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

A CLEARER VIEW OF EMERGING RISKS

EMERGING RISKS
REPORT
SEPTEMBER 2015

MARSH & McLENNAN
COMPANIES

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

GUY CARPENTER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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.

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

Technological progress is accelerating at a rapid pace and with it are the risks and opportunities that accompany those changes in many different segments of our economy:

- Exposures to cyber-attacks are increasing due to proliferation of technology, cloud computing and electronic commerce.
- Medicinal advances, pharmaceutical breakthroughs and a continued focus on healthy life styles are prolonging our lives, increasing exposure for annuity or pension plan providers.
- The cost of medical services continues to increase, putting pressure on health (re)insurers to price their products correctly as well as adequately quantifying potential claims volatility over multiple years.
- New chemicals are being used every day in new products — and these new products could lead to new diseases that are not yet quantifiable, creating unknown implications for any number of product lines.
- New mechanical products and processes, such as drones, 3-D printing and self-driving automobiles are transforming the liability potential for (re)insurers in many different industries.

The emergence of these increasingly complex global risks are challenging the way the (re)insurance industry evaluates, analyzes and manages these new exposures.

Last year, in our report, “*Ahead of the Curve: Understanding Emerging Risks*,” we noted that the industry needs “to build credible models of potentially accumulating incidents so that risk appetites can be aligned with the exposures being faced.” However, the problem with emerging risks is the lack of historical data with which to build these models.

In this year’s report, “*A Clearer View of Emerging Risks*,” our goal is to assess the challenges facing the (re)insurance industry in modeling and quantifying the most pressing technological risks that society may face. Whether they are high-profile cyber-attacks that could stretch across several industries or a nation’s power grid to the global phenomenon of longer life spans that are having a major impact on pension funds and annuity writers, these risks require the industry to ask different questions in order to formulate effective models that will provide a more robust view into how these risks could develop over time.

Crystalizing risks, as defined in 2014’s report, are highly interrelated with the technology risks discussed in this report. When we refer to crystalizing risk, the term refers to the timescale over which underwriters realize that the technology risk is manifesting itself — and how this view changes and intensifies until ultimate understanding of quantum is reached and liabilities are discharged. The risks associated with new technologies, implemented rapidly on such a global scale, by their nature operate to a large extent somewhat outside the bounds of our current knowledge. A viable 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.”[1] Most (re)insurers have groups of experts assigned to the task of building early warning systems that attempt to identify such lead indicators. Once such indicators are identified it is important that their financial and reserving implications are recognized promptly and accounted for correctly. In this respect a key task of regulators is to enforce prudent risk management and reserving methodologies that preserve a sustainable and level playing-field for responsible competition.

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 as described in the following sections. However, there is one consistent theme across all of them: to bring a robust analytical thought process to better understand and to the extent practical, quantify the risk. This will create a marketplace where these risks can be transferred to third parties or retained with greater confidence by (re)insurers. This occurs against a backdrop of increased regulatory oversight with rating agencies asking these same parties to quantify these unknown risks with a formalized risk evaluation process. Underwriters addressing crystalizing technology risks should provide a competitive advantage to those ahead of the curve in their identification, modeling and mitigation. In addition, regulators also have the responsibility to ensure that improvements in the data and modeling of emerging risks are not underestimated or overlooked, resulting in long term industry instability.

All of these dynamics are combining to force the (re)insurance industry to bring these standardized processes to the casualty marketplace.

In our report, we examine four key areas where risks continue to emerge or, perhaps more importantly, contain elements where the risks are unknown at this time:

- Cyber
- Life, health and longevity
- New technologies
- Casualty catastrophe reserving

[1] *Dr. Andreas Tacke, Hannover Re: Hannover Re on Emerging Risks, February 2013.*

CYBER RISK

Consider the evolving nature of cyber risk. Cyber-attacks are now considered to be above average in terms of likelihood and impact, according to the *Marsh 2015 World Economic Forum Global Risks Report*.[2] At the same time, data breaches continue to evolve, with organizations and individuals not knowing the potential form(s) and target(s) of the next cyber-attack. For instance, breaches in the United States have spread from the retail sector in 2014 to healthcare, government and other parts of the economy in 2015.

The key function of modeling is trying to determine what the likelihood of an event occurring is and, once that happens, what the size of that loss might be. But, the level of historical data that has been used to build probabilistic models for natural catastrophes does not yet exist for cyber risk. (Re)insurers have little information when assessing the severity and frequency of possible cyber catastrophe scenarios. Add in the potential for multiple insureds being implicated in a single breach, and the scope of the necessary modeling needed in an emerging risk class is daunting with a wide range of potential loss estimates.

LIFE, HEALTH AND LONGEVITY RISK

Meanwhile, longevity risk is beginning to raise concerns. The United Nations expects the aggregate expenses of the elderly will double over the period between the years 2010 and 2050. Beyond the impact on governments, this directly challenges pension fund managers and annuity writers who are assuming whole-of-life financial liabilities. Faster than expected improvements in mortality can result from improvement in underlying population health or dramatic changes in the underlying prognoses for specific pockets of individuals. The issue for (re)insurers regarding longevity risk lies in the inability to measure it because changes in longevity are difficult to forecast, particularly if there is a precursor to a change that is inconsistent with the long-term health patterns present in historical data. Being able to anticipate and quantify that impact is the key challenge.

TECHNOLOGY RISK

Technological risks are genuinely new and emerging from new technologies and processes. In this report, we consider two areas where technology risk has rapidly become apparent:

1. Nanotechnology — chemical technology breakthroughs such as those involved in making stronger and enhanced materials may have unknown liability outcomes many, many years in the future. How should this be analyzed?
2. Drones and other technological advances that remove human input into the machine's operations. Commercial applications are increasing rapidly and potential for misuse of this technology needs to be considered.

Any further attempt to categorize the risks associated with these emerging technologies is increasingly challenging due to the numerous new advances that are interdisciplinary in nature.

Clearly, we are entering a new phase of technological advances that will bring new exposures that were not present in any historical database. As a result, (re)insurers will need to develop models that are based more on estimates and assumptions than on experience.

Accordingly, the report then considers the limitations in using traditional actuarial modeling methods to factor in unknown and new risks in order to ensure that adequate capital is best positioned to protect the (re)insurer through casualty catastrophe and reserving risks.

[2] *Global Risks 2015 (10th Ed.), World Economic Forum, Geneva, 2015.*

CASUALTY CATASTROPHE AND RESERVING

Casualty or liability based catastrophes in general have become increasingly frequent and severe over the past decade, exposing (re)insurers to increased and newer risks and for which they may not have made appropriate reserves provisions. These can take any number of forms, including advserse reserve development or large events that impact multiple insureds across several different lines of business.

