GUY CARPENTER

INTERACTIVE PDF INSTRUCTIONS

This interactive PDF allows you to access information easily, search for a specific item, or go directly to the first page of that section.

GUIDE TO BUTTONS


go to table of contents


search this PDF


go to next page


go to previous page

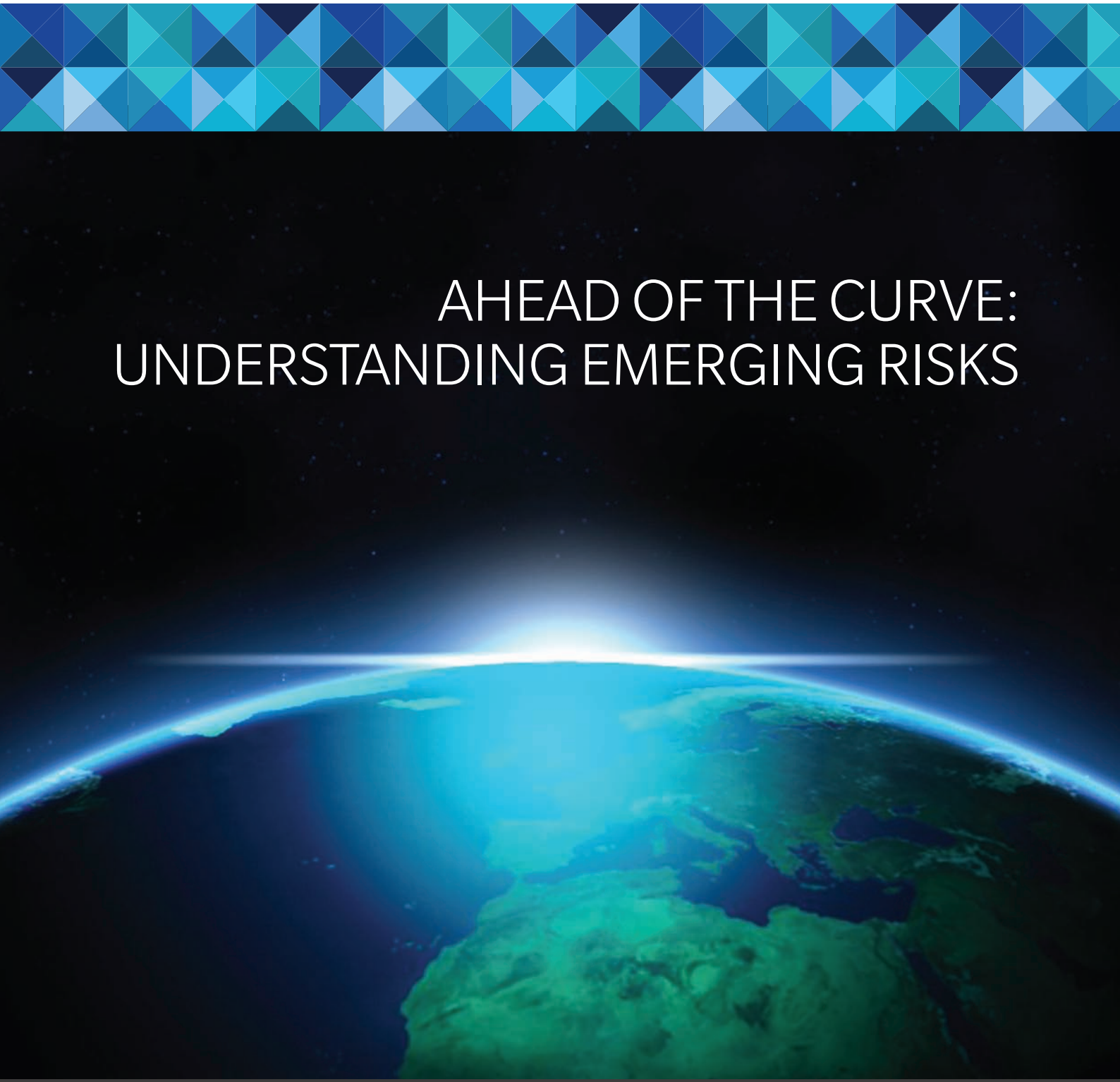
TABS

Clicking on one of the tabs at the side of the page takes you to the first page of that section.

Please note: if you are viewing this content on a tablet or mobile device, functionality for Buttons and Tabs will be disabled.

GUY CARPENTER

AHEAD OF THE CURVE: UNDERSTANDING EMERGING RISKS

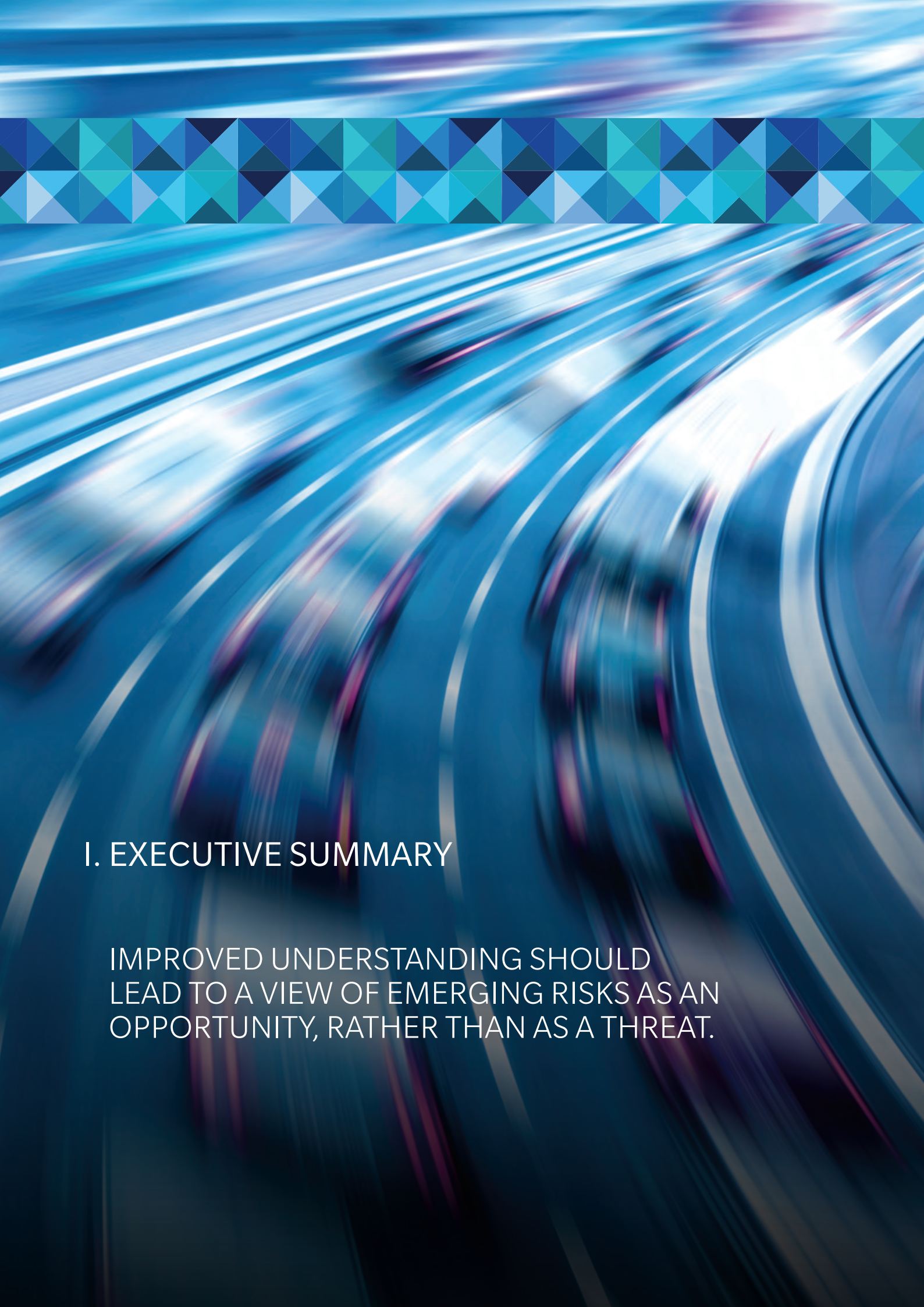


EMERGING RISKS
REPORT
SEPTEMBER 2014

MARSH & McLENNAN COMPANIES

GUY CARPENTER

TABLE OF CONTENTS



I. EXECUTIVE SUMMARY

IMPROVED UNDERSTANDING SHOULD LEAD TO A VIEW OF EMERGING RISKS AS AN OPPORTUNITY, RATHER THAN AS A THREAT.

(Re)insurers today face a degree of change and uncertainty that appears to be evolving at an ever quickening pace.

Emerging risks can be new and unforeseen risks whose potential for harm or loss is not fully known. In looking at the universe of emerging risks it becomes increasingly clear that a significant portion are by their nature not observable by traditional methods, even though their impact will no doubt at some point be felt. This report's goal is to contribute to a greater understanding of this insurance "dark matter." This improved understanding should lead to a view of emerging risks as an opportunity, rather than as a threat. Ultimately, greater knowledge will mean these are, by definition, no longer emerging risks, any more than aviation risks are now.

This report examines emerging risks in a more analytical way in order to take practical steps to deal with them and create value for the (re)insurance industry. It places emerging risks in three categories: technical, crystalizing and aggravating.

Technological risks are those that are genuinely new, which emerge from new technologies and processes. This category would include genetically modified organisms, nanotechnology, E-cigarettes and driverless cars. This report takes an in depth look at the risks associated with cyber technology as an example of technological risk. *Crystalizing* risks are those that are not new, but whose manifestation and implications are emerging. In this context we are looking as much at emerging losses, as emerging risks. This category would include asbestos in the developing world and aluminium health risks. This report looks in depth at bodily injury compensation schemes as an example of crystalizing risk. *Aggravating* risks are relatively well known, but where their incidence and impact are becoming potentially more aggravated. This category would include climate change, pandemics, megacities and resistance to antibiotics. This report looks at terrorism developments as an example of an aggravating risk.

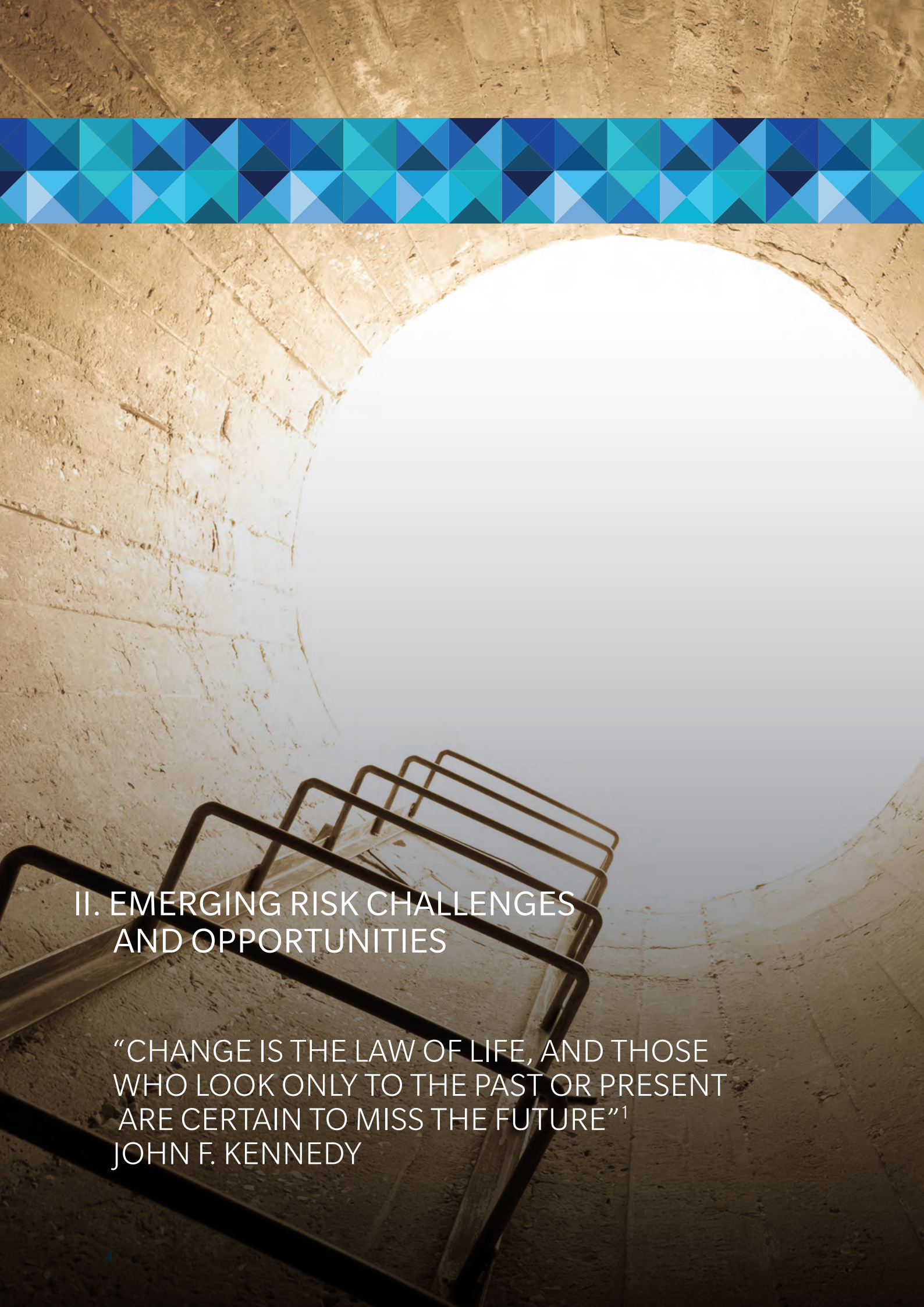
These categories are not water-tight compartments – some, if not all, emerging risks contain elements of all three categories. However, a focus on the predominant characteristic makes it possible to see that each category requires a different response.

Whatever the category of emerging risk the main challenge lies in modeling and quantifying their potential impacts. Only in this way can (re)insurers leverage their key capability, which is the creation of value by risk management.

The challenges are described in the "Modeling" section of this report.

The final section of this report looks at reinsurance responses to the threat of emerging risks and their impact on loss reserving cycles. It is clear that insurers' risk management initiatives need to take note of the trend, identified by the World Economic Forum, "away from technical planning for individual risks and towards holistic planning for a range of unspecified risks."

