computing, manufacturing and infrastructure assets operating in an Industry 4.0 world are more exposed to cyber-attack than ever before. There is much greater systemic OT potential, yet current models are not yet quite as credible as those property catastrophe carriers use to define a given event's impact when taking into account a particular exposure zone and resiliency level.

In the U.S. and soon, Europe – given the General Data Protection Regulation and plans for a new U.K. Data Protection Bill – regulation drives data confidentiality and breach solutions. And while these protect against data reconstruction costs, if that data has been compromised, it may be worthless. Data integrity and availability is as critical as data confidentiality, and are not always associated with a company-specific breach or malicious attack. Reliance on an infected or malfunctioning operating system or internet service may render a company's information

assets useless without them even knowing it, and without a common risk understanding that recognizes and defines the intrinsic value of data integrity, providing the most comprehensive coverage for the risk is difficult.

The new year will also offer cyber carriers the chance to seize opportunities created by innovative technologies to adapt lessons from other lines of business. Today, risk management of a cyber event reflects characteristics of pandemic containment. The medical community has developed clearly defined metrics and rigorous procedures for public and private stakeholders to reduce the impact of an outbreak. Similarly, the date of occurrence, duration, common source connection, frequency and severity are significant factors in adjusting cyber re/insurance claims, and often depend on some level of collaboration with public entities. But as discussed above, a common currency to analyze and discuss cyber exposures is still being perfected. Quantification of cyber losses is also complicated by 'silent' all-risk policies where cyber is the peril, but no cyber exclusions exist.

Further, one of the key steps in addressing a pandemic outbreak involves early intervention and treatment, just as response to a cyber event depends on patching, repairing, and rebuilding software and networks quickly to restore customer confidence. Modern travel means a carrier of MERS or Ebola can potentially infect hundreds of people in a day. Malware such as Wannacry and Petya can spread and infect global networks even faster. Wannacry alone has impacted banks, factories, hospitals, government agencies, schools, and transport systems in at least 150 countries, freezing computers, encrypting data, and demanding money through online bitcoin payments. The next attack could threaten critical infrastructure such as nuclear power plants or a power grid. Response and containment depend on early detection, robust understanding, and effective treatment.

But the challenge of the current modeling techniques is that the inputs and outputs are often not fully understood, which can be the key decision-making variables for re/insurers, who have a fiduciary obligation to understand their risks. The Internet of Things, insurtech startups, and the proliferation of smart devices enable the transparent, real-time data capture that can empower advanced interoperable models.

> "The re/insurance industry needs to continue to innovate to address potential systemic events, aggregations, and modelling capabilities"

More effective, nimble analytics validated in an open source environment will allow users to confidently set enterprise risk management plans around cyber exposures. As our industry continues to better understand the cyber landscape, a push to develop interoperable models that leverage user-sourced, real-time data will increase the speed in which practitioners in both cyber and health fields can analyze events, quantify impacts, and deploy forensic response resources, lessening the loss for what can often be a global event.

The transparency of interoperable models also allows users a clear understanding of the assumptions that drive the results, encouraging collaboration by re/insurers, entrepreneurs, scientists, actuaries, computer programmers and others. This empowers multiple scientific views to inform hazard modules, the use of clients' own claims experience to shape vulnerability assumptions and financial engines better reflect the complex nature of policy coverages. As the variety of threat actors continue to increase, such as state-sponsored agents, this diversity of inputs will especially help when confronting zero-day cyber-attacks, which can confound established treatment processes. Interoperable, transparent, and auditable catastrophe models will benefit cyber stakeholders in both the public and private sectors by aiding the development of a common cyber currency that empowers ownership of risk and more informed, effective, and defensible risk management decisions.

Along with interoperable models, the right insurtech investment decisions can bring potential value-add opportunities to cyber risk management. The insurtech marketplace is expanding and represents the evolutionary next step for re/insurance, combining data, analytics and technology in new and innovative ways. By more effectively and efficiently leveraging the robust data these companies create, and delivering it in seconds via mobile devices, the industry can drive down costs and increase client value.

To advance cyber solutions, Guy Carpenter continues to work alongside our clients to better understand this emerging risk, applying our history of broking, analytical and strategic advisory expertise to dynamic trends in OT, business interruption and data integrity coverages. We are collaborating with thought leaders in both the re/insurance space and in technology, robotics, and computer fields to gain insights into some of the most difficult to model exposures for this product and peril. This not only creates profitable growth opportunities for insurers, but improves the speed and effectiveness of public and private containment efforts that can help avoid a national or global event, better protecting communities, businesses, families, and resources.

By Jeremy S. Platt, Managing Director and U.S. Cyber Specialty Practice Leader, Guy Carpenter & Company, LLC

ZBIGNIEW ROŚ

CYBER RISKS PRACTICE LEADER AND SENIOR RISK MANAGER, MAI CEE

With the implementation of General Data Protection Regulation (GDPR) on the horizon, risk managers and insurance buyers in Central and Eastern Europe are becoming more aware of the cyber threat. The severe penalties for data breaches GDPR carries is spurring investment in cyber security in a way that hacks and breaches have not. The take-up of cyber insurance policies, however, remains low, largely due to a lack of a co-ordinated promotional effort.