Implicit in the very idea of emerging risks is the impact on reserving and capital setting. A single product or another high-tech risk can result in a chain reaction that can produce losses over several accident years' reserves simultaniously and even expose a company to insolvency.

Most commonly used reserving techniques rely on historical data, but for emerging risks, that information may not yet exist. Additionally, there will be risks for which there is no data and no available model.

The section of the report that examines reserving risks outlines the problems in many models and what is being done to resolve those issues. In recognition of the dearth of data, the use of Structured Expert Judgment (SEJ) for quantifying many difficult-to-analyze risks is on the rise. SEJ is being utilized to estimate the probability of hard to estimate risks such as volcanic eruptions and cyber aggregations. The process involves extracting loss scenarios, estimates of loss quantum and likelihood of occurrence from a panel of experts.

The report also examines a critical element that is missing from most models: the timescale over which an insurer realizes that the risk is manifesting itself and how this view changes until the quantum of damages is reached and all liabilities are discharged. As we have seen in the past, these quanta can represent billions of dollars of payments.

The best historic example is the liability from exposure to asbestos. A.M. Best has stated that asbestos has cumulatively paid out over USD85 billion, and by some accounts after several decades, is just entering its third wave of emergence.[3]

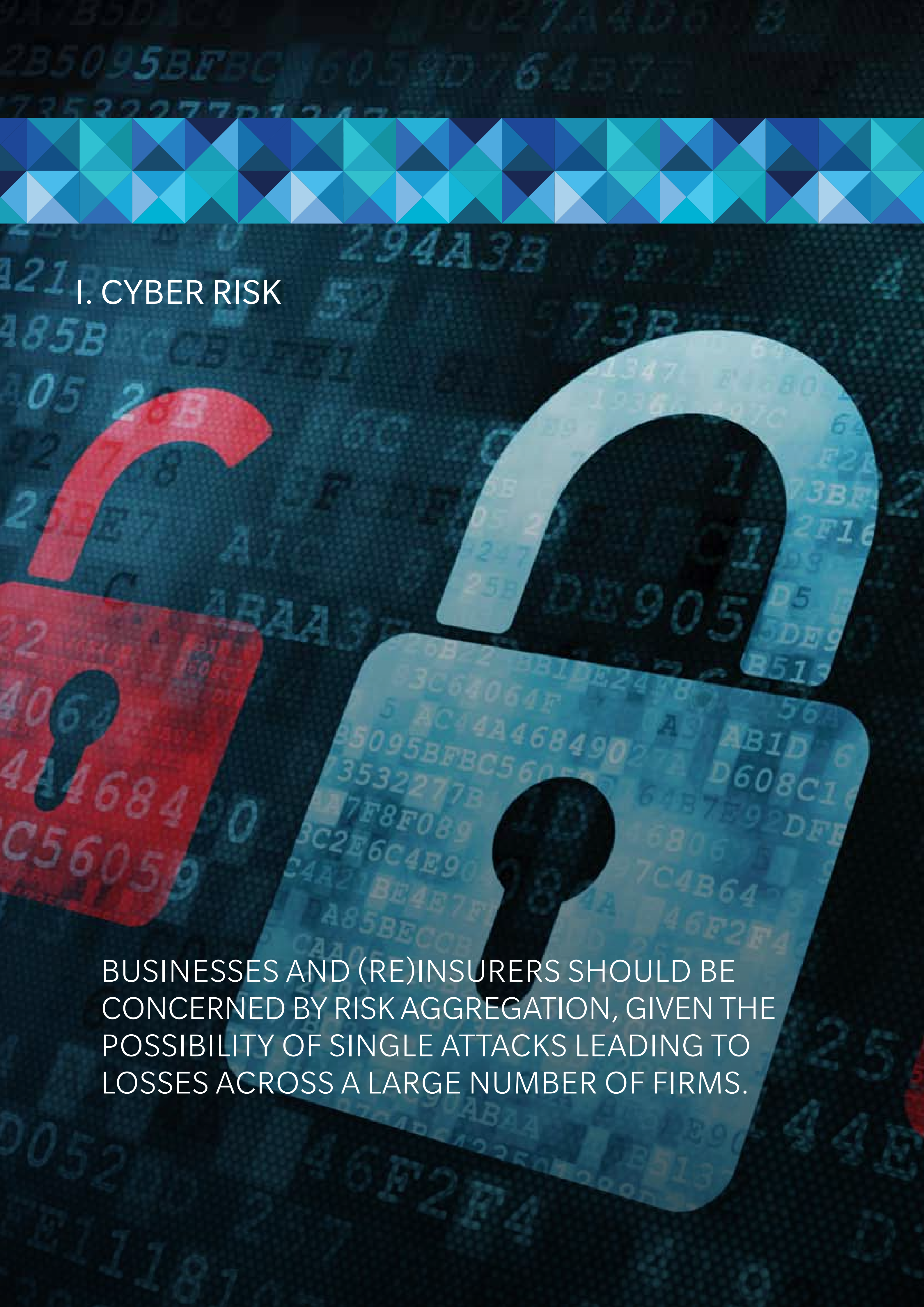
The reserves have crept up, been affected by various court decisions and are still not fully concluded in many cases and jurisdictions. In fact, new asbestos claims and settlement of previous ones are still ongoing, in part because of the long latency period of asbestos illnesses — about 40 years according to the Manville Personal Injury Settlement Trust. Additionally, some commentators have noted that actuarial models consistently underestimate exposures from this risk.

This report is not meant to find the next asbestos, but rather to examine what are emerging/unknown exposures, show how the industry can think about quantifying these exposures and what tools can be used to start to build that standardized process (however non-standard that exposure might be).

Rapid scientific advancement will only continue and the (re)insurance industry should be anticipating the risks of new technologies, developing new products in response to those threats and solving for how to manage these exposures. It is that level of innovation that will translate risk into opportunity.

[3] *A.M. Best: Asbestos Losses Fueled by Rising Number of Lung Cancer Cases, October 2013.*

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion



I. CYBER RISK

BUSINESSES AND (RE)INSURERS SHOULD BE CONCERNED BY RISK AGGREGATION, GIVEN THE POSSIBILITY OF SINGLE ATTACKS LEADING TO LOSSES ACROSS A LARGE NUMBER OF FIRMS.

Cyber risk is one of the most pressing and public topics that industry is grappling with and is being addressed as a strategic priority in corporate boardrooms and by governments around the world. As the global economy becomes increasingly dependent on e-commerce and cloud computing, the susceptibility to cyber risk increases exponentially.