As a leading integrated solutions provider to the (re)insurance industry, Guy Carpenter offers advice and guidance to clients in these areas by delivering a powerful combination of specialized reinsurance broking expertise, strategic advisory services and industry-leading analytics.



II. EMERGING RISK CHALLENGES AND OPPORTUNITIES

"CHANGE IS THE LAW OF LIFE, AND THOSE WHO LOOK ONLY TO THE PAST OR PRESENT ARE CERTAIN TO MISS THE FUTURE"[1]
JOHN F. KENNEDY

A cursory reading of just a few of the publications on the topic of emerging risks quickly resembles a crash-course in risk aversion therapy. We have been subjected to a bewildering and ever lengthening series of lists of emerging risks. Swiss Re recently identified 26 such risks,[2] Hannover Re has an ongoing list of 14 while the World Economic Forum in its *Global Risks 2014* [3] lists 31 global risks.[4]

According to Swiss Re, emerging risks are "newly developing or changing risks that are difficult to quantify and could have a major impact on society and industry." For Hannover Re they are "new or future risks whose hazard potential is not yet reliably known and whose implications are difficult to access." On the basis of these definitions it would appear that emerging risks are, by their nature, not modelable and hence not susceptible to traditional risk management techniques – this appears to be a distinguishing feature of emerging risks.

The World Economic Forum observes that a key characteristic of global risks is their potential systemic nature. Its definition of systemic risks aligns global risks with emerging risks, given that "systemic risks are characterized by:

- Modest tipping points combining indirectly to produce large failures
- Risk-sharing or contagion, as one loss triggers a chain of others
- "Hysteresis, or systems being unable to recover equilibrium after a shock."[5]

It is plausible that these global risks are similarly unrecognized as emerging risks. The World Economic Forum's intention is to remedy the lack of understanding of global risks:

"To manage global risks effectively and build resilience to their impacts, better efforts are needed to understand, measure and foresee the evolution of interdependencies between risks, supplementing traditional risk-management tools with new concepts designed for uncertain environments."[6]

In broad terms the premise is that global risks, emerging risks and systemic risks are more or less synonymous.

Armed with this insight one can start to examine emerging risks (as we shall now call them) in a more analytical way. This sets up a progression from confronting lists of nightmare scenarios to taking practical steps to deal with them thereby creating value for the (re)insurance industry.

THE CATEGORIES OF EMERGING RISK

For purposes of this analysis we have developed three categories of emerging risk:

- Technological
- Crystalizing
- Aggravating

Technological

Technological change has always presented a challenge, but when addressed correctly it has also presented an opportunity – think of satellites and offshore rigs. The response here is to develop technological competence and construct policy forms that are fit-for-purpose, rather than an untidy amalgam of outmoded and inappropriate wordings. Above all there is a need to build credible models of potentially accumulating incidents so that risk appetites can be aligned with the exposures being faced. Ultimately, greater knowledge will mean these are, by definition, no longer emerging risks, any more than aviation risks.

1. Speech, Frankfurt, West Germany, June 25, 1963., 2. Swiss Re SONAR, New Emerging Risk Insights, July 2014., 3. World Economic Forum, Global Risks 2014., 4. For a complete list of the 31 global risks surveyed by the World Economic Forum's Global Risks 2014 report, to which Marsh & McLennan Companies was a contributor, see Appendix in Section IX of this report., 5. World Economic Forum, Global Risks 2014, Page 12., 6. World Economic Forum, Global Risks 2014, Page 9.

Crystalizing

Crystalizing risks, by contrast, will by their nature always operate to a large extent outside the bounds of current knowledge. The only response is therefore to establish business practices that aim to detect "weak signals" and monitor them in case they become "clear tendencies with a high potential for danger."[7] Most reinsurers have groups of experts who have been assigned to the task of building early-warning systems that identify lead-indicators.

Once such indicators are identified it is important that their financial implications are recognized promptly and correctly. In this respect a key task of regulators is to enforce a prudent risk management methodology that preserves a sustainable and level playing-field for responsible competition. Failure to address crystalizing risks should not provide competitive advantage. On the other hand regulators need to ensure that structural inflexibility does not in fact create further instability.

Aggravating

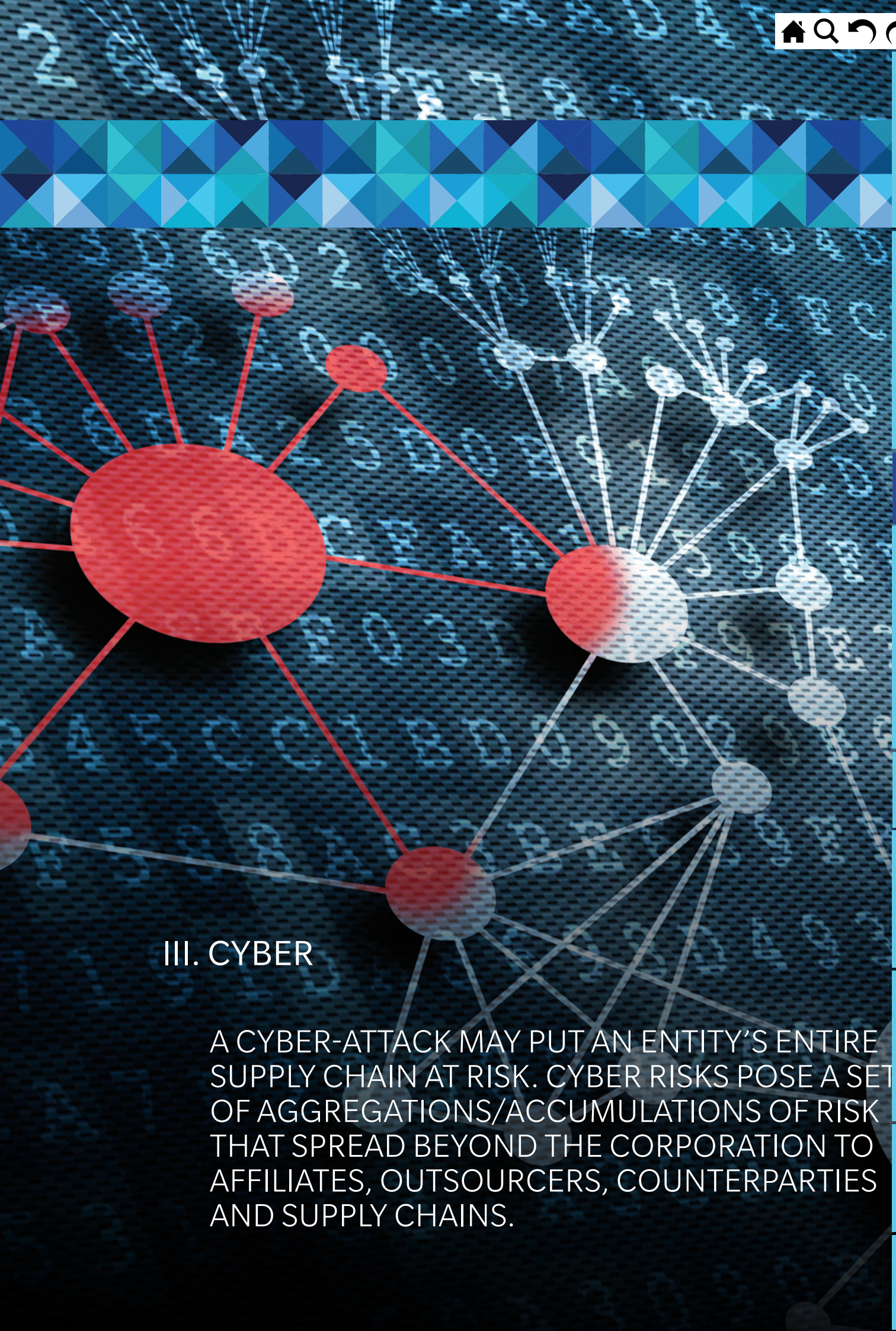
Aggravating risks are by their nature fairly well understood. The difficulty arises from misestimating their scope and extent. The response is very similar to that for technological change in terms of building expertise and knowledge. However, globalization gives these risks a dimension that makes them very difficult to quantify. Emerging risks do not observe boundaries, territorial or otherwise.

In fact the World Economic Forum makes the point that globalization creates systemic risk. This point is made strikingly clear by John Gray in *Al Qaeda and What it Means to be Modern*,[8] which argues that modern-day terrorism can only be properly understood within the context of the benefits of globalization and the internet. These benefits have actually enabled asymmetric warfare.

Whatever the category of emerging risk the main challenge lies in modeling and quantifying their potential impacts. Only in this way can insurers leverage their key capability, which is the creation of value by risk management. The challenges are described in the report section on modeling. In this connection it is worthwhile once again to quote from the World Economic Forum. "Systemic risks include elements that cannot be easily quantified using traditional tools and formulas from probability theory and mathematics, or made to fit the classical distinction between risk and uncertainty".[9]

Following the "Modeling" Section this report looks at reinsurance responses to the threat of emerging risks and their impact on loss reserving cycles. It is clear that insurers' risk management initiatives need to take note of the trend, identified by the World Economic Forum, "away from technical planning for individual risks and towards holistic planning for a range of unspecified risks."[10]

7. Dr. Andreas Tacke, Hannover Re, Hannover Re on Emerging Risks, February 2013., 8. John Gray, Al Qaeda and What it Means to be Modern, Faber, 2003., 9. World Economic Forum, Global Risks 2014, Page 27., 10. World Economic Forum, Global Risks 2014, Page 42.



III. CYBER

A CYBER-ATTACK MAY PUT AN ENTITY'S ENTIRE SUPPLY CHAIN AT RISK. CYBER RISKS POSE A SET OF AGGREGATIONS/ACCUMULATIONS OF RISK THAT SPREAD BEYOND THE CORPORATION TO AFFILIATES, OUTSOURCERS, COUNTERPARTIES AND SUPPLY CHAINS.

The development of information technology and online connectivity has changed the way businesses operate. "Big data" and intricate information technology systems are vital to today's economy. As such, we look at risk associated with cyber technology as an example of the realm of emerging "technology risk."

Guy Carpenter provided an overview of cyber risk in the 2013 report, *Tomorrow Never Knows; Emerging Risks*.[11] This chapter expands on that report.

Cyber-attacks of all varieties are now top of mind for governments, utilities, individuals, medical and academic institutions and companies of all sizes. Because of increasing global interconnectedness and explosive use of mobile devices and social media, the risk of cyber-attacks and data breaches have increased exponentially. Hackers can shut down a company's network or steal customer and employee personal and financial information.

With the high-profile cyber incident involving credit card and debit card breaches at Target Corporation and other US retailers, 2013 became known as the "Year of the Mega-Breach," according to the Organization of American States.[12]

"In 2014, cyber issues are becoming more of a concern for companies that once felt they had relatively little exposure," according to the recent Marsh report, *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*.[13] In fact, cyber-attacks were ranked fifth among the top five global risks in terms of likelihood in this year's World Economic Forum's annual *Global Risks 2014* [14] report.

Cyber-attacks are now seen as one of the most serious economic and national security challenges now facing governments around the world.

Some of the risks that entities face in this realm include:

- Legal liability
- Computer security breaches
- Privacy breaches
- Cyber theft
- Cyber espionage and cyber spying
- Cyber extortion
- Cyber terrorism
- Loss of revenue
- Recovery of costs
- Reputational damage
- Business continuity/supply chain disruptions
- Cyber threats to infrastructure

11. Guy Carpenter, Tomorrow Never Knows; Emerging Risks Report, 2013, 12. Organization of American States and Symantec, Latin American + Caribbean Cyber Security Trends, June 2014., 13. Marsh, Benchmarking Trends: Interest in Cyber Insurance Continues to Climb., 14. World Economic Forum, Global Risks 2014, Page 17.

COSTS OF CYBER-ATTACKS

A cyber-attack can burden companies with substantial costs. For instance, a cyber-incident may result in a business interruption loss as systems are unavailable both internally and externally. Exceptional expenses are incurred and revenues reduced through the loss of business.

The amounts involved depend on the time it takes to restore the affected systems or conduct criminal probes.

There are other resultant costs including expenses for measures taken to notify customers, recover systems and data or ameliorate reputational damage. However, third-party losses can be exceedingly costly as well. Companies may face class action lawsuits and have to pay damages to customers in data breach cases. The costs of defending the results of a cyber-attack can include lawyers' fees for defending cases in court, keeping cases out of the courts and costs for legal analyses of the situation and recommendations on how to proceed.

High-profile data breaches and other cyber security incidents have grown more commonplace with increasingly onerous outcomes. As previously mentioned, one of the largest retailers in the United States, Target Corporation, suffered a massive cyber breach in late 2013. According to Target's 10-Q filing for the quarter ending May 3, 2014, an "intruder accessed and stole payment card data from approximately 40 million credit and debit card accounts of guests who shopped at [its] US stores between November 27 and December 17, 2013 through malware installed on [its] point-of-sale system in [Target's] US stores. In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals." The resulting publicity from the event cost the company a significant amount in lost sales, loss of reputation, class action lawsuits and the ouster of its chief executive officer.

Since the data breach, Target has incurred USD88 million of cumulative expenses, partially offset by expected insurance recoveries of USD52 million, for net cumulative expenses of USD35 million, according to the 10-Q filing for the quarter ending May 3, 2014. To limit its exposure to losses relating to data breach and other claims, the retailer states that it maintains USD100 million of network-security insurance coverage, above a USD10 million deductible. This coverage and certain other customary business-insurance coverage cut Target's exposure related to the data breach, the company explained in its filing.

Another high profile incident involved the UK charity, British Pregnancy Advisory Services. It was fined GBP200,000 in February 2014 following a data breach by a hacker who targeted its website because he disagreed with abortion. He threatened to publish the stolen data.

Impact on Supply Chains

Today, organizations, through their interconnectedness and participation in global supply chains, are subject to an increasingly complex network of networks. A cyber-attack may put an entity's entire supply chain at risk. Cyber risks pose a set of aggregations/accumulations of risk that spread beyond the corporation to affiliates, outsourcers, counterparties and supply chains.

Cloud-based computing is another cyber risk causing concern. Aggregation of data from many companies in a cloud service could spell catastrophic loss for many companies if an attack or breach occurred. Whether it is a private cloud using dedicated servers or a public cloud, where data is stored on shared servers, cyber threats exist.

CYBER INSURANCE

Cyber insurance has grown out of recognition that cyber-crime and data privacy are among the most concerning risks facing organizations today. With the increasing severity and frequency of cyber-attacks and data breaches worldwide, the demand for cyber-specific insurance is growing. Cyber-related risk to critical infrastructure and the overlap with cyber-terrorism are also issues that have come to the forefront.