With few examples of high-profile hacks in CEE, a knowledge gap exists regarding the damage that hacks, leaks or data breaches can cause. Awareness is also lacking about how insurance can help, with many policies offering immediate expert assistance following a breech. Closing that gap will require a coordinated response from both brokers and insurers, to educate business leaders.

As yet, cyber coverage remains niche in the region. However, the largest insurers in more developed markets such as Poland are hoping the launch of their own cyber products before GDPR's May deadline will start to change that. A number of banks are also planning to include cyber in their SME bancassurance.

"The take-up of cyber insurance policies remains low"

A key development in 2018 will be the growth of simplified products, with modular coverage set to become widespread. Higher limits are also increasingly required by international entities investing in the region. The added benefits of cyber coverage, such as external cyber forensics as part of the policy, must be promoted to buyers.

In 2017 dozens of data breaches affected millions of people globally and those of us operating in CEE must ensure our clients fully grasp the issues and gain the necessary protection. GDPR and the ongoing rise in hacks globally are gradually focussing minds in CEE, and the market must continue its efforts to strengthen local resilience against the growing cyber threat.

KATHLEEN SAVIO

CEO-DESIGNATE ZURICH NORTH AMERICA

Our world is changing at a faster rate than ever before. Some say we are in a period of exponential change that will have a profound impact on the insurance industry and our customers. This rapid change will exacerbate certain risks, such as distracted driving, severe weather and cyber, and Zurich is helping our customers to better understand and manage these and other risks.

Distracted driving has caused rising losses throughout the industry and created a particular challenge for risk managers whose organisations rely on fleet auto and trucking as core to their businesses. While technology (namely, smart phones) is typically to blame for the increased risk, it is technology that may ultimately reduce the risk. Autonomous vehicles and accident-avoidance technology have the potential to propel us to safer roadways.

Severe weather continues to be a major risk for our customers, especially as populations concentrate in coastal cities. Nearly 80% of the US population lives in counties that experienced at least one weather-related disaster, based on six years of data from FEMA. Insured losses from Harvey, Irma and Maria could reach $100bn, but the total economic impact from these events is expected to be much higher.

"Distracted driving has caused rising losses throughout the industry"

When it comes to cyber risk, our customers look to us for risk avoidance as much as risk transfer. The Internet of Things presents complex security and privacy challenges and a wide range of vulnerabilities, from hacking into a nuclear energy facility to accessing your webcam. Technology is evolving the way we live and work, and risk management must evolve with it.

These are complicated risks. Our focus is to help customers be more resilient. Helping them solve these complex problems is what drives me and is at the heart of Zurich's purpose.

FRANK SCHEPERS

INSURANCE CONSULTING AND TECHNOLOGY LEADER, EMEA, WILLIS TOWERS WATSON

So, why would we regard something – IFRS17, the new global insurance accounting standard – that comes into effect for reporting periods beginning in January 2021 as the big issue for 2018?

Starkly put, if the industry thought Solvency II was and is complex and challenging, IFRS is a blue whale in comparison. Some CFOs are talking about the industry implementation bill being double that of Solvency II. So, the rest of the world should be on notice of the scale of the challenge that will face all listed insurers (in the European Union), as well as many unlisted insurers in a number of jurisdictions.

Add to that, the 2021 live date is deceptive. The reality is that, due to the need for comparatives, companies that report on a calendar year basis will have to be able to produce a complete set of numbers for 2020 as well. For insurers looking at performing a full dry run, realistically that means being ready as early as 2019.

Maybe that would be fine if companies had started preparing early, but most haven't. Failure to start accelerating the pace in 2018 is likely to lead to panic, inefficiency and poor decisions in 2019 and 2020. Notably, in Europe, business and strategies that work under Solvency II may look completely different in the IFRS17 world.

"If the industry thought Solvency II was challenging, IFRS is a blue whale in comparison"

Understandably, a new accounting standard doesn't get most people's blood racing. The prospects for InsurTech, cyber risk coverages or autonomous cars may indeed make for more exciting conversations, but whereas their impact on the insurance industry may ultimately be groundbreaking, IFRS will have a real, short-term effect.

The time for talking and contemplation of the tasks involved is over. The complexity of IFRS 17 means that proper groundwork and action are crucial to facilitate the shift. For many insurers that means 2018 will (or should) be the year of IFRS.