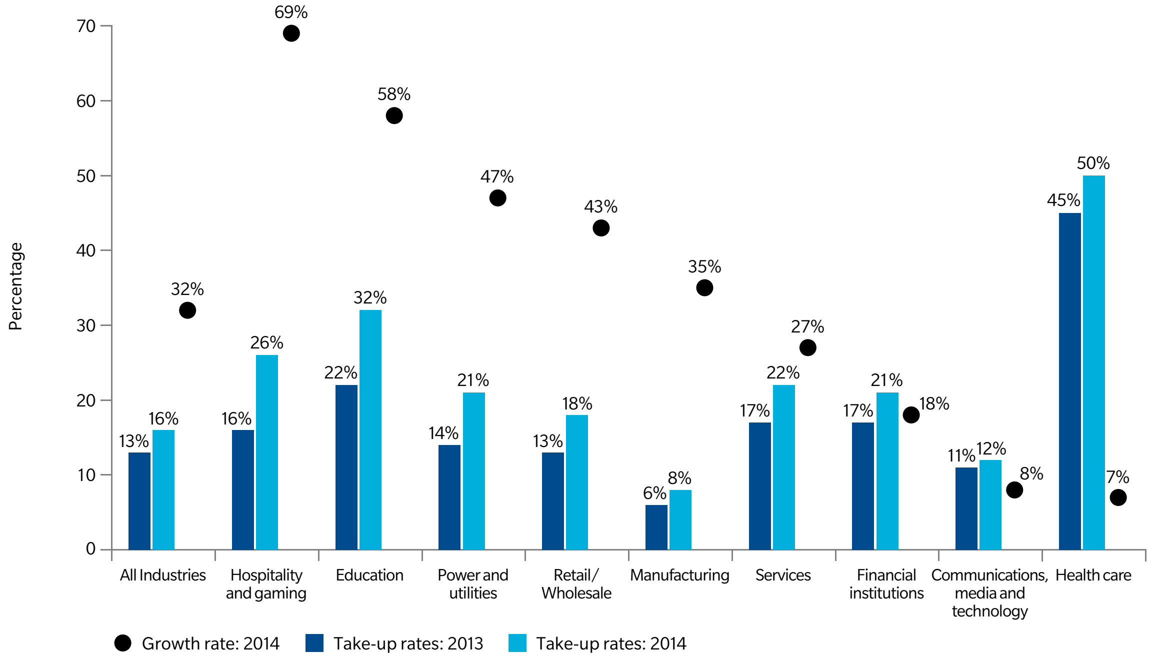
While this emerging risk presents significant opportunities for the industry, there are also many challenges. In addition to exposure from cyber network security and privacy liability policy portfolios, the potential for loss to physical assets could be especially significant for energy and utility infrastructures, financial institutions and power grids that are now facing the consequences of "cyber" as a peril.

The limited history, lack of data and emerging exposure make it difficult for (re)insurers to measure cyber risk and calculate capital needs. There is an opportunity to innovate with the development of modeling capabilities that can measure and quantify the cyber risk to determine pricing, correlated loss and capital support.

This is critically important because of the expected growth of the cyber insurance market, which is projected to increase from approximately USD2 billion today to USD5 billion over the next five years. This is driven by new purchasers of the product as well as by existing buyers purchasing more limit:

- The number of US-based clients of Marsh, Guy Carpenter's affiliate, purchasing standalone cyber insurance increased 32 percent in 2014 over 2013.[4]
- The cyber take-up rate — the percentage of existing Marsh financial and professional liability clients that purchased cyber insurance — rose to 16 percent.[5]
- The number of first time purchasers is increasing, while many existing buyers continue to increase limits purchased.

F-1 | CYBER INSURANCE TAKE-UP AND GROWTH RATES BY INDUSTRY



Note: In the above chart, "growth rate" refers to the percentage increase from 2013 to 2014 in the number of clients purchasing standalone cyber insurance. "Take-up rate" refers to the overall percentage of clients that purchased standalone cyber insurance

Sources: Marsh Global Analytics

[4] *Marsh: Benchmarking Trends; As Cyber Concerns Broaden, Insurance Purchases Rise, March 2015.*
[5] *Marsh: Benchmarking Trends; As Cyber Concerns Broaden, Insurance Purchases Rise, March 2015.*

This increased demand is being driven by:

1. The significant degree of discomfort at board level given the newness of the risk and its potential for costly and public disruption.
2. Approximately half of the UK business leaders Marsh has met with are not aware that there is a specific product that covers cyber risk.[6]
3. Although the penetration of network/privacy liability insurance in the United States is estimated to be 30 percent, just 2 percent of large UK firms have explicit cyber cover, a figure that drops to close to zero for smaller firms.[7]

As publicity around cyber continues to increase and regulators require more and more disclosures and protections for consumers, we would expect more and more insureds will purchase cyber, leading to a greater need for analytics in this product line. Accordingly, the (re)insurance market is grappling with how the peril of cyber and its exposure can be managed within specialty, casualty and property reinsurance programs.

Many firms place cyber among their leading risks in terms of the likelihood and severity of impact.[8] Consequences that cause the greatest concern include data loss, business interruption and theft of intellectual property, with the impact being dependent upon the industry, risk profile and size of a particular firm. There is a growing concern with the physical damage impacts of cyber-attacks (whether indirectly or directly), given the increasing connectedness of assets linked to the Internet.

A Marsh–HM Government report found that large firms have done a lot to make themselves cyber secure, yet significant risks remain.[9] The risks include exposure from third parties from a variety of sources, including service providers, product suppliers, customers or in the case of banks, their borrowers. Businesses therefore need to improve supply-chain resilience to cyber-attack, particularly in cases where they have smaller business partners who are typically less well protected.

CYBER-ATTACKS

The UK Government has recognized cyber-attacks to be one of the most significant risks facing the country. The costs to businesses are rising as hackers become more focused and persistent in their attacks. Several attempts have been made to quantify the economic cost of cyber crime on UK businesses. While there are a wide range of estimates, figures consistently range in the billions of pounds.

In its broadest form, cyber risk is synonymous with information technology (IT) risk — that is, "the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."[10] Such a broad definition makes sense because similar outcomes may arise from an IT event, irrespective of whether its cause was malicious or not and whether it arrived via the Internet or from internal systems.

Damage to an organization resulting from a cyber-attack can be categorized into 11 forms, indicating the extent to which cyber risk deserves to be afforded much greater consideration than the current focus on data breach. This categorization also recognizes that where a cyber-attack is directed at an organization that companies depend on as part of their supply chain, have system links with or use to store data on corporate or personal customers, the impact of the attack may be felt well beyond the attacked organization. As such, companies should consider the impact a cyber event at a supplier or other affiliate could have on their own business.