"Cyber" is perhaps a misleading term to describe the type of cover offered by this product. The term generally describes a number of different modules that provide cover around an organization's computer system, data and other multimedia activities. These covers are normally designed to include the following in some form or another:

Data privacy

- Third party liability
- Liability from disclosure of confidential commercial and/or personal information (privacy)
- Liability from economic harm suffered by others from a failure of network security

Regulation breaches, fines, and penalties

- Defense of regulatory action due to breach of privacy regulation
- Coverage for fines and penalties due to breach of privacy regulation

Network business interruption

- Income loss and expenses incurred during the period of interruption following a computer system failure or breach of network security
- Extensions can cover business interruption caused by the outage of a service provider, when caused by a computer failure or network security

First party loss – data damage and cyber extortion

- Destruction, corruption or theft of electronic information assets and/or data due to failure of the computer system or network
- Threats or extortion relating to release of confidential information or breach of computer security

Crisis management and identity theft response

- A number of costs associated with managing the aftermath of a privacy breach including, but not limited to: forensic investigation, legal costs, notification costs, call center costs, credit monitoring costs (where identification is stolen and a line of credit is obtained) and public relations costs

F 1 | HISTORICAL DEVELOPMENT OF CYBER (RE)INSURANCE
How Has This Product Evolved Over Time?

Evolution of the US Product

1996
- Cyber Insurance first emerged as a product.

2003
- Privacy breach notice laws enacted in California, furthering demand for Cyber products.

2000s
- Following California's example, 47 of the 50 states have now enacted compulsory breach notification legislation, driving the Cyber market in the US.

2006
- Cyber becomes privacy.

2014
- Cyber is underwritten by over 60 insurers and produces over USD1billion a year in premium income.

Evolution of the European Product

1995
- Data Protection Directive in the EU.
- Established data protection as a right for EU citizens.

Mid 2000s
- Increased reliance on IT and high-profile hacking scandals lead to increase in enquiries for cyber insurance in Europe.

2012
- Reform of Data Protection Legislation released by the EU. These detailed compulsory breach notification rules increase fines to be enforced and other require-ments for data protection.

2013
- EU announced the Cyber Security Directive, which will impose minimum security measures on businesses.

2013/14
- Insurers develop international offerings. 25-30 markets in London.

2015
- Expected implementation of the Reform of Data Protection Legislation. (However, this date is a moving target).

Source: Guy Carpenter

However, companies are uncertain of how much coverage to acquire and whether their current policies provide them with protection. One of the roots of the uncertainty stems from the difficulty in quantifying potential losses because of the dearth of historical data for actuaries and underwriters to model cyber-related losses. Furthermore, traditional general liability policies do not always cover cyber risk. In the United States, ISO's revisions to its general liability policy form consist primarily of a mandatory exclusion of coverage for personal and advertising injury claims arising from the access or disclosure of confidential information.

Marsh estimates the US cyber insurance market was worth USD1 billion in gross written premiums in 2013 and could reach as much as USD2 billion this year. The European market is currently a fraction of that, at around USD150 million. Estimates see the European market reaching a size of EUR700 million to EUR 900 million by 2018. The European cyber coverage market could get a big boost from draft European Union (EU) data protection rules in the works that would force companies to disclose breaches of customer data to them.

Though still very much in its infancy, the market's potential is vast with cyber-crime costing the global economy about USD445 billion every year, according to an estimate published in June 2014 from the Washington-based Center for Strategic and International Studies.[15] While many companies have in the past counted on their general commercial liability policies for coverage, they are increasingly taking out standalone contracts.

15. Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II, June 2014, Page 6.

Interest in cyber insurance continues to increase, according to the recent Marsh benchmarking trends report on cyber insurance. The report found that the number of the firm's clients who sought to purchase this type of coverage increased by 21 percent from 2012 to 2013. Media reports of serious data breaches have undoubtedly prompted more companies to buy cyber coverage of USD100 million or more compared to the prior year.

Since traditional insurance products often do not cover damages resulting from an incident like a computer breach, specific cyber liability insurance may be necessary. Carriers have been adapting their policies to include a variety of loss prevention and risk mitigation tools, ranging from turnkey breach response teams to pre-emptive risk analytics.

Insurance Coverage: Limits

Average limits purchased by companies with revenues exceeding USD1 billion rose 10 percent in 2013 to USD28.2 million from USD25.7 million in 2012. For companies of this size, financial institutions purchased the highest average limits at USD53.2 million, which represented a 9 percent increase from 2012. These average limits do not reflect the limits purchased by companies that blend cyber with the limits they purchase for errors and omissions (E&O) or bond. Since December 2013, there has been a stronger desire to obtain much higher limits than those purchased earlier in 2013. That trend is expected to continue.

The average limits purchased for cyber risk rose to USD11.5 million for all industries and all company sizes in 2013, representing a slight increase over the average of USD11.3 million in 2012.

Across major cyber risk-impacted industries, the communications, media and technology sectors continued to purchase the highest limits, with USD23.9 million in 2013. That represented an increase from USD21.7 million in 2012.

During 2013, cyber liability renewal rates — as measured by average and median annual changes in the year-over-year price per million of limits — remained generally stable for both primary layers and total programs. Average increases were typically small, ranging between 2 percent and 3 percent compared to pricing in the prior year.

Regional Variations in Cover

United States

- There is no all-encompassing federal legislation regulating data protection and individual privacy.
- Each state has different laws. Federal laws are enacted on a sectoral approach. Legislation exists for certain industries but each industry's legislation is different. The complexity of legislation combined with mandatory breach notice laws introduces opportunities for class action as well as punitive actions by regulatory bodies, state Attorney Generals and the Federal Trade Commission (FTC).
- Last year, the US Securities and Exchange Commission (SEC), which oversees publicly-traded companies, adopted a directive requiring certain regulated financial institutions and creditors to adopt and implement identity theft programs in light of the new cyber threats.
- In the United States, **data privacy** is the focus of cyber.

Europe

- In Europe, data is viewed as human right and the "right to be forgotten" has ensured that comprehensive regulation exists to protect the individual's data and privacy.
- The collection and purpose of data is subject to strict conditions but with limited (EUR600,000) monetary sanctions, no compulsory notification of data subjects and no tradition of class action.
- For European organizations, the **business interruption** element **(first party)** is of at least equal importance as the cyber coverage.

The EU is looking to update its data protection regulation in the coming year. The exact wording of the regulation is yet to be finalized, but it is expected to come into place in 2015, with a two year implementation period. This is the EU Data Protection Reform.

The new regulation will harmonize European law and introduce new measures including notifications of data breaches and removing data of individuals who withdraw consent for them to be held. Fines and penalties for non-compliance are expected to increase.

Furthermore, in February 2013, the Commission proposed the Cyber Security Directive. This contains measures that would impose minimum security requirements on business in terms of network and information security.

CRITICAL INFRASTRUCTURE

The table below shows the sectors identified as critical by both the US government in the recent Presidential Policy Directive 21, and by the European Commission, as stated in the proposal, Directive on European Critical Infrastructure.

T 1 | CYBER-RELATED RISK TO CRITICAL INFRASTRUCTURE

Critical Sectors	
American Government	**European Commission**
Food and Agriculture	Food
Water and Wastewater Systems	Water
Dams	Research Facilities
Healthcare and Public Health	Health
Nuclear Reactors, Materials and Waste	Nuclear Industry
Emergency Services	Space
Information Technology	Information, Communication Technology (ICT)
Energy	Energy
Transportation Systems	Transport
Financial Services	Financial
Chemical	Chemical Industry
Communications	
Defense Industrial Base	
Commercial Facilities	
Critical Manufacturing	
Government Facilities	

(Source: US Presidential Policy Directive 21 (February 12, 2013), "Critical Infrastructure Security and Resilience" and Council Directive 2008/114/EC)

For US critical infrastructure businesses, such as power utilities, telecommunications and water suppliers, the threat of cyber-attack is a growing and persistent concern. The White House recently issued its cybersecurity framework for critical infrastructure, developed by the National Institute of Standards and Technology.

The Bipartisan Policy Center, in its February 2014 report entitled *Cybersecurity* and the *North American Electric Grid: New Policy Approaches to Address an Evolving Threat*,[16] stated that the federal government should set up backstop cybersecurity insurance through legislation modeled after the Terrorism Risk Insurance Act (TRIA). Utilities in the United States are expected to spend more than USD7 billion on cybersecurity by 2020,[17] the report said.

So-called "smart grid" technologies may make utilities more vulnerable to hackers and other types of cyber-attacks. For instance, the number of installed smart meters that connect customers to their utilities through the web is expected to rise to 1.1 billion in the year 2022 from 313 million in 2013, according to a report from Navigant Research.[18]

Cyber insurance coverage for utilities is limited and often expensive, the Bipartisan Policy Center report stated. "Another question for power sector entities and other operators of critical infrastructure is how the insurance market can address large-scale events with both cyber and physical components." [19]

DIRECTORS & OFFICERS (D&O) LIABILITY

Cyber coverage is also having an effect on D&O liability in the United States. Oversight and increased requirements for disclosure on cybersecurity are making D&O coverage more important than ever. With the rise of data breaches and other cyber-attacks, directors and officers are responsible for making sure that they are taking sufficient steps to protect their company's digital assets. In the case of a data breach, directors can be hit with shareholder suits and shareholder derivative actions claiming that the directors breached their fiduciary duty to the company for failing to put adequate cyber security measures in place.

Legal experts predict that there will be more cyber-related D&O lawsuits resulting from increased regulatory oversight. In October 2011, the SEC issued a disclosure guidance stating that previous disclosure requirements "may impose an obligation" on publicly traded companies "to disclose such risks and incidents." The SEC noted that companies should "review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." The SEC went on to state in the guidance that the company "may need to discuss the occurrence of the specific attacks and its known and potential costs and other consequences." Among those costs would be reduced revenues, an increase in expense for cybersecurity protection, litigation or the effects of theft of material intellectual property. A company should disclose any substantial costs incurred to prevent cyber incidents as well, the SEC guidance stated.

In addition, the FTC issued a regulation requiring many companies to adopt an identity theft protection program. Known as the "Red Flags Rule," it requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent such incidents and mitigate the damage. The FTC rule requires that a company's board of directors create reasonable policies and procedures to detect the red flags of identity theft that may occur in day-to-day operations. The rule states that a company's board — or an appropriate committee of the board or someone in senior management — must approve the initial plan and then oversee, develop, implement and administer the program.

16. Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, February 2014, Pages 10 and 41., 17. Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, February 2014, Page 61., 18. Navigant Research, The Installed Base of Smart Meters Will Surpass 1 Billion by 2022, November 11, 2013., 19. Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, February 2014, Page 40.

Cyber insurance products are being broadened to include coverage that now addresses nearly all aspects of technology-based risk faced by today's companies. Carriers are now adapting their policies to include a variety of loss prevention and risk mitigation tools, ranging from turnkey breach response teams to pre-emptive risk analytics. Opportunities for innovation exist within the cyber coverage market.

Insurers willing to offer more cyber capacity need to be aware of issues such as insured use of outsourced providers, definitions of computer systems, aggregations, first party breach response capabilities and business interruption event triggers, in their product development.

Cyber risks will continue to evolve with each new technological advance and cyber liability policies will in turn be adapted to meet the specific needs of the policyholder. Since companies everywhere, in all industries, from multinational giants to small operations are now exposed to cyber risk, the demand for comprehensive cyber risk insurance coverage will only continue to grow.

IV. EMERGING COMPENSATION STRUCTURES

Compensation for provision of long-term care for bodily injury is becoming an increasingly challenging problem for society in general and insurers in particular.

Due to the confluence of a number of global systemic factors that characterize "emerging risks," traditional responses need to be replaced by a more collaborative and imaginative approach. Uncertainties that had previously been transferred to the claimant are now retained by the insurer in many regions.

"LUMP SUM" COMPENSATION

In many countries bodily injury typically involves providing a "lump sum" compensation package to the claimant. The calculation of this "lump sum" is determined by estimations of the following factors:

- Annual cost of care
- Life expectancy, given the nature of the injury
- Inflation on the annual cost of care
- Investment yield

The annual cost of care is relatively straightforward to estimate. Advances in medical technology have had two major effects: First, a greater rate of survival from injuries that previously would have proved fatal, simply causing more people to need long-term care, and second, a significant increase in the cost of such care, in some cases as much as USD500,000 per year for a single claimant.

Life expectancy for impaired lives is a complex subject, not helped by the relatively limited data base. Generally the reductions from normal life expectancy have been weighted in favor of the claimant. However, one point is certain: for any particular claimant, the chosen life expectancy will most likely turn out to be incorrect.

The relationship between inflation on annual cost of care and investment yield is critical. In many cases the working assumption has been that they effectively cancel-out. Recent experience in the United Kingdom, however, suggests that inflation for medical care costs (as shown by the Annual Survey of Hours and Earnings (ASHE),[20] which measures earnings of healthcare workers), differs from general wage inflation, as well as the Retail Price Index (RPI).

The "cancelling-out" assumption implies a real discount rate (RDR) of 0 percent, however some observers suggest an RDR of -1 percent to -1.5 percent relative to RPI, and as much as -3 percent relative to the current yield curve. There are therefore substantial uncertainties involved in the estimation of "lump sum" packages, given the prospect of an 80 year "tail" and annual costs of up to USD500,000.

Given these uncertainties the benefits to an insurer paying a "lump-sum" compensation far outweigh the potential downside, namely that the claimant might not reach the assumed life-expectancy. The main point is that the insurer achieves certainty.

20. United Kingdom, Office for National Statistics, Annual Survey of Hours and Earnings.

However, this certainty is only achieved by passing on the uncertainties to the claimant. For a number of reasons public sentiment views this as an unacceptable burden to the claimant, as well as his or her family and the broader social network that supports the claimant, not to mention the state welfare system – the provider of last resort.
This changing perception should be seen in the context of the erosion of traditional social networks while governments are increasingly trying to reduce welfare obligations. Long-term care is effectively being privatized and someone needs to pay for it.

Demographic changes only add to the problem. The systemic risk of improving longevity arguably applies equally to impaired lives as it does to normal lives. Generally the growing preponderance of an aging population, as well as the need to provide care for the associated chronic illness, will also have an effect on healthcare costs. Moreover, there is a systemic risk of a medical breakthrough that extends the life expectancy of a previously impaired category of lives.