PATRICIA TITUS

CHIEF INFORMATION SECURITY AND PRIVACY OFFICER, MARKEL CORPORATION

Digital transformation and innovation are key areas that many companies are embracing, largely for fear of being left behind in the marketplace. However, the stakes have never been higher as the Internet of Things (IoT) bursts into mainstream and consumerisation of information technology is placing cyber security as an emerging risk in many enterprise risk management reports. With the explosion of insurtech investments in the billions many insurance companies are looking to grab these new capabilities with the intention of being first to market. Unfortunately, cyber security continues to be lagging in the technical or software design which means companies will have to scramble to either add it in, accept the risk or delay delivery until security measures are implemented to close the security gaps.

A great example is the Mirai malware which attacked IoT devices and was used to launch a denial of service attack against several companies causing business disruptions. Because this attack didn't directly impact the consumers the IoT manufacturers were in no rush to fix the problem. Imagine how the expansion of IoT in the workplace and the far reaching ramifications will continue to emerge over the coming months.

"Cyber security continues to be lagging in the technical or software design"

While cyber security has been recognised as a risk, the continued growth in digital and innovation coupled with the threat surface complexity, cyber security is once again moved from mainstream business as usual and compliance requirements to an emerging disrupter.

DAN TRUEMAN

GLOBAL HEAD OF CYBER, AXIS

2018 will see a renewed focus from regulators, senior executives and reinsurers on the impact (or potential impact) of "silent," or non-affirmative, cyber coverage and the correlates with affirmative cyber coverage.

As a company's digital assets increasingly interact with its physical property (such as through the Internet of Things), there is a growing concern that businesses are not adequately prepared for the business interruption or physical damage that can occur as a result of a large-scale cyberattack.

Cyber is a peril, not just a product – and cyber as a peril is not just about data breaches. Thus, when firms purchase a cyber product it may not fully address the ways that cyber events may impact the business. The industry is right to begin to question this ambiguity. Leaders are right to be asking for more clarity.

The world is changing, and cyber risks are becoming far more prevalent across most developed economies.

Digital risks for businesses are now inherent in almost every activity a company undertakes.

"Digital risks for businesses are now inherent in almost every activity a company undertakes"

Cyber risks can have a significant impact on a company's existence, physical or financial. Losses that occur for these inherent digital risks are being pushed into traditional property insurance markets, which are not adequately pricing for the potential losses to physical property or properly understanding the full scope of the risks and the coverage that is required.

The industry must do a better job educating brokers and insureds on the specialised nature of cyber risk, as well as its expanding scope.

In 2018, the cyber risk debate will no longer be confined to just data breaches. Cyber risk exists across the insurance industry's products. Where cyber risk exists it must be priced accordingly.

We can no longer be silent on the risks of "silent cyber".

KEITH WOLFE

PRESIDENT US P&C, SWISS RE AMERICA

In the wake of an extremely active 2017 hurricane season there's a growing conviction that the private insurance industry needs to take on more flood risk now that it understands the peril better than ever.

That can only help the flood insurance crisis, which up until now has challenged the public and private sectors alike. There's reason for optimism because of significant movement on two fronts:

A broad based coalition of realtors, insurance regulators, taxpayer advocates and environmental groups supports legislation to accelerate growth of the private flood insurance market.

Reinsurers and insurers are using increasingly advanced technology and mapping to quantify flood risk at a granular level.

When it comes to flooding, there are two important numbers to remember: 10 and 15. In an average year we see a staggering gap of $10bn between insured and uninsured flood losses, due in part to the fact that only 15% of American homeowners have flood insurance.

"In an average year we see a staggering gap of $10bn between insured and uninsured flood losses"

The reasons are often intuitive. Some people incorrectly assume they're covered, others think it won't happen to them and many believe they can't afford flood insurance.

That will change, however, as reinsurers and insurers develop affordable coverage that accurately reflects the risk because it's priced on the individual exposure and its unique characteristics.

The private market is ready to assume a substantial share of the burden, which will bring relief to financially stretched governments. While Swiss Re and others support the NFIP through reinsurance arrangements, the program's future depends in part on the will of the legislative and executive branches of federal government. That's why private market involvement in flood risk transfer will be more essential than ever.

Lose the ROLODEX

JOIN OUR LINKEDIN NETWORK

Over 4,000 [re]insurance professionals on Linkedin at:
Reactions - Global Insurance and Reinsurance

Reactions - Global insurance and [re]insurance is the platform to:

- ★ Read exclusive Reactions' content ★
- ★ Post relevant industry information ★
- ★ Create and engage in discussions ★
- ★ Network with other industry professionals ★
- ★ Receive important updates and event information ★

Reactions gets social!
www.reactionsnet.com

Reactions

GUY CARPENTER

BRINGING
OPPORTUNITY
TO RISK

ADAPTATION + OPPORTUNITY = GROWTH

With the increasing sophistication of technology, adaptation brings opportunity. As large-scale cyber breaches become more damaging and pervasive, the (re) insurance industry as a whole needs to evolve and continue to innovate. Guy Carpenter helps clients adapt to change, thrive and prosper. To be added to our distribution list for cyber risk news updates, please visit https://cmp.guycarp.com/cyber-newsletter/.

MARSH & McLENNAN
COMPANIES