Cyber-attacks represent a present and growing danger that threatens businesses, irrespective of size and sector. The UK Government's annual breach report shows that 81 percent of large businesses and 60 percent of small businesses suffered a security breach in 2014.[11]

[6] *Marsh, HM Government: UK Cyber Security; The Role of Insurance in Managing and Mitigating the Risk, March 2015.*

[7] *Estimate based on policies placed/written by insurers who participated in the Marsh, HM Government: UK Cyber Security project.*

[8] *Global Risks 2015 (10th Ed.), World Economic Forum, Geneva, 2015.*

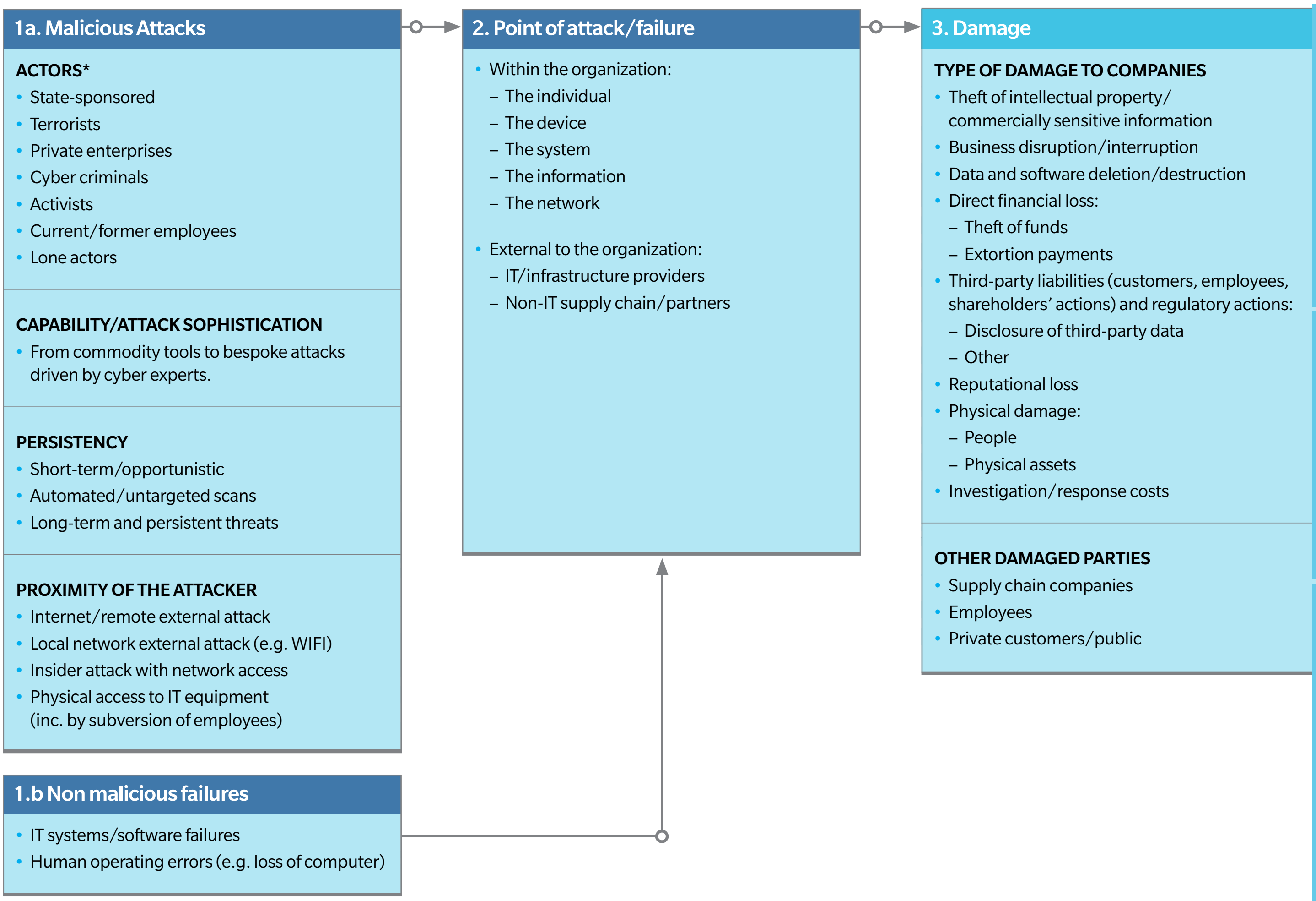
[9] *Marsh, HM Government: UK Cyber Security; The Role of Insurance in Managing and Mitigating the Risk, March 2015.*

[10] *ISACA Risk IT Framework Excerpt, 2009.*

[11] *2014 Information Security Breaches Survey, UK Department of Business Innovation and Skills, 2014.*

BUSINESSES AND THEIR EXPOSURES

T-1 | TAXONOMY OF CYBER RISK FOR CORPORATIONS



1a. Malicious Attacks

ACTORS*
- State-sponsored
- Terrorists
- Private enterprises
- Cyber criminals
- Activists
- Current/former employees
- Lone actors

CAPABILITY/ATTACK SOPHISTICATION
- From commodity tools to bespoke attacks driven by cyber experts.

PERSISTENCY
- Short-term/opportunistic
- Automated/untargeted scans
- Long-term and persistent threats

PROXIMITY OF THE ATTACKER
- Internet/remote external attack
- Local network external attack (e.g. WIFI)
- Insider attack with network access
- Physical access to IT equipment (inc. by subversion of employees)

1.b Non malicious failures

- IT systems/software failures
- Human operating errors (e.g. loss of computer)

2. Point of attack/failure

- Within the organization:
  - The individual
  - The device
  - The system
  - The information
  - The network
- External to the organization:
  - IT/infrastructure providers
  - Non-IT supply chain/partners

3. Damage

TYPE OF DAMAGE TO COMPANIES
- Theft of intellectual property/ commercially sensitive information
- Business disruption/interruption
- Data and software deletion/destruction
- Direct financial loss:
  - Theft of funds
  - Extortion payments
- Third-party liabilities (customers, employees, shareholders' actions) and regulatory actions:
  - Disclosure of third-party data
  - Other
- Reputational loss
- Physical damage:
  - People
  - Physical assets
- Investigation/response costs

OTHER DAMAGED PARTIES
- Supply chain companies
- Employees
- Private customers/public

*Actors often correlated with MOTIVATION (1 Warfare/terrorism, 2 Propaganda , 3 Commercial gain/advantage, 4 Direct financial gain, 5 Protest, 6 Fun/demonstrate ability, 7 Revenge).