Finally, the recent global economic crisis has highlighted the financial risks of taking lump-sum compensation, especially given the low-yield environment for "risk-free" investments that seems likely for at least the medium-term.

COMPENSATION "EMERGING RISKS"

From an "emerging risks" perspective it can be seen that the inadequacies of the "lump sum" method of compensation have been highlighted by a number of systemic factors:

- Advances in medical technology/medical inflation
- Increasing life expectancy
- Government down-sizing/privatization of long-term care
- Compensation culture which requires "risk free" solutions

These systemic factors are being seen globally. They may manifest themselves to varying degrees in different regions but it is likely that they will only become more pressing.

Annuities

For varying social and cultural reasons, annuities have been commonplace in a number of countries in Continental Europe for some time, most notably in Germany and France. However, their impact has been somewhat mitigated by the relatively low level of medical care costs (due to the provision of substantial state-funded care) and the fact that inflation was either discounted or covered by the government, as in the case of France.

These developments make France a good example of an "emerging risk" because the government has recently withdrawn the full extent of its inflation protection. This exposure has now been "privatized" and is the subject of negotiation between French insurers and their reinsurers.

Recent cases in Spain have highlighted the inadequacies of the Baremo system in relation to long-term care compensation and there is an ongoing review into the establishment of some form of annuity compensation structure.

Similar issues are arising in Central Europe, most notably in the Czech Republic where there is already a comprehensive framework for annuity structures. At the moment the monetary amounts at stake are relatively insignificant so recognition of their financial impact has not been fully articulated by insurers or by their reinsurers.

Periodic Payment Orders (PPOs)

For a number of reasons the United Kingdom represents an extreme example of the impact of annuity compensation structures. For severe bodily injury cases it is now highly likely that the claimant will opt for an annuity structure (known as a periodic payment order, or PPO) rather than a lump-sum. These are often indexed accordingly to ASHE. As a consequence, the uncertainties that had previously been transferred to the claimant are now retained by the insurer (and to a certain extent, its reinsurers). Unlike an individual claimant, the insurer needs to articulate these risks in its capital modeling. These risks can be categorized as follows:

- Longevity
- RPI (RDR relative to RPI, given the insurer's investment strategy)
- ASHE ("basis" risk between RPI and ASHE, which is currently unhedgeable)

Keeping in mind that these risks are being generally funded by non-life motor insurers, it becomes readily apparent that PPOs present these insurers with significant challenges. Shareholders who have invested in non-life companies face the prospect of finding themselves owning what are essentially life insurance businesses.

The mismatch between life exposures and a non-life balance sheet is accentuated by regulatory treatment. Accounting practice, such as US Generally Accepted Accounting Principles, which permits discounting of reserves for life business, does not permit this for ostensibly non-life loss reserves. Regulators of non-life companies discourage investment strategies that might mitigate these risks, as would be normal practice for a life insurer, instead, pushing non-life insurers towards low-yield bonds.

Ultimately, regulatory treatment has the effect of apparently creating "new" losses, as in the case of the risk margin, which is prescribed by forthcoming International Financial Reporting Standards (IFRS) guidelines and incorporated within the Solvency II regime. The risk margin is in effect the discounted future cost of capital of funding PPO claims, in addition to the actual compensation paid to the claimant. Holding risk margin results in a market-consistent valuation – the amount a third party would charge the insurer in return for taking over the liability. In some cases, this may have the effect of doubling the economic impact of a PPO on an insurer.

It may be argued that the risk margin is not so much a "new" loss as the articulation of an existing loss that simply has not previously been recognized. Certainly, this would be the implication of the IFRS guidelines on risk margin. For this reason we would characterize PPOs as a "crystalizing" emerging risk, whose dimensions are still uncertain. For insurers the cost of uncertainty is very high. However, the crucial question arises as to the extent to which insurers have correctly recognized this in their financial statements. There is still a "tension" between the life and non-life sectors that underlines the potential shortfall in valuation of PPOs. This "tension" is exhibited by current market pricing of the non-life capitalization RDR of 1.5 percent and the life annuity RDR of -1.5 percent to -2.0 percent. This "tension" would at least be partially resolved by application of the IFRS Risk Margin.

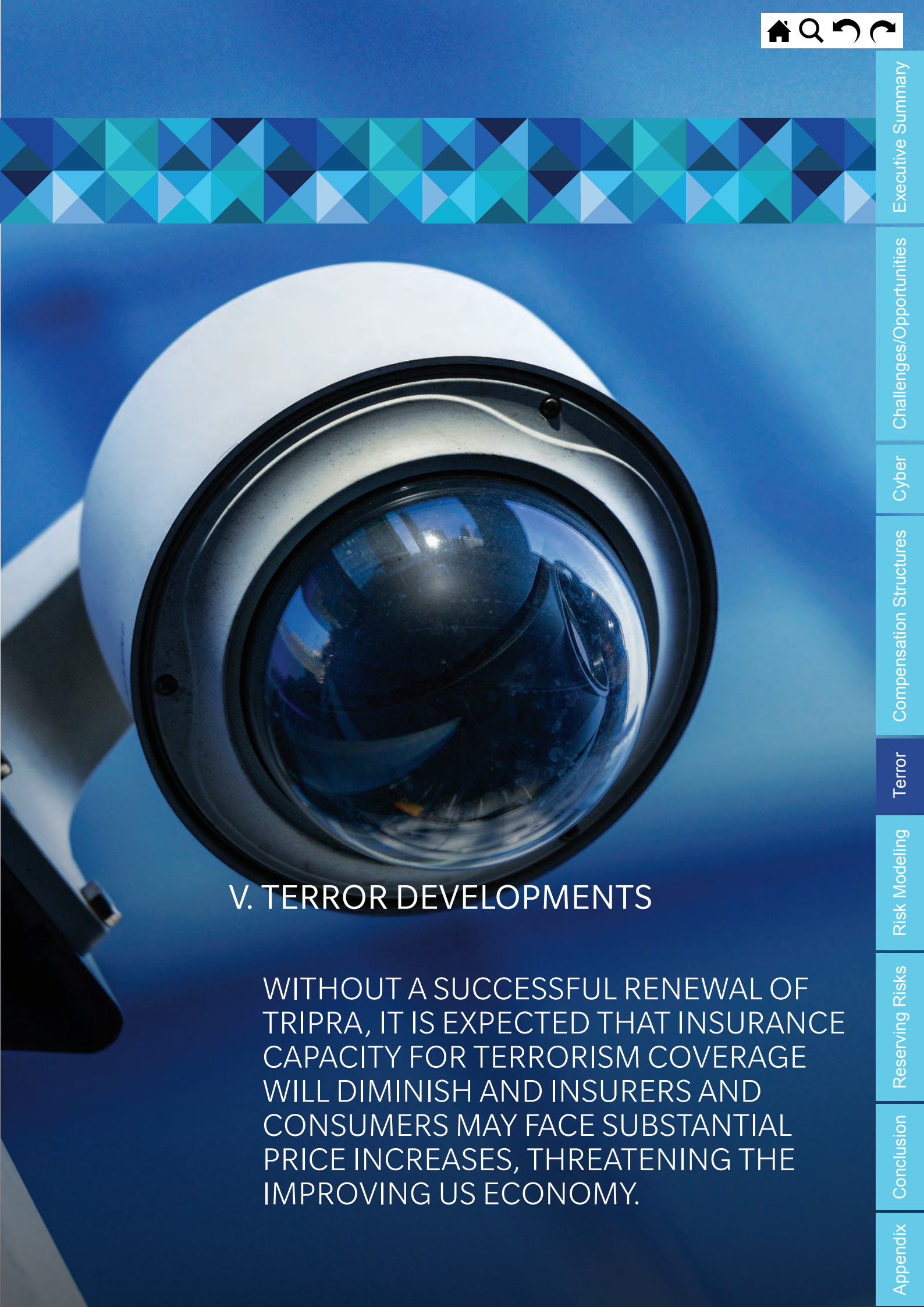
This is a good example of where the risk is defined by the methodology, which is a recurring theme in the realm of "emerging risks." Some feel that this is the fundamental task of regulators: to enforce a prudent risk management methodology that preserves a sustainable and level playing-field for responsible competition.

The PPO example also reveals other recurring themes in "emerging risks." The most notable of these is that "emerging risks" do not respect the boundaries of how the insurance industry has traditionally been organized. The traditional demarcation between life and non-life has in this case proven to be an obstacle to a solution. Rather than exploiting the relative capabilities of their respective balance sheets in order to create value from the PPO problem, the life and non-life sectors have tended to accentuate their own shortcomings. Faced with a problem that crosses traditional boundaries, it is necessary to find a solution that transcends those boundaries and mobilizes risk capital accordingly.

Thinking more broadly, it is worth considering whether a more collaborative approach would actually benefit the claimants themselves – after all, this is the whole point of the endeavor. A more coordinated approach to long-term care might result in tangible benefits to the claimants, as well as having economic benefits for insurers. Going even further, governments might consider issuing debt with instruments that match the duration and indexation of annuity payments.

As the Executive Chairman of the World Economic Forum writes in the preface to Global Risks 2014, "Moving from urgency-driven risk management to more collaborative efforts to strengthen risk resilience would benefit global society."[2] These words could not apply more than to the risk of emerging compensation structures.

 21. World Economic Forum, Global Risks 2014, Page 7.



V. TERROR DEVELOPMENTS

WITHOUT A SUCCESSFUL RENEWAL OF TRIPRA, IT IS EXPECTED THAT INSURANCE CAPACITY FOR TERRORISM COVERAGE WILL DIMINISH AND INSURERS AND CONSUMERS MAY FACE SUBSTANTIAL PRICE INCREASES, THREATENING THE IMPROVING US ECONOMY.

Some may question why terrorism risk has a place in a document dedicated to emerging risk. Terrorism as a form of violence to promote cause or promote change is one of the original human conflicts. The wind blows and the earth shakes much the same way now as it has for hundreds, thousands of years. However, terrorism as a risk and a peril has evolved over the years and is a current concern in all parts of the world. Given the growing population, regional conflicts producing a broad list of potential instigators, the expansive reach of social media for extremists spreading their messages and recruiting and the diversity of possible attack modes to cause human and economic loss, terrorism does qualify as an emerging risk. With this contemporaneity in mind, we will discuss terrorism as an example of an emerging risk that is being aggravated by changes in geo-political events and in the continued notable challenges in modeling its ever changing underlying complexities.

Beyond the risk of terrorism itself, there is uncertainty in the US terrorism market coming from the fact that the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) is scheduled to expire on December 31, 2014 and US lawmakers have not yet authorized a renewal program. Without a successful renewal of TRIPRA, it is expected that insurance capacity for terrorism coverage will diminish and insurers and consumers may face substantial price increases, threatening the improving US economy. The potential of notably higher TRIPRA retentions being imposed on US insurers (or in the extreme case, no federal back-stop) also clearly exacerbates the "crystallization" characteristics of terrorism as "re-emerging" risk for many exposed carriers.

T2 | OVERVIEW OF TRIPRA AND EXTENSION PROPOSALS AS OF JUNE 11, 2014

	Terrorism Risk Insurance Program Reauthorization Act of 2007	Terrorism Risk Insurance Program Reauthorization Act of 2014 (Senate)	TRIA Reform Act 2014 (House)
Termination	December 31, 2014	December 31, 2021	December 31, 2019
Make-Available Provision	Must make coverage available for certified acts of terrorism on same terms and conditions as for other covered risks.	No change.	January 1, 2016 — small insurers (to be defined) can opt-out of the mandatory "make available" requirement.
Covered Acts	Foreign and domestic terrorism in the United States and on specific US interests abroad (such as embassies, missions, consulates, air carriers or flag vessels). Includes an act of war for workers compensation policies only.	No change.	No Change
Certification Level	USD5 million.	No change.	• Remove USD5 million threshold. • January 1, 2015 — the Secretary of Treasury must consult with the Attorney General and the Secretary of Homeland Security (replaces the Secretary of State from previous legislation).
Program Trigger	USD100 million insured loss in a program year.	No change.	• 2015 - USD100 million • 2016 - USD200 million • 2017 - USD300 million • 2018 - USD400 million • 2019 - USD500 million Nuclear, biological, chemical, or radiological (NBCR) certified acts trigger at USD100 million.
Covered Lines	Commercial property/casualty insurance (including excess insurance, workers compensation and directors and officers insurance).	No change.	January 1, 2016 - separate the definition of an "act of terrorism" into two categories: • NBCR acts • Non-NBCR acts.
Insurer Deductible (percent of direct earned premium)	20%	No change.	No change
Federal Reinsurance Quota Share	85%	• 2016 - 84% • 2017 - 83% • 2018 - 82% • 2019 - 81% • 2020 - 80%	For non-NBCR acts of terrorism • 2015 - 85% • 2016 - 84% • 2017 - 83% • 2018 - 82% • 2019 - 80% For NBCR acts of terrorism • 2015 -2019 - 85%
Insurance Industry Retention for Mandatory Recoupment	USD27.5 billion	Increase the Treasury's recoupment rate from 133% to 135.5%. • 2015 - USD29.5 billion • 2016 - USD31.5 billion • 2017 - USD33.5 billion • 2018 - USD35.5 billion • 2019 - USD37.5 billion	• January 1, 2016 - increase the Treasury's recoupment rate from 133% to 150%.
Cap on Liability	USD100 billion.	No change.	No Change
Timing of Certification	Not addressed	Final rule from the Treasury Department no later than 180 days from the enactment that would establish a time line for certifying an event as covered or not covered.	• Preliminary certification by the Secretary of Homeland Security no later than 15 days after an occurrence. • Final certification no later than 90 days after an occurrence.