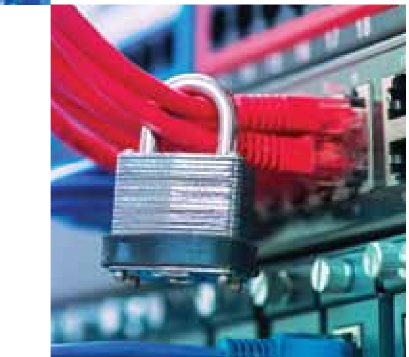
Source: Mars

As referenced in the taxonomy provided in Figure T-1, the potential losses deriving from cyber-attacks or non-malicious IT failures fall into the following 11 categories:

T-2 | LOSS CATEGORIES DERIVING FROM CYBER ATTACKS AND NON-MALICIOUS IT FAILURES

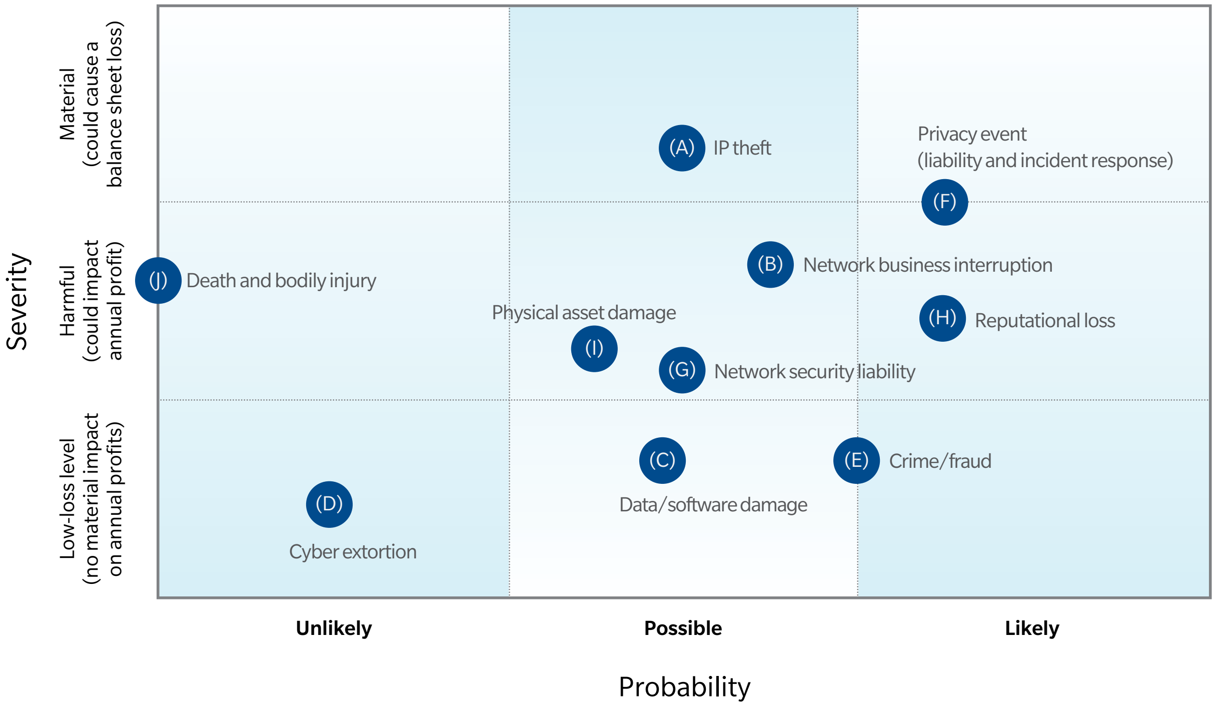
Loss category	Description
A Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
B Business interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber-attacks or other non-malicious IT failures.
C Data and software loss	The cost to reconstitute data or software that has been deleted or corrupted.
D Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
E Cyber crime/cyber fraud	The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities or other property.
F Breach of privacy event	The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.
G Network failure liabilities	Third-party liabilities arising from certain security events occurring within the organization's IT network or passing through it in order to attack a third party.
H Impact on reputation	Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
I Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber-attacks.
J Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber-attacks.
K Incident investigation and response costs	Direct costs incurred to investigate and "close" the incident and minimize post-incident losses. Applies to all the other categories/events.

Source: Marsh



The insurance industry underwrites cyber risk by forming a view of the severity and frequency of cyber events. Figure 2 summarizes that view for the different loss categories for large UK businesses, noting that one event can trigger more than one loss category. Furthermore, in almost all cyber events, the company incurs incident investigation and response costs, which can account for around 10 percent to 20 percent of the cost of a cyber-security breach for a large business,[12] according to a survey of UK companies.

F-2 | RISK PROFILE FOR LARGE UK BUSINESSES



Source: Marsh

Physical losses are a growing concern — both in terms of severity and frequency — given the interconnectedness of cyberspace and the physical world. One example of this new category of risk can be seen in the way that industrial control systems operate in the energy sector. Today, these new generation control systems are built on the concept of openness and interoperability, and this has exposed the sector to a host of cyber security risks that are only just beginning to be understood.

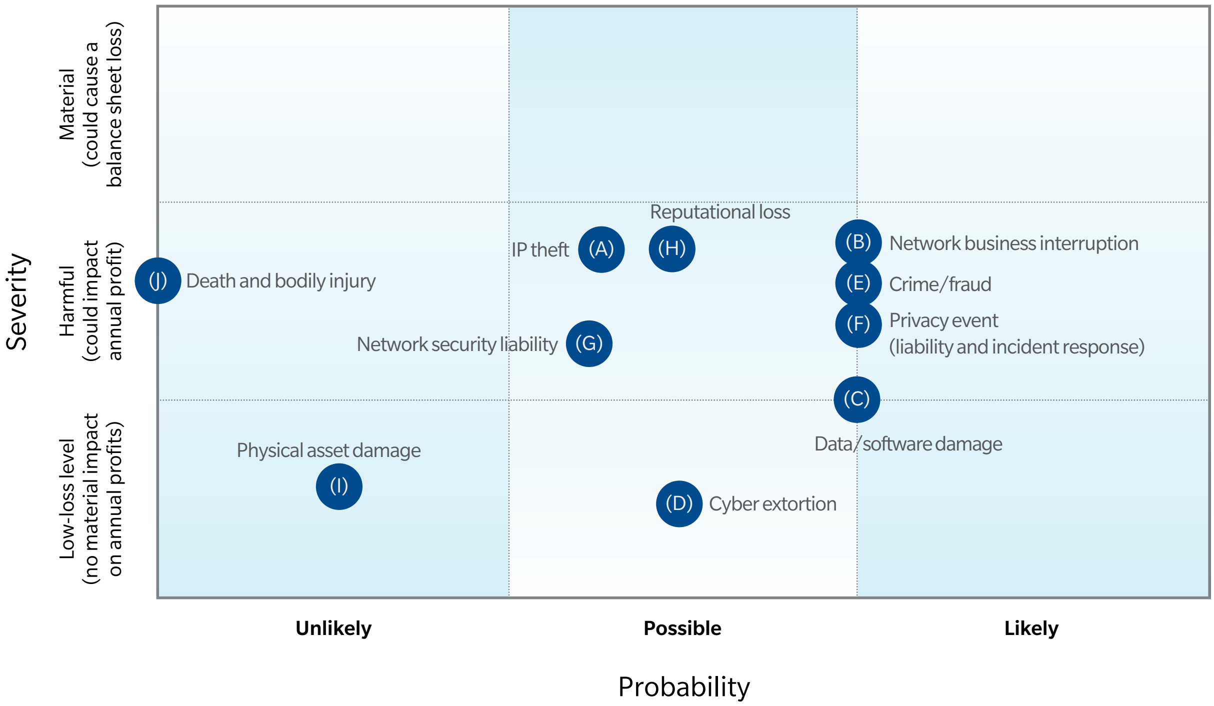
A recent example of a physical loss resulting from a cyber-attack occurred at a steel mill in Germany after hackers managed to gain access to the control systems following a successful "spear phishing" attack, which targeted particular individuals for login details. Once access was secured, the hackers were able to cause the unscheduled shutdown of a blast furnace that resulted in "massive damage," according to the German Federal Office for Information Security.

For the time being, the probability of death and bodily injury resulting from a cyber-attack is considered to be negligible. We should note, however, that in the future, as more devices go online, cyber hacks and system malfunctions could pose a more material threat to human life.

[12] 2014 Information Security Breaches Survey, UK Department of Business Innovation and Skills, 2014.

The picture for small to medium-sized enterprises or SMEs in the United Kingdom (see Figure 3) is broadly consistent with that for larger firms, but for this segment of companies, (re)insurers see a higher incidence of cyber crime. For example, a small broker was targeted by a phishing scam, where an e-mail containing a link to malicious software was sent to the financial controller within the business. The controller was tricked into installing the software onto his personal computer, and this software was used to steal banking credentials. The cyber criminals were subsequently able to complete electronic wire transfers to the total of GBP100,000 over the following 10 days.

F-3 | RISK PROFILE FOR UK SMES



Source: Marsh

SMEs are also considered to be at a greater risk of data/software damage. This reflects the belief that SMEs are more vulnerable to attack and lack the back-up disaster-recovery solutions of larger firms. On the other hand, with the exception of those working on innovative technologies, most SMEs are considered less likely to suffer from losses connected to damaged reputation or intellectual property theft.

Most companies' typical risks involve low-level impacts that can be managed within the business, monitored via a risk register and mitigated by insurance. That approach is likely to be inadequate for a tail risk like cyber, however, given the scale and pace with which it can threaten business viability. This becomes a reporting issue for listed firms under the viability statement now required by the UK Corporate Governance Code. More generally, it becomes a challenge for how risk governance operates.

CYBER GAPS IN TRADITIONAL INSURANCE PRODUCTS/ STANDALONE INSURANCE PRODUCTS

Although the insurance market has developed a dedicated product line that addresses the initial risks faced by companies, such as data breach and business interruption due to network failure, traditional insurance products in their design have not historically contemplated the exposure to protect against cyber risks. Companies can purchase cyber specific cover in the form of extensions to traditional policies or as standalone cyber policies.

In addition, underwriters of traditional insurance business lines have, in some cases, reacted to the emergence of this new class of risk by introducing several endorsements addressing the disclosure or access of confidential personal information within the commercial general liability policy through exclusion endorsements (CG 21 06 05 14, CG 21 07 05 14 and CG 21 08 05 04). The result is a mix of implicit and explicit cover as well as a number of exclusions to contend with. It makes it an exercise in and of itself to ascertain the true level of cover for any given cyber risk scenarios.

Cyber gaps and exclusions in traditional policies, together with the emergence of standalone cyber insurance solutions for new risks, often create a complex picture, where businesses struggle to fully understand the boundaries of their cover.

AGGREGATION/RATINGS AGENCIES

Businesses and (re)insurers should be concerned by risk aggregation, given the possibility of single attacks leading to losses across a large number of firms, which can create counter-party risk for the insured and potential failure for the insurer. At the moment, a large systemic event has not materialized, but that does not mean that the risk is not present.

While some market participants have suggested that a possible government backstop may be necessary, there is no conclusive evidence of the need for such a solution at present. Where a government "pool" might be required is in the area of "systemic" losses that could potentially exceed the resources of the insurance industry, as with terrorism or flood. However, the establishment of such pools requires a clear articulation of the systemic peril, as well as a significant market dysfunction, which is generating a meaningful consumer response. Cyber is not yet at this stage. One of the roles for the data pooling forum described above will be to improve insights on aggregation risk and cyber disaster scenarios. The insurance sector will continue industry discussion on market capacity and the cyber risk pool.

Therefore without the governmental back-stop and the industry's ability to address/absorb these risks in the marketplace through traditional insurance products and risk transfer methods, cyber risk has become a factor for rating agency evaluations:

- Fitch Ratings recently stated that "the potential for any future credit impact to major providers is kept in check by the still relatively small size of the cyber-related insurance market." Fitch also noted that it is "less clear how loss aggregation could play out under a severe cyber-attack that leads to insurable events covered by non-cyber related catastrophe policies, including standard commercial liability, business interruption and professional liability."
- A.M. Best indicated that it will ask:
  - Specific questions on cyber risk on its Supplemental Rating Questionnaire.
  - How the policy is sold — whether it is standalone or as a sublimit within another policy.
  - Enquire about lines of business and types of coverage purchased, such as business interruption or theft of cyber assets.
  - In meetings with rating analysts, there will be questions, such as whether the client has ever been the target of a cyber-breach or attack and where responsibility lies within the organization when it comes to managing cyber related risks. There will also be a focus on premium and loss expectations for cyber risk as well as estimated costs for crisis services and legal defense.[13]

[13] *A.M. Best Insurance Industry Update IASA NY/NY Chapter May 18, 2015.*

With the increased scrutiny from these types of outside institutions, (re)insurers will need to quantify and address these questions in the future to ensure they are viewed favorably.

The aggregation of risk is ever more present because cyber insurance is a global class of business with losses emanating from any part of the world. The non-physical nature of cyber risk makes it possible for (re)insurers to suffer losses from a vast number of insureds spread across different geographies as a result of a single event. That creates aggregation risk, for which an insurer or reinsurer could find itself burdened with catastrophic losses.

Some of the steps for (re)insurers meeting these challenges involve enhancing the quality of data available and to continue the development of probabilistic modeling for cyber risk, particularly with respect to potential loss accumulations.

Modeling the aggregation of physical risks is well established. For example, a large amount of historical data is used to build probabilistic models with regard to natural catastrophes. This level of data does not exist for cyber risk, which means that (re)insurers have to rely on experts making educated assumptions when assessing the severity and frequency of possible cyber catastrophe scenarios. This has led to there being an extremely wide range of estimates for the likely cost of each of the scenarios listed above.

So too with the difficulty facing individual firms in quantifying their cyber risk, an alternative approach is to look at total exposure and capacity. If we consider that the cyber insurance market could treble in the next three to five years, the industry's probable maximum loss (PML) for cyber risks could easily exceed the global (re)insurance capacity available for other aggregating events, such as nuclear disaster (GBP3 billion) or natural catastrophe (GBP65 billion).