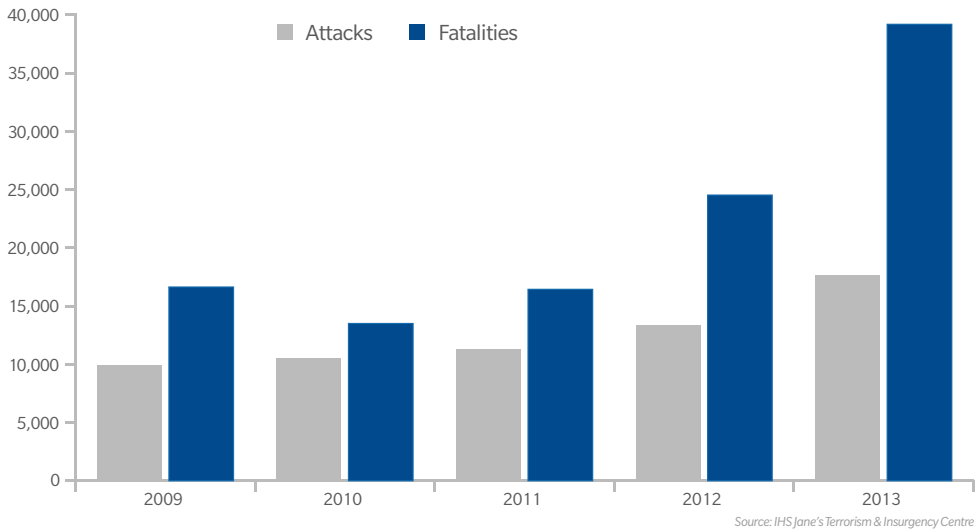
Source: Marsh, Guy Carpenter

During the second quarter of 2014 US Congressional activity involved two proposals being raised by legislative sub-committees. The full senate passed their committee's recommended version 93-4 on July 17, 2014. The House of Representatives has yet to vote on their version and as of press time there is not a scheduled vote.

In the Guy Carpenter Global Terrorism Report *Uncertain Future: Evolving Terrorism Risk*[22] we provide a comprehensive review and outlook of terrorism risk. Key components of the report are highlighted below.

The threat from terrorism has undergone significant change since the attacks of September 11, 2001. Heightened and more effective counter-terrorism activities in the following years have prevented repeat attacks on the scale of those carried out in New York and Washington D.C. Nevertheless, al-Qaeda and its affiliates, along with individuals inspired by the movement, still pose a significant threat to Western interests around the world as events of the last 18 months have shown.

F2 | GLOBAL TERRORIST ATTACKS – 2009 TO 2013



Source: IHS Jane's Terrorism & Insurgency Centre

Islamic militants have shifted to softer targets with attacks and plots becoming more localized as senior al-Qaeda leaders have increasingly called on individuals to execute unsophisticated attacks in their home countries and regions. An increased focus on inflicting civilian casualties and the targeting of "un-Islamic" assets, such as government buildings and personnel and nightclubs has resulted. This trend has been reflected in developments over the last 18 months as individuals and cells inspired by al-Qaeda carried out relatively low capability but high profile attacks in several cities around the world. A number of other unsuccessful attacks perpetrated by lone attackers have also taken place.

The volatile landscapes in Syria, Ukraine, Iraq and other Middle Eastern and North African countries raises important questions about the future of the international terrorist threat. United States and European policy and activities in these landscapes may further motivate militants to launch additional attacks and target Western interests.

Cyber terrorism and cyber security, discussed earlier in this report, are emerging risks that have the potential to threaten countries' national security. Critical infrastructure, including nuclear plants and other industrial facilities, is increasingly being targeted by cyber hackers intent on causing damage, disruption and potential loss of life. Nevertheless, terrorist groups such as al-Qaeda are currently seen as lacking the necessary sophistication and capability in this area to successfully disrupt a major facility. For insurers with terrorism-related risks on their books, it will be important to understand the threat and how it is evolving, the varying risk in different regions and which developments and risks are likely to emerge in the remainder of 2014 and beyond.

22. *Guy Carpenter, Uncertain Future: Evolving Terrorism Risk, Global Terrorism Report, June 2014.*

MODELING TERRORISM

Modeling methodologies for terrorism have been continually refined and updated since the three major modeling companies – AIR Worldwide (AIR), EQECAT and Risk Management Solutions (RMS) – released their first terrorism models in 2002. Quantifying the economic, insured and human losses from a terrorist attack continues to pose major challenges for (re)insurers and alternative capacity providers. There are three main techniques to model terrorism risk:

Probabilistic modeling estimates losses based on a large number of events. A key factor is the estimated frequency being attached to all the events that could occur. Due to the difficulty in predicting the probability of terror events, there is considerable uncertainty associated with probabilistic terrorism modeling.

Exposure concentration analysis identifies and quantifies concentrations of exposures around potential terrorist targets. Target-based accumulation assessments utilize predetermined targets (typically with high economic, human and/or symbolic value) and aggregate an insurer's exposures in and around various distances from these targets.

Deterministic modeling represents a compromise between the lack of accuracy in accumulation analysis and the uncertainty surrounding probabilistic models. By imposing an actual event's damage "footprint" at a specified target, a specific, yet hypothetical, scenario can be analyzed with some certainty. Major modeling firms offer an array of deterministic-analysis tools for conventional and nuclear, biological, chemical and radiological attacks at defined target and non-target locations.

Compared to natural hazards such as hurricanes and earthquakes, terrorism modeling continues to be faced by unique challenges due to its lack of acceptance by rating agencies and some markets. Insurers, reinsurers and modeling companies are constantly refining their models and the assumptions that underlie their products, thereby increasing their ability to manage terrorism risk in an educated and more quantitative fashion. Currently, deterministic, scenario-based testing is the most common tool used by (re)insurers to assess their vulnerability to terrorism.

Commercial Models

The catastrophe modeling companies have regularly updated their terrorism models over the years to reflect the changing threat landscape and help (re)insurers and other market participants perform robust terrorism risk assessments. Such updated products from RMS and AIR include:

RMS Probabilistic Terrorism Model (PTM) Exceedance Probability (EP) Analysis: EP results and deterministic losses for certain weapon/target combinations.

RMS RiskLink Deterministic Analysis: Identifies accumulations around designated RMS terror targets as well as portfolio-specific hot spots used to respond to the A.M. Best Supplemental Rating Questionnaire.

AIR CLASIC/2 Terrorism Analysis: EP results and deterministic losses for certain weapon/target combinations. Accumulation analysis is available on a consulting basis.

AIR Touchstone Terrorism Analysis: Next generation version of AIR platform incorporating terrorism-related features of CLASIC/2 along with interface usability and analysis efficiency enhancements.

AIR US Terrorism Model

AIR implemented significant model updates in version 13 of CLASIC/2™, released in 2011. The updates impacted hazard components such as the target and landmark database, event frequency estimates and exposure and policy conditions.

AIR's target and landmark database now includes approximately 300,000 landmarks and 100 high-risk trophy targets across the United States. Several hundred new structures were added to the database to account for newly prominent and constructed landmarks.

AIR also updated its frequency estimations in the release of version 13, using intelligence analytics and the AIR expert group threat assessment. The result was a significant fall in the number of likely events per year, causing a reduction in the average annual loss (AAL) of approximately 70 percent for property and workers compensation. Additionally, AIR released software updates in version 13 that added flexibility in choosing analysis options. Examples included terror event fire loss covered under the standard fire policy as well as exclusions such as pollution and bacteria and virus resulting from NBCR.

In 2012, AIR released version 14 of CATRADER® and CLASIC/2™. Although no changes were made to the terrorism model in this update, standard yearly workers compensation benefit level updates were released to reflect updated legislation and cost estimates for injury payments. In 2013, AIR released its next generation modeling platform, Touchstone™ and also updated CLASIC/2 version 14 to version 15. There was no change in the terrorism model on either platform.

RMS Global Probalistic Terrorism Model

RMS released an updated PTM in July 2012, version 3.1.2. The new model revised the annual frequency of a terrorist attack on US soil. No updates were made to geographies outside the United States.

RMS used a panel of terrorism experts and closely tracked data from the past ten years on terrorist arrests and indications of planned and thwarted attacks. The result of this research was a reduction in the annual number of planned macro attacks in the United States from four to three, implying a 19 percent reduction in average frequency and a 19 percent reduction in the AAL. The reduction in frequency was the only change made to the model. The impact on the AAL was therefore the same across all books of business, but could vary by return period.

In August 2012, RMS reported that the overall macro attack frequency rate was reduced from 0.61 to 0.49 for the standard risk outlook for 2013, resulting in a change in the average number of macro attack plots annually. The interdiction rate and the suppression factor remained unchanged.

The reduced risk outlook was also updated, resulting in the average number of plots decreasing from three to two and the average frequency decreasing from 0.49 to 0.36. The increased risk outlook also decreased from an average of five attempted plots to 3.5, giving an average frequency of 0.55.

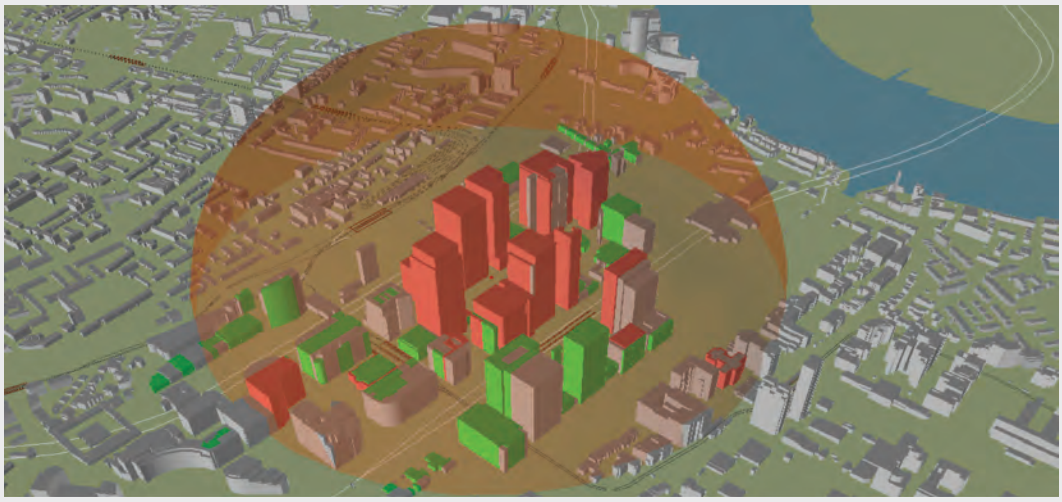
RMS updated its US workers compensation cost severities in October 2014 to reflect the latest legislation and cost estimates for injury payments.

GUY CARPENTER SOLUTIONS

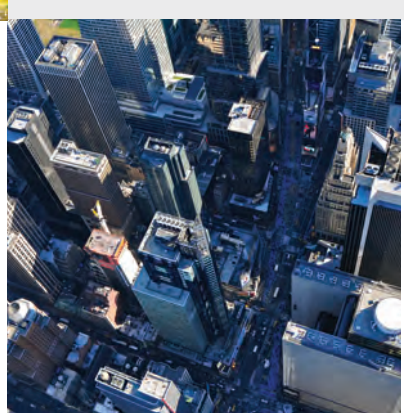
3-D Terrorism Modeling

Guy Carpenter has enhanced terrorism modeling capabilities to take into account the 3-D nature of structures in the vicinity of a target. The method considers the dampening effect on the hazard by shielding objects before it contacts a risk. Our method identifies a more realistic estimate of the risks affected by an event.

3D MODELING SAMPLE



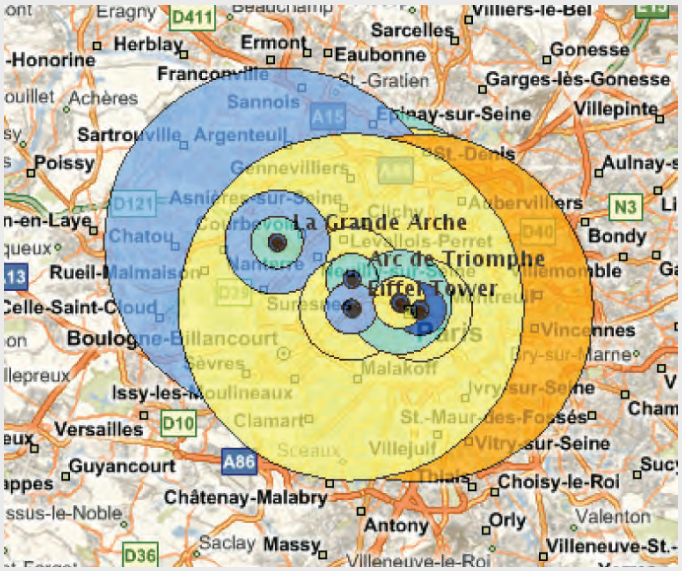
Source: Guy Carpenter



i-aXs

In addition to our 3-D modeling capabilities, Guy Carpenter offers a number of other tools to help clients manage their terrorism risks. i-aXs®, our web-based data management platform, allows insurers to quantify their exposure to a potential terrorist attack and highlight concentrated areas in their portfolio. Managing exposure to terrorism loss is an integral function within i-aXs, with several different tools on offer to help insurers assess their largest levels of accumulation.

I-AXS MAP SHOWING EXPOSURE TO TERROR TARGETS IN PARIS



Source: Guy Carpenter i-aXs®

The following global proprietary terrorism exposure reports are available within i-aXs:

- Cluster Accumulation: Clusters of total exposure within grid points spaced at various grid sizes.
- Portfolio Accumulation: Top portfolio accumulations for 1, 0.5, and 0.25 mile radiuses.
- Terror Accumulation: Portfolio terror for all targets by total exposure and zone.
- Terror Target by Zone Accumulation: Terror accumulation for global portfolios using targets from Exclusive Analysis (part of IHS), RMS and Guy Carpenter compiled databases.

Thematically shaded maps and satellite imagery, along with easy-to-understand reports, provide detailed accumulation information within a user-defined geographic range.

i-aXs allows companies to measure parameters such as total insured value, exposed limits, risk count, deductibles and premiums. Users can also drill down to individual policy details within terror accumulations such as construction type or line of business.

GC Risk Profiler assesses new locations and combines them with existing portfolios to determine proximity to terror targets and risks already in a portfolio. The tool also allows an overlay of infrastructure maps such as highways, railways and airports while it geocodes the risk and accesses a satellite image. GC RealCat, meanwhile, evaluates loss potential from the very onset of an event and delivers insight and guidance all the way through the claims management process. Such an event would include a major terrorist attack, such as a large-scale bomb blast impacting a significant geographic area.

VI. CASUALTY CATASTROPHE RISK MODELING

THE "CASUALTY CATASTROPHE" IS PERHAPS THE MOST DAUNTING THREAT THAT CASUALTY (RE) INSURERS FACE TODAY. ONE ROOT CAUSE HAS THE POTENTIAL TO TRIGGER A CHAIN REACTION OF LIABILITY THROUGH A WEB OF TIGHTLY INTERTWINED BUSINESS RELATIONSHIPS THAT IN MANY CASES CAN INVOLVE MULTIPLE LINES OF BUSINESS.