An "extreme loss scenario" does not necessarily arise solely from a single large loss event involving numerous insureds. It also may stem from a number of unrelated loss events affecting numerous insureds during any given annual period or a combination of scenarios. A final layer of complexity arises from the potentially high level of systemic risk overlapping multiple insurance lines of business.

Despite the lack of a clear consensus of the size of the PML that the insurance industry could face, at the moment most insurers are comfortable with the size of their total exposure to affirmative cyber coverage provided through stand-alone policies and/or endorsements. That being said, given the nature of this emerging risk, some insurers are exploring and electing to purchase reinsurance solutions to protect their portfolios against volatility and catastrophic loss.

It is possible that aggregate exposure either does already or will soon become a problem for the market to absorb, since the fact that such an event has not yet occurred is no doubt encouraging the market to continue to increase its exposure.

CYBER RISK MANAGEMENT

Cyber risk is already an embedded feature of the global risk landscape, not only as a privacy/network liability, but also as a peril affecting traditional insurance lines. As such, insurance has the potential to greatly enhance cyber risk management and resilience for a wide range of organizations and individuals who are exposed to its impacts. Nevertheless, the likelihood and impact of severe events remain subject to much uncertainty, and the pace of insurance innovation should be linked to the rate at which this uncertainty can be reduced.[14]

Data will be a key factor for enabling further analysis and the development of models to enhance the understanding of cyber risk. The systemic, intangible and constantly evolving nature of cyber threats presents significant challenges for gathering the data required to achieve accurate quantification of the risk for insurance portfolios that could trigger a wide range of economic losses on a global basis.

[14] Lloyd's: Emerging Risk Report, Business Blockout, The Insurance Implications of a Cyber-attack on the US Power Grid, 2015 .

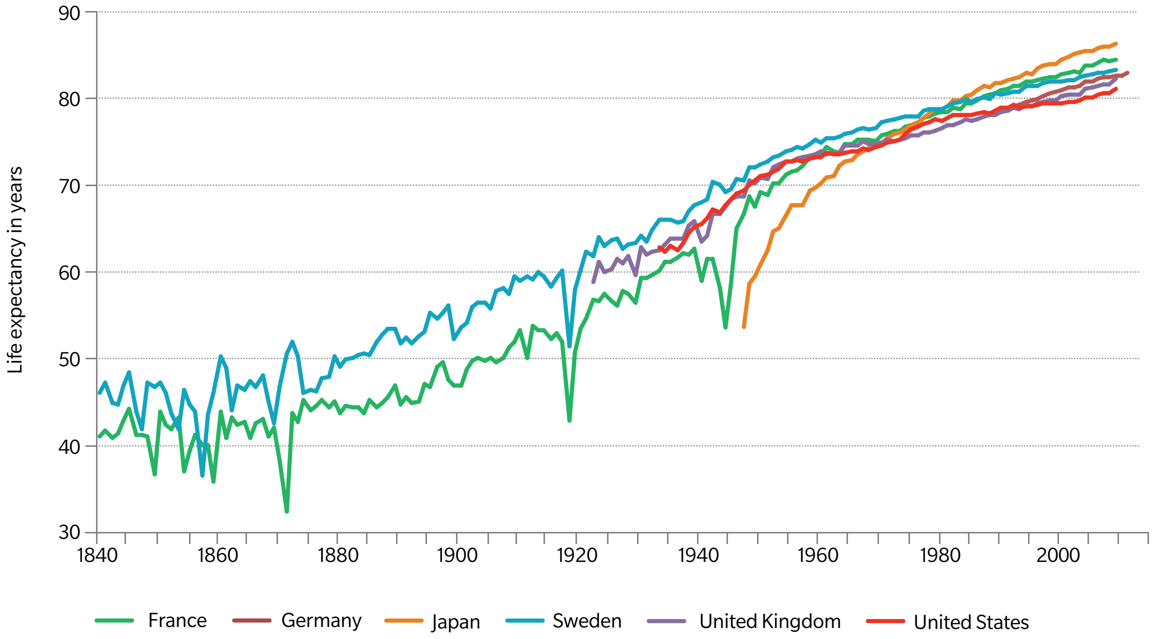
II. LIFE, HEALTH AND LONGEVITY EMERGING RISKS

ADVANCEMENTS IN SOPHISTICATED MEDICAL TECHNOLOGIES, INCLUDING SPECIALTY DRUGS AND INNOVATIVE CURES, COMPOUNDED WITH AN AGING POPULATION ARE CREATING A "CHICKEN AND EGG" SCENARIO THAT WILL CONTRIBUTE TO THE RISK OF HEALTHCARE COSTS EXPANDING AT A MORE GEOMETRIC RATE.

In the last 150 years, dramatic improvements have been made in life expectancy. Some developments such as immunizations for smallpox, polio and measles created quantum improvements, while the proliferation of better lifestyles, clean water and more nutritious diets provided gradual and continuing change.

While most historical life expectancy developments resulted from improvement in children's mortality, in the 20th century, mortality rates declined significantly for older ages.

F-4 | FEMALE LIFE EXPECTANCY IN DEVELOPED COUNTRIES:1840-2009



Source: Human Mortality Database

While this is a tremendous success for humanity as a whole, it changes the economics of working and retiring, of earning and spending and of living in general. It impacts the employers who provide pensions, governments that provide social insurance and public assistance and (re)insurers that provide annuities, disability protection, long term care, critical illness and other lifestyle protection coverages.