Casualty (or liability based) catastrophes have become increasingly frequent and severe over the past decade, exposing (re)insurers to much more risk than they may have realized and reserved for. One root cause can trigger a chain reaction that can bleed balance sheets and even imperil solvency. Until recently, casualty carriers had little choice but to accept this risk as losses emerged.

The maturation of enterprise risk management (ERM) practice and the development of new niche, open-platform and casualty-specific catastrophe models, though, signal a change. The more complex the casualty risks and regulations carriers face, the more they are recognizing that improving their underwriting and ERM practices could in some cases even yield competitive advantage.

It is becoming possible to model the accumulation of an increasing number of casualty risks, whether technological, crystalizing or aggravating, both knowable and manageable. As casualty catastrophes become more common and more models become accepted, insurers should be able to take informed action to protect and allocate their capital as they have on the property side.

On a relative scale, property catastrophes are utterly familiar and have had the ability to be modeled for over 25 years. The same exposures generally can be found in the same regions with little change from one year to the next. As a result, property (re)insurers have access to a considerable amount of historical exposure and event data, which is evident in the sophistication and utility of the models at their disposal. In fact modeling firms have responded to an increasing demand on property by broadening the scopes of property risks, regions and perils. They are also increasingly opening their models and shifting to open-source platforms as a means of expanding their demand and offering. Part of this increased demand has resulted from the need to accommodate an increasing number of complex and changing risks, perils and countries emanating from the aggregating emerging risk category. Examples of these risks include climate change, the growing complexity of supply chains and megacities. Unfortunately, casualty (re)insurers have not had similar access to models and the data required to run them near this depth. The historical record on casualty and liability risks has been relatively thin and constantly changing. And in some cases the variables almost seem infinite, making it very challenging to identify, model, prioritize, evaluate and integrate a large set and broadening array of scenarios.

The "casualty catastrophe" is perhaps the most daunting threat that casualty (re)insurers face today. One root cause has the potential to trigger a chain reaction of liability through a web of tightly intertwined business relationships that in many cases can involve multiple lines of business.

The proliferation of liability is replicated in casualty (re)insurance portfolios, leading to the possibility of unexpectedly high claims, a drain on capital, and, in the extreme, risk to a firm's solvency. Multiple lines of business insureds and even multiple accident years can be swept up in a casualty catastrophe, and the carriers involved may have to pay claims that may at first seem unrelated to the event's initial trigger.

Casualty catastrophe occurrences have become increasingly common over the past decade. The recent 2008 financial catastrophe is the easiest to cite, due to its sheer size and the fact that it continues to unfold even today. But, there have been many others. The collapse of the "dotcom economy" led to scandals around initial public offering laddering and equity analyst conflicts of interest. Accounting firms were not alone in suffering financial loss related to such debacles as Enron, WorldCom, Tyco and Adelphia. While insured losses did not reach those of property catastrophes, economic damages were profound. Enron's loss of USD66 billion in market capitalization alone — not including the economic damage caused to other companies — was more than double that of Hurricane Ike (approximately USD30 billion). The financial catastrophe is estimated to have caused economic damage of above USD1 trillion, with more likely to follow. When considered in the context of the Deepwater Horizon industrial accident, the casualty catastrophe that unraveled from the largest US offshore energy event over the past 40 years was by no means remote. Beyond the initial property loss of the actual drilling rig, liability risk in paying claims continues to extend and ripple throughout the supply chain involved as well as the environmental impact to numerous coastal and commercial businesses. Asbestos litigation, perhaps the longest casualty catastrophe on record, has paid out over USD70 billion and by some accounts may be entering its third wave. Therefore, asbestos is an emerging crystalizing risk that needs to be continuously monitored, measured and modeled for those who continue to be exposed to it.

Casualty catastrophes, unfortunately, do not follow patterns — unlike property catastrophes.

The geographies, natural conditions and other indicators of hurricanes, earthquakes and other property disasters offer some relative sense of predictability. A hurricane on the Florida coast is not unusual. Casualty catastrophes, however, rarely arise from the same conditions — or whose triggers emanate from the same companies or industries — as their predecessors. In fact, many potential casualty catastrophes (especially those in the broad "technological" emerging risk category) are still considered "black swans," to at least some of the (re)insurers that cover them. Some can appear out of nowhere and wreak havoc quickly.

Just about every large public or private company and its service providers (manufacturers, pharmaceuticals, technology firms, investment banks, law firms, accountants and consultants), strategic partners and supply chain participants are potential flashpoints. The data set is vast, and when casualty catastrophe indicators appear, it may be typically too late to take preventive action. Therefore, casualty writers need to be proactive in regards to these unknowns. As amorphous and complex as these risks may appear, the minimum expectation is that carriers need to proactively and systematically understand these emerging and casualty exposures and be able to measure the directional impacts they will have on their portfolios' exposures and aggregate limits.

Uncertainty is always a factor in insurance risk and capital management decision-making. Targeted, supported assumptions applied to available data using thoroughly researched and carefully designed models are intended to counteract the unknown, at least to the extent possible. Thus, to protect their capital from the casualty catastrophe risk, carriers have needed tools and models that can probe a portfolio to apply potential new and emerging realistic disaster scenarios, identify likely exposures and map how liability would spread from the epicenter to other industries, jurisdictions and lines of business. Not only has the modeling technology been challenging to develop, it tends to be exasperated by the lack of available essential data and the prevailing practice of siloed risk management.

TRACKING INTEGRATED, INTRICATE RISKS

Casualty (re)insurers do not cover standalone risks. A steep drop in stock price, product defect with recall or other event could lead to class action lawsuits and ultimately large claims. This emergent reality, however, is difficult to address. A carrier would need to identify the many possible starting points of a liability chain reaction and follow their rapidly spreading implications throughout a portfolio. Without powerful modeling technology, this process is time-consuming, impossible to complete and likely to miss key threats and underlying exposures.

Because of the impracticality of integrated liability risk management under these conditions, most casualty (re)insurers segment their efforts to protect their capital, for example, by geography or line of business. This approach leaves gaps, some of them quite wide. An anticipated D&O claim for a particular insured may arise from an event that also triggers D&O — and possibly errors and omissions (E&O) — claims for other insureds. The losses begin to mount, often in excess of carrier expectations.

Because of the complexity and uncertainty involved in integrated casualty catastrophe risk management, carriers generally had not advanced their risk management practices in this regard. They instead have managed liability risks independently and assume the integrated risks, sometimes unknowingly. The capital needed to support cover for a specific D&O peril, for example, may not account for ancillary D&O effects from an event elsewhere in the portfolio – not to mention the E&O implications. In the event of a casualty catastrophe, it is not enough to model these scenarios separately and aggregate the results. The whole may be greater than the sum of the parts. Catastrophe risks must be identified, prioritized, accumulated and modeled as entireties in order for their implications to be understood and hedged. Recommended steps include:

1. Locate areas of vulnerability to catastrophe risk in a portfolio
2. Identify casualty catastrophe mechanisms/determine how they operate within a portfolio
3. Stochastically model major disaster scenarios that could trigger substantial casualty losses
4. Formulate a risk management plan to address the full reach of the various scenarios identified

Ultimately, identifying and managing casualty catastrophe risk requires a systematic approach. The various connections within a portfolio must be scoured in order to understand the implications of a particular event. A product recall could lead to product liability, D&O and E&O claims. A plane crash due to equipment malfunction could cause claims for product liability, D&O and life. Likewise, as we have seen with Deepwater Horizon, an industrial accident causing property damage, workers compensation or employers liability losses could lead to general liability, environmental, D&O claims and business interruption – only to morph into further liabilities. The implications of a particular situation can reach far beyond the root cause, even if it stretches the imagination.

THE RISE OF EMERGING RISK AND CASUALTY CATASTROPHE MODELS

The modeling of emerging and casualty catastrophe risks remains challenging and the models continue to vary in their approach, level of development and industry acceptance. With the potential scenarios numerous, diverse and constantly changing, there is no single model or approach that could contemplate all of them. Unlike their fully probabilistic property counterparts, the various perils and scenarios also need to be adapted and structured according to each carrier's specific exposure. Furthermore, the various disaster scenarios with which carriers are being increasingly confronted need to be prioritized and synthesized within their ERM framework. By their very definition, there may be limited data on hand on which to base any modeling. As a result, much of the industry continues to rely on multiple models and actuarial approaches that encompass: model applications, probable maximum loss (PML) estimates, realistic disaster scenarios, experience and exposure ratings to create a broad set of scenarios and deterministic views.

In addition to peril and scenario based commercially available catastrophe models, niche data best practices and models are being developed to meet the demand in varying degrees within the crystallization and aggravating categories. Here, ample data and modeling applications are being synthesized and adapted within existing model frameworks allowing carriers to get their underwriting grip on these scenarios. Examples of these efforts within Guy Carpenter include the various flood models we have developed specifically for Asia and Central Europe. Other applications involve identifying and quantifying emerging "aggregating" exposure concentrations such as those in Asian industrial parks. The losses emanating from the Thailand floods were more about the insureds and the industry taking its eye off of exponential exposure growth and changes in global supply chain dynamics – in lieu of the size of loss and return period dynamics – after they were flooded. Other niche models, such as Guy Carpenter's MetaRisk® Reserve™ can focus on various "crystalizing" emerging threats emanating from the accumulation of systemic reserves over multiple years.

The Oasis Loss Modeling platform, of which Guy Carpenter is a member and supporter, will help facilitate further development of additional niche catastrophe models by allowing independent developers to create and input various hazards, vulnerability and exposure elements. We believe that open-source platforms such as Oasis will lower the barrier of entry for academics and small specialist teams on innovating and developing models that will create more views of overall risk and the ever-increasing number of emerging perils and cat risks. Access to these additional views should prove instrumental to our clients where credible views of particular emerging risks may not currently exist and should be analyzed from a variety of different modeling perspectives.

The mapping and deterministic modeling of emerging risk scenarios has and will continue to play an important role in this area. Lloyd's approach to emerging liability risks in some ways has been no different than what has been required of their syndicates to report on for well-established property risks. Specific realistic disaster scenarios (RDS) are required to quantify and model for specific earthquake, windstorms and even terrorism event footprints through a combination of licensed software (AIR, EQECAT or RMS), internally modeled or via maximum line estimates. With a relative shortage of these options and data available for professional, non-professional as well as multiple public and products-based liability RDS losses, a reliance on simpler market share or premium derived PMLs based on de minimis approaches has been typically required. However, as the level of sophistication and tools for deterministic modeling capabilities here increases, the next question that arises involves the more challenging leap towards a more fully probabilistic and holistic model approach. It is important to note that although probabilistic terrorism models have been available in several countries including the United States for nearly a decade, the A.M. Best rating agency continues to rely on deterministic loss scenario modelings due to what they continue to view as a lack of historical and credible probabilistic based events.

The availability of essential insured-level data on emerging and casualty catastrophe risks remains an important challenge that many carriers continue to work towards improving. Property catastrophe models that were developed during the 1980s contemplate highly granular and sophisticated geo-coded data that is readily available today and get interfaced with very specific and robust building construction and historical event sets. Casualty catastrophe modeling similarly also requires highly granular exposure data related to the particular industry(ies) covered within the portfolio. Models that are beginning to emerge in this area differ according to the data they require, the approach taken as well as the specific scenario set(s) the development is focused on. Some are taking a highly granular data intensive bottom-up approach whereas others may be contemplating a more general top down approach to the exposure data required. Some are loss experience-based and are contemplating an integrated historical event set, yet others are much more exposure-based. The exposure-based models tend to be highly ingrained in generally accepted scientific and mass tort data and operate under the fundamental assumption that past losses and patterns may not necessarily be indicative and directly applicable to future emerging threats. And as a result they tend to focus predominantly on products-based liability scenarios and their latent impact on bodily injury.

GUY CARPENTER'S CASUALTY CAT MODELING APPROACH

Due to the current challenges with casualty exposure data and the numerous assumptions that need to be made to estimate casualty catastrophe losses, Guy Carpenter is developing a model that is as simple, transparent and as data-driven as possible, while still being able to achieve results that are sensitive to the things insurers can do to mitigate their casualty cat risk, such as changes to insured industry concentrations, limits, attachments and reinsurance coverages. Our model is intended to focus initially on a select group of technological, crystalizing and to a lesser extent aggravating risks that are of interest to our clients. It is also intended to be complementary and supplementary to the various other models and approaches being pursued.

Simple and transparent: our model is scenario-based. This provides an intuitive check on results.

Data-driven: To create these scenarios we have relied upon a variety of industry sources including Advisen's® database of 200,000 historical losses.

Version 1 of our model, scheduled to be released later this year, is an essential start in this complex field that will enable clients to:

1) View and analyze unexpected industry portfolio concentrations. It is easy to see where concentrations are in any one industry. However, clients will be able to map how all the industries have been interrelated in past, similar events. These linkages can reveal unexpected concentrations in portfolios.

F 3 | IF ONE INDUSTRY IS TRIGGERED BY AN EVENT, WHAT IS THE PROBABILITY THAT ANOTHER INDUSTRY IS HIT BY THE SAME EVENT?

a) If these industries are hit by an event...

b) ...here are the probabilities that these industries will be hit by the same event:

	Standard Industrial Classification	Chemicals And Allied Products	Business Services	Executive, ..& General Gov'nt...	Electric, Gas, And Sanitary Services	Transportation Equipment
		28	73	29	91	51
Chemicals And Allied Products	28		20%	20%	31%	40%
Business Services	73	10%		10%	23%	30%
Executive, ..& General Gov'nt...	29	19%	20%		31%	20%
Electric, Gas, And Sanitary Services	91	19%	30%	20%		30%
Transportation Equipment	51	19%	30%	10%	23%	

Source: Guy Carpenter

Note: Output is estimated from our database of historical casualty catastrophe losses.
These results are for Sudden & Accidental Disaster events only, and represent only a small subset of our overall output.

2) View and analyze how casualty catastrophe loss estimate changes as the portfolio changes. Instead of focusing on the absolute value of an estimated casualty catastrophe loss, a carrier may get more value by seeing how the loss changes directionally and on a relative basis as their portfolio's industries and exposed limits change. An insurer can also apply "what if" analyses to analyze the impact of proposed changes.

3) View, analyze and stochastically model how the casualty loss estimates compare with the industry loss for various specific realistic disaster scenarios. Guy Carpenter's approach allows an insurer to see how their loss compares with the industry loss, and whether it is out-sized compared to an insurer's market share.

ENTERPRISE-WIDE EVALUATION

The purpose of ERM is straightforward and unequivocal. It is intended to help (re)insurers determine how much capital is needed to support the risks they assume (subject to risk tolerance). Instead of segmenting portfolios and handling each peril on a standalone basis, ERM calls for a holistic approach to risk and capital management. These frameworks are used to identify and monitor all threats, develop action plans and measure results. The result, of course, should be the optimal deployment of capital, ultimately leading to an increase in firm value.

Unlike the traditional tools of the trade, ERM entails the assumption of risk based on its marginal impact to the company as a whole. While one risk, on its own, may seem tolerable, it could lead to disproportionate accumulation of linked risks. A portfolio may appear to be diversified, but one event (known and/or emerging) could expose a costly underlying reality. This is exactly the problem that casualty writers experience in regard to casualty catastrophes and emerging risks among our three categories. Insureds from several industries or countries could be affected by the same event, diluting the benefits of risk and geographic diversification. Separate risks do not reflect the integrated reality, masking a greater risk that typically goes unhedged.

Using ERM frameworks, casualty (re)insurers can ascertain the impacts of new and emerging risks on their entire businesses. Within the casualty catastrophe context, this includes the risks resulting from the proliferation of risk along a supply chain or through other business relationships, such as joint ventures and partnerships. The implications of covering a new insured may be more profound than they appear at first.

The careful evaluation of each new risk added to a portfolio moves the firm toward a metrics-based approach to risk and capital management, facilitating governance and enhancing the deployment of capital. The only problem for casualty writers, however, has been the availability of data and models to determine the true effects of a new risk to the carrier's entire portfolio. Even if a casualty carrier wanted to make the most of an ERM framework, it would be limited by data, models and technology. Fortunately, this situation is changing.

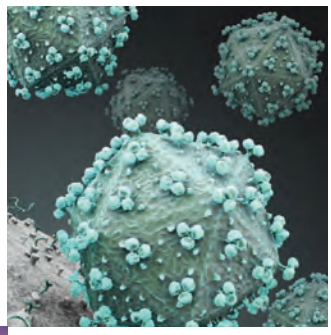
Innovation is catching up with the casualty catastrophe and emerging threat to (re)insurer capital.

Access to rich data sets and the development of new technology is beginning to enable insurers to see how emerging and liability risks can radiate from one insured through an entire portfolio of risks.

Although their development stage varies by peril and modeling approach, in an increasing number of scenarios, the unknown, in effect, are beginning to become knowable through the various models in development – and then can be integrated into an economic capital model framework.

VALUE OF METARISK® 7.3 & BENCHMARQ℠ IN INTEGRATING AND SYNTHESIZING THE MANAGEMENT OF EMERGING RISKS

Proper ERM assessment requires relative quantification of the various risks to the firm in addition to the absolute quantification of each of them. These risks encompass underwriting risk, reserve /payout pattern risk, reinsurance risk, traditional catastrophe risk as well as the various emerging and casualty cat risks previously discussed. Guy Carpenter's MetaRisk 7.3 and BenchmaRQ are standardized economic capital models empowering key decision makers with a deeper and more sophisticated view of complex risk drivers throughout their business. They also generate complete scenarios and the financial statements for each scenario contemplated. Built on the same foundation for each insurance company, they can facilitate comparisons of a company's risk profile to that of its peers and peer composites. This clarifies the severity and frequency risk profiles both on an absolute and essential relative basis. Emerging and casualty risks are typically quantified and correlated by Guy Carpenter subject-matter experts. An example of an event correlation may be between a product fault/failure and an interrelated financial collapse. An external structural model representing a company's various cat and emerging risks can be incorporated into our economic capital model framework for a more holistic and complete view of total enterprise risk. Without this, the absolute measure of one particular risk, known or emerging, would lack the essential context of their relative importance and correlation to all other risks the enterprise can encounter.

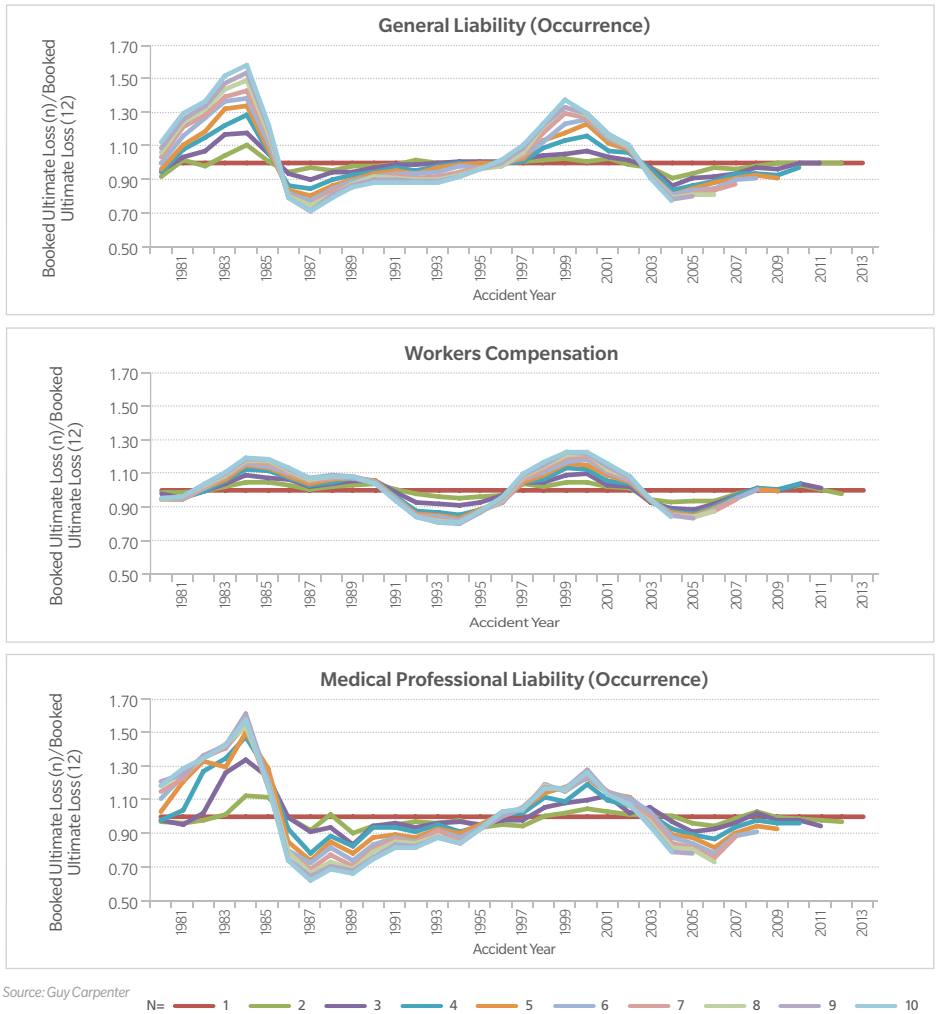


VII. RESERVING RISKS

The previous sections suggested how "dark matter" can be lurking on an insurer's balance sheets in the form of a casualty catastrophe or an emerging and not as yet fully understood risk such as cyber. While there have been significant advances in quantifying the uncertainty pertaining to these risks, it is worth considering how they may manifest themselves in the future and what can be done about them now to protect from the "dark matter" downside.

Insurance cycles are not a new development but the reasons why they are likely to persist are beyond the scope of this report. The Guy Carpenter/Oliver Wyman *Risk Benchmarks Report*,[23] published annually, clearly demonstrates that cycles are present. Figure 4 shows the reserve cycles present in various US insurance lines of business from accident years 1990 to 2013. The United Kingdom shows a similar but less pronounced picture. The exhibits show the movement in reserve at the end of the first year (the black line) to the ultimate position and each increase or release in reserves along the way. What can be inferred from these charts? It is clear that consecutive accident years tend to move in the same direction so there is clear correlation between accident years. The recognition of

F 4 | RESERVE CYCLES IN VARIOUS LINES OF US BUSINESS, 1990 TO 2013.
Booked Ultimate Loss After N Years of Development / Booked Ultimate Loss After One Year's Development, by Accident Year, US Industry in Aggregate by Line of Business, Net of Reinsurance



Source: Guy Carpenter

23. Guy Carpenter and Oliver Wyman, Insurance Risk Benchmarks Report.

any deterioration or improvement tends to happen gradually with bad years slowly getting worse and good years slowly getting better. It is also very evident that lines of business are heavily correlated. With correlation across the dimensions of time and line of business, correlation is everywhere.

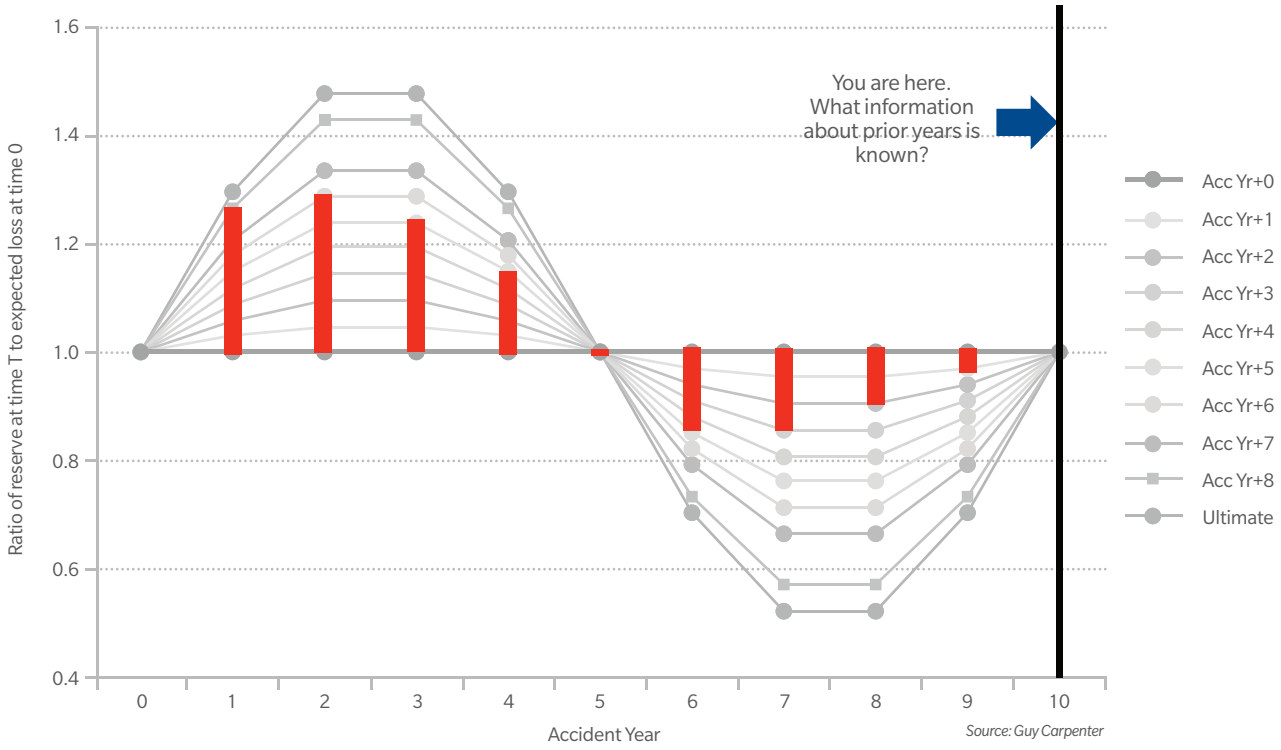
So what causes these correlations between years and between lines of business? The answer is a variety of events, some known and some as yet unknown. One of them, inflation, can be a driver of claims costs that will impact multiple classes and may continue for some time, causing increases or decreases in reserves across years. Similarly, legal changes and developments can impact multiple liability classes and will likely affect all open claims impacting successive years. Also, historically, asbestos-related claims affected multiple product lines and many accident years. These events prompt the question of what emerging risks could manifest themselves in some super-cycles to come.

IMPACT ON RESULTS

To consider the impact that these cycles may have on the financial statements and solvency positions of insurers there has to be an understanding of the magnitude of any change in ultimate loss and the likely timing of the recognition of that change. The profit or loss in any financial year is a combination of the profit and loss from that accident year and also any recognised changes in the reserves from prior years.

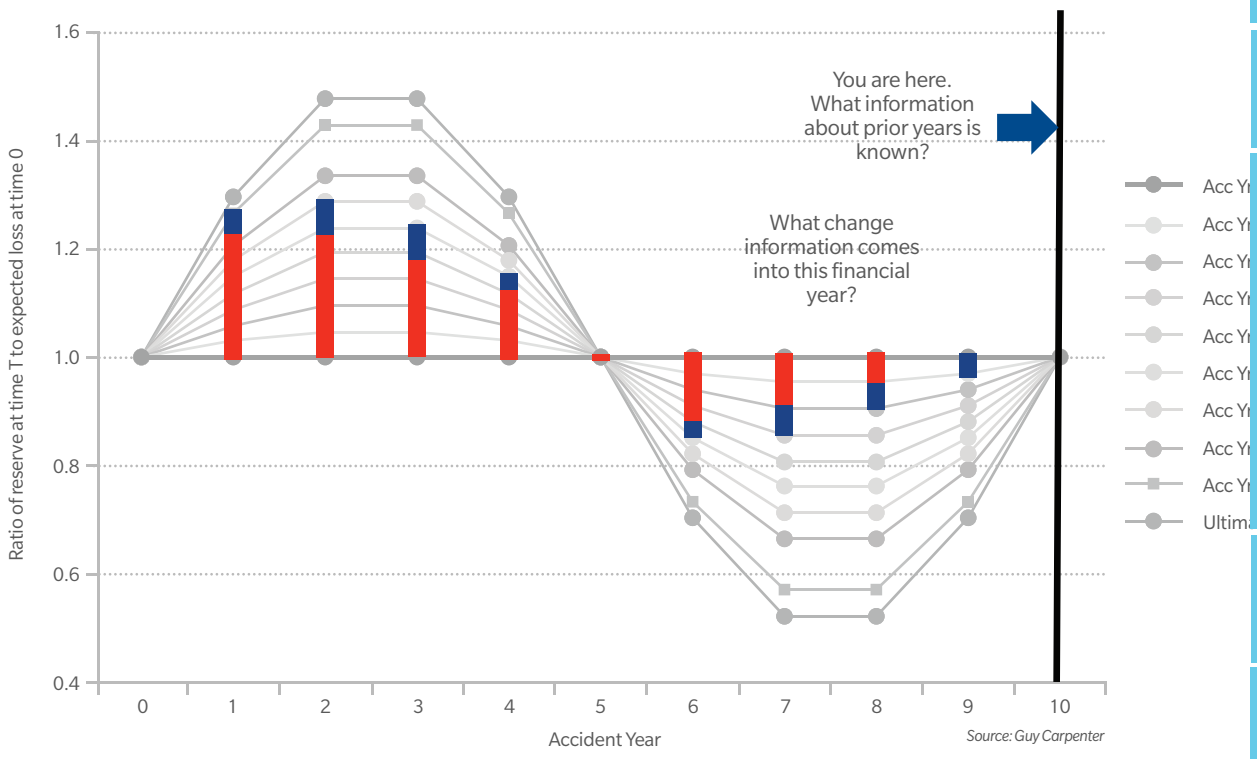
A simplified example of a cycle shows how the emergence of information flows through into the financial results. In Figure 5 below, if there is an assumption that financial results are about to published in Year 10, which is indicated by the black line, what information exists about the likely ultimate position of prior year reserves at that time? This information is shown by the red bars. There are reserve releases from prior years 6 to 9 and recognized increases in reserves from Accident Years 1-5.

F 5 | THE EMERGENCE OF INFORMATION OVER TIME:
What Information About Prior Years is Known?



The balance sheet will reflect this level of anticipated liability by a recording of this as the best estimate of liabilities for all years. From an earnings perspective in Financial Year 10 it is only the change in prior years, over the course of the last year, that will have an impact. The change information that comes into Financial Year 10 is shown by the blue bars in the chart below.

F 6 | THE EMERGENCE OF INFORMATION OVER TIME:
What Change Information Comes into This Financial Year?



In this simplified example of a perfectly symmetrical cycle and a constant volume of business, the reader would be forgiven for not being overly concerned about such a cycle scenario. The increases in the more distant back years have been mainly cancelled out by the releases in the more recent history. The real life situation, unfortunately, is rarely so simple. The choices made at each point in time in terms of business volumes and reinsurance buying strategy can be hugely influential on the outcome.

Following a period of sustained reserve releases, what would result if in Accident Years 0 to 5 volumes were dramatically increased across all lines? At Years 6 to 7, there is then some recognition of likely deterioration in Years 0 to 5, so the company contracts sharply. An assumption can be made that the increase in the reserves in Years 0 to 5 in this case is driven by large claims. At that time, however, it was thought that pricing in the excess of loss market for long-tail claims was too expensive. This leads to a decision to dramatically increase retentions. The result of these decisions would be a perfect storm. The company is heavily weighed down by reserve increases on years of expansion without having the full offsetting benefit of releases in more recent years. Reinsurance is set at a level that means it is not sufficient to dampen the large claim volatility.

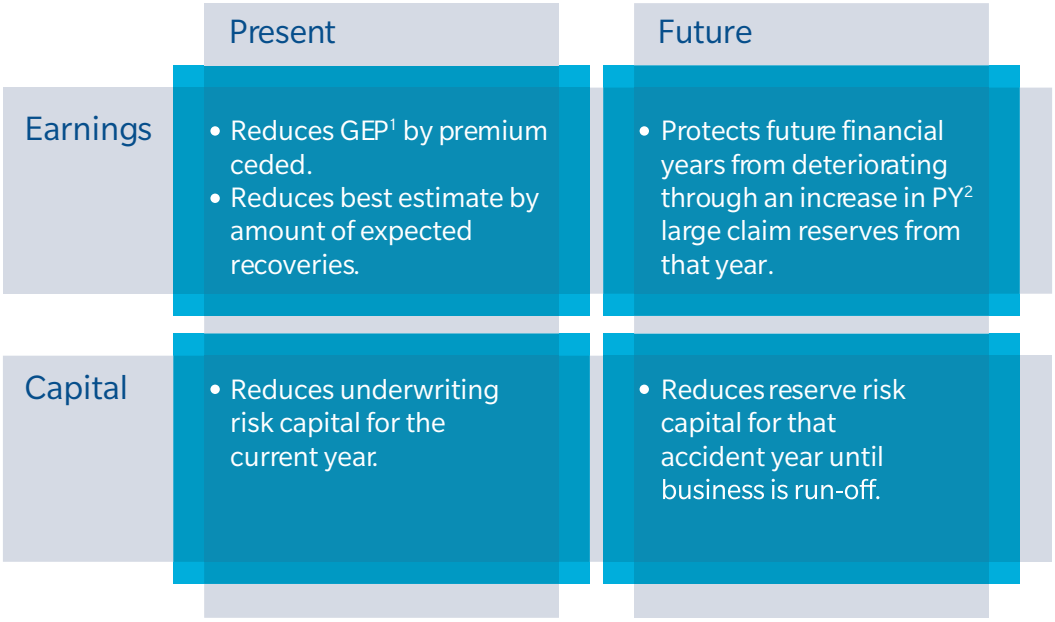
Is this scenario far-fetched? It appears not. A cursory search reveals examples of companies who have fallen foul of misreading the cycle to some extent or another.

CYCLE MITIGATION

So what can be done to mitigate such cyclical effects? The first steps are to acknowledge them and to try to quantify their impact. The latter is more of a challenge than the former. Most internal capital models are not truly multi-year and arguably fail to adequately capture both the correlation between lines of business and in particular across accident years. Cycle (and recognition pattern) scenario testing is a good way to achieve this. This provides a neat and practical way to correlate between years and lines of business.

A reconsideration of the construction of reinsurance buying strategy is needed. Before that reconsideration, however, it is worth remembering exactly how reinsurance (particularly for long-tail lines) can impact both earnings and capital both in the present and the future. Figure 7 shows this.

F 7 | CONSTRUCTION OF REINSURANCE BUYING STRATEGY



1) GEP: Gross earned premium
2) PY: Prior year

Source: Guy Carpenter

Reinsurance buying strategies have traditionally focused too much on the present cost and benefits and not nearly enough on the future costs and benefits. The industry could be accused of being tactical in this respect and not strategic. Short-termism can be damaging. For example many companies will consider reinsurance decisions in the context of economic value added (EVA).[24] This can be a sound approach but requires consideration of the definition of capital. It should theoretically be "total capital" but in most cases "underwriting risk capital" is used. This makes the EVA calculation appear to ignore the reserve risk capital benefits associated with buying reinsurance. Guy Carpenter has challenged this approach for some time and introduced the concept of the reserve value added (RVA) metric to capture this effect in reinsurance decision making.[25] RVA is analogous to the Solvency II risk margin – the calculation is very similar and it captures the time dimension of risk. Under Solvency II companies should be considering the impact on risk margin of their reinsurance strategy particularly where the liabilities are very long-tailed and the risk margin will be substantial and will not diversify away against shorter tail risks.

24. EVA is defined as the change in expected economic value that results from pursuit of a certain reinsurance strategy either versus the status quo or against buying no reinsurance with economic value defined as the expected profit or loss less the cost of capital associated with supporting the business.
25. See Jenkins, Leong, "The Total Value of Reinsurance" for more details: http://www.gccapitalideas.com/2014/06/16/the-total-value-of-reinsurance-for-long-tail-business-2/

Incorporating RVA into reinsurance decision making for long-tail lines is a step in the right direction. However, it is not the full story, as the decision is still typically made in the context of a single accident year and usually for a single line of business in isolation. The cycle correlations clearly show that this is sub-optimal. We are encouraging our clients a step further along the sophistication and hence simplicity/complexity spectrum.

F 8 | LONG TAIL REINSURANCE DECISION MAKING – THE SIMPLICITY/COMPLEXITY SPECTRUM

Simplicity (past) — Sophistication of Approach — Complexity (future)

Single year EVA[a]	Single year EVA and RVA[b]	Multi-year, multi-line EVA and RVA
• Impact on earnings • Impact on underwriting risk capital • Single accident year	• Impact on earnings • Impact on underwriting risk capital • Impact on future reserve risk capital (lifetime cost of capital) • Single accident year	• Impact on earnings • Impact on underwriting risk capital • Impact on future reserve risk capital (lifetime cost of capital) • For current year and **PAST YEARS** • Across all correlated lines of business.

Source: Guy Carpenter

a) EVA: Economic Value Added
b) RVA: Reserve Value Added

The future involves considering reinsurance not only in the context of one-year but in the context of all past-years and how, across all lines, they could develop. Unfortunately, we have not seen many capital models that accomplish this in a coherent way. There has not been much attention focused on true multi-year modeling that captures the potential for correlation across years – perhaps the distraction of the Solvency II one-year view of risk is to blame here. Capital modeling actuaries are challenged here. Parameterizing this correlation will be highly subjective and relies on limited data available from short time periods.

The complexity of the issue should not be intimidating. This is where scenario testing really comes into its own.

By overlaying different reinsurance strategies on a variety of cycle and recognition scenarios there can be serious improvement in reinsurance decision making.

This process helps to select a strategy that works well across the cycle and not solely for a single year in isolation. Hypothetical cycles themselves are actually a very neat way of generating the correlation. History can be replayed as it occurred, replayed with some tweaks or exteme scenarios from as yet emerging risks can be considered. Because the years and product lines are connected, reinsurance decision making across those years and lines needs to also be connected.

VIII. CONCLUSION

The downside focus of risk measures highlights what could be a key problem with the debate around emerging risks – when people think about risk they only consider the downside. Cars, penicillin, fossil fuels, the internet – all of these were once emerging risks, and they have caused global destruction through car accidents, antibiotic resistance, climate change, and now, possibly through cyber risk. But they have also brought far better travel, longer and much healthier lives for almost everyone, affordable electricity for people in their own homes, and an explosion of information on a scale never seen before available freely at the click of a button.

Continually improving our understanding of risk is imperative for the future of insurance, and of finance as a whole. Finding new ways to visualize and communicate risk is something we can all do to make this possible. Only when the true *origin* of a risk is discovered, can it be truly mitigated.

Whatever the category of emerging risk the main challenge lies in modeling and quantifying their potential impacts. Only in this way can insurers leverage their key capability, which is the creation of value by risk management.

Guy Carpenter offers advice and guidance to clients in these areas by delivering a powerful combination of specialized reinsurance broking expertise, strategic advisory services and industry-leading analytics.

IX. APPENDIX

F 9 | WORLD ECONOMIC FORUM: RISK CATEGORIES AND SURVEYED RISKS

Economic	Environmental	Geopolitical	Societal	Technological
• Fiscal crises in key ecomomies • Failure of a major financial mechanism or institution • Liquidity crises • Structurally high unemployment/ underemployment • Oil price shock to the global economy • Failure/shortfall of critical infrastructure • Decline of importance of US dollar as a major currency	• Greater incidence of extreme weather events • Greater incidence of natural catastrophes • Greater incidence of manmade environmental catastrophes • Major biodiversity loss and ecosystem collapse • Water crises • Failure of climate change mitigation and adaptation	• Global governance failure • Political collapse of a nation of geopolitical importance • Increasing corruption • Major escalation in organized crime and illicit trade • Large-scale terrorist attacks • Deployment of weapons of mass destruction • Violent inter-state conflict with regional consequences • Escalation of economic and resource nationalization	• Food crises • Pandemic outbreak • Unmanageable burden of chronic disease • Severe income disparity • Antibiotic-resistant bacteria • Mismanaged urbanization • Profound political and social instability	• Breakdown of critical information infrastructure and networks • Escalation in large-scale cyber attacks • Massive incident of data fraud/theft

Source: World Economic Forum, Global Risks 2014

CONTACTS

Morley Speed
Managing Director
+44 20 7357 5271
Morley.Speed@guycarp.com

Christopher Apps
Technical Innovation
+44 20 7357 5819
Christopher.Apps@guycarp.com

Mike Brown
Managing Director
+1 917 937 3033
Mike.Brown@guycarp.com

Aaron Bueler
Managing Director
+1 206 223 4891
Aaron.D.Bueler@guycarp.com

Kirsten Eickstaedt
Senior Vice President
+44 20 7357 5083
Kirsten.Eickstaedt@guycarp.com

Victoria Jenkins
Managing Director
+44 207 357 1684
Victoria.Jenkins@guycarp.com

Emil Metropoulos
Senior Vice President
+1 203 229 8817
Emil.Metropoulos@guycarp.com

Jeremy S. Platt
Senior Vice President
+ 1 917 937 3002
Jeremy.S.Platt@guycarp.com

ABOUT GUY CARPENTER

Guy Carpenter & Company, LLC is a global leader in providing risk and reinsurance intermediary services. With over 50 offices worldwide, Guy Carpenter creates and executes reinsurance solutions and delivers capital market solutions* for clients across the globe. The firm's full breadth of services includes line-of-business expertise in agriculture; aviation; casualty clash; construction and engineering; cyber solutions; excess and umbrella; excess and surplus lines; healthcare & life; marine and energy; mutual insurance companies; political risk and trade credit; professional liability; property; retrocessional reinsurance; surety; terrorism and workers compensation. GC Fac® is Guy Carpenter's dedicated global facultative reinsurance unit that provides placement strategies, timely market access and centralized management of facultative reinsurance solutions. In addition, GC Analytics®** utilizes industry-leading quantitative skills and modeling tools that optimize the reinsurance decision-making process and help make the firm's clients more successful. For more information, visit www.guycarp.com and follow Guy Carpenter on Twitter @GuyCarpenter.

Guy Carpenter is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and human capital. Marsh is a global leader in insurance broking and risk management; Mercer is a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman is a global leader in management consulting. With annual revenue exceeding $12 billion, Marsh & McLennan Companies' 55,000 colleagues worldwide provide analysis, advice, and transactional capabilities to clients in more than 130 countries. The Company prides itself on being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information.

*Securities or investments, as applicable, are offered in the United States through GC Securities, a division of MMC Securities Corp., a US registered broker-dealer and member FINRA/NFA/SIPC. Main Office: 1166 Avenue of the Americas, New York, NY 10036. Phone: (212) 345-5000. Securities or investments, as applicable, are offered in the European Union by GC Securities, a division of MMC Securities (Europe) Ltd. (MMCSEL), which is authorized and regulated by the Financial Conduct Authority, main office 25 The North Colonnade, Canary Wharf, London E14 5HS. Reinsurance products are placed through qualified affiliates of Guy Carpenter & Company, LLC. MMC Securities Corp., MMC Securities (Europe) Ltd. and Guy Carpenter & Company, LLC are affiliates owned by Marsh & McLennan Companies. This communication is not intended as an offer to sell or a solicitation of any offer to buy any security, financial instrument, reinsurance or insurance product. **GC Analytics is a registered mark with the U.S. Patent and Trademark Office.

MARSH & McLENNAN COMPANIES

GUY CARPENTER