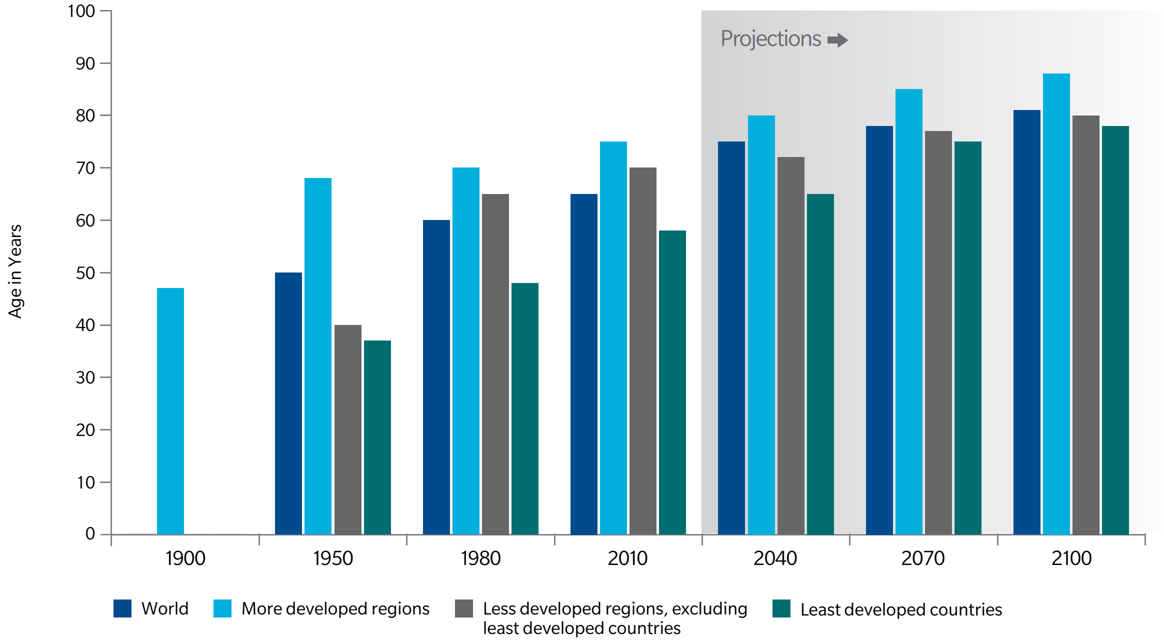
LONGEVITY RISK

The impacts to society from changes in longevity and life expectancy will be wide-ranging and incredibly difficult issues to grapple with.

A 2012 International Monetary Fund (IMF) study revealed that if individuals lived three years longer than expected the cost of aging could increase by 50 percent.

This translates to 50 percent of 2010 gross domestic product (GDP) in advanced economies and 25 percent of 2010 GDP in emerging economies. Globally that amounts to tens of trillions of US dollars. The United Nations expects the aggregate expenses of the elderly will double over the period between 2010 and 2050. The below figure shows the projected trend of rising life expectancy to continue in all regions of the globe regardless of economic advancement.

F-5 | LIFE EXPECTANCY AT BIRTH PREDICTIONS



Sources: Global Financial Stability Report, IMF, April 2012

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

For (re)insurers, increased longevity creates very specific risk, as improvements are notoriously difficult to measure and to forecast. Diversification is challenging if not impossible. For traditional life insurance with death benefits, mortality improvements have been positive for the industry – for both (re)insurers and consumers. However, with an aging population, insurance buyers are transitioning to products with living benefits – annuities and disability insurance to protect income streams and long-term care and critical illness coverage to help meet the expenses of aging and morbidity. For these products, inaccurate estimates of longevity change the economics of the business in significant and potentially overwhelming ways. Mortality and longevity risk are often considered to hedge each other, but the underlying populations are so different that it is difficult to translate that hedge into real risk mitigation.

To illustrate the propensity to underestimate longevity, consider the extreme examples of two defunct insurance markets – the viatical settlement market and stranger-owned life insurance (STOLI). Viaticals were formed to buy policies at a discount from face value from AIDS victims, effectively transforming life insurance policies into living benefits. The viatical had to pay a premium until the policyholder's death and would then make a profit. But due to the innovations in treatment and drug therapies, victims lived much longer than previously expected and virtually all viatical settlement companies eventually went out of business. STOLI investors bought new policies on behalf of groups specifically chosen to have higher mortality than life (re)insurers anticipated in their pricing. Despite this selection, almost all STOLI portfolios performed much worse than expected, losing millions of dollars. These were both speculative businesses, but highlight how difficult longevity risk is to anticipate – even when it is the primary risk specifically underwritten.

Though longevity risk has been a persistent industry issue, we identify it as an emerging risk for two main reasons:

1. The persistent low interest rate environment is magnifying the impact of longevity risk for long-term coverages and,
2. Many (re)insurers will increase their longevity exposure dramatically over the next several years as consumer interest in lifestyle products grows and as pension liabilities are transferred to the insurance sector.

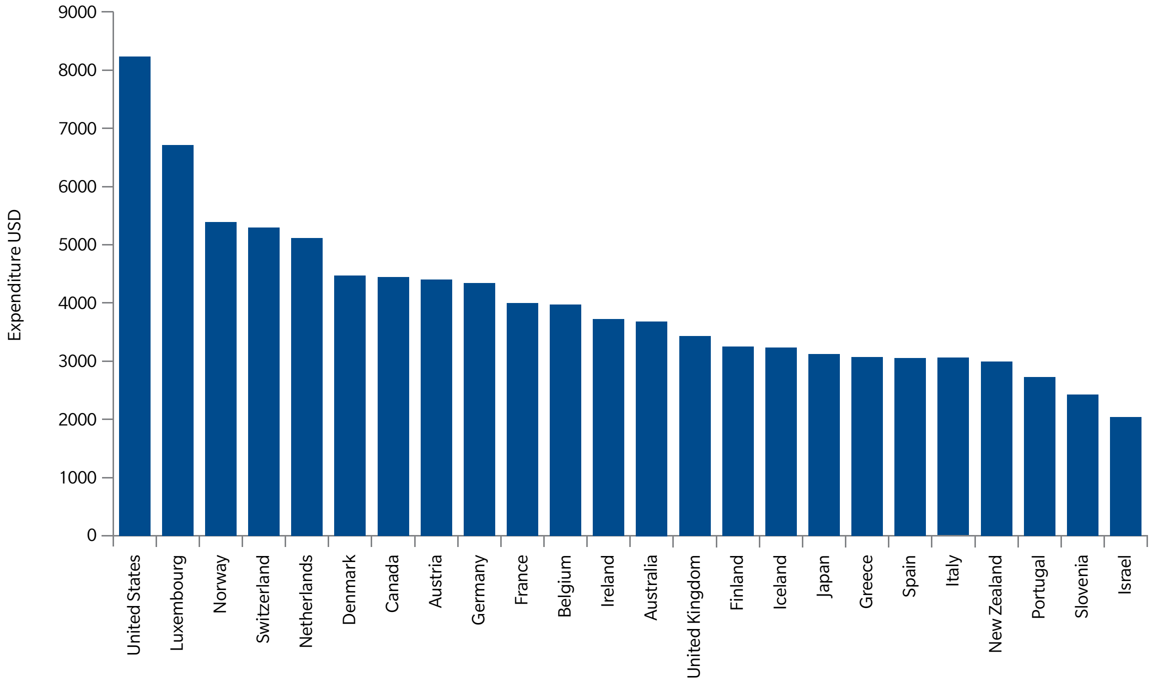
Traditional actuarial forecasting methods extrapolate historical trends into the future, taking into account known changes between the study base and the projected cohort. This has proved adequate for mortality studies, as underlying decreases in mortality have helped projections be sufficiently accurate for death benefit projections, pricing and reserving. For longevity studies, however, that approach, applied simplistically, is practically useless. A more granular method, evaluating the several leading causes of death and their changes over time, taking into account different rates of change by age, gender, risk profile, and several other factors, is better, but still very problematic for reliable modeling.

One reason that modeling is more challenging for longevity risk than mortality risk, is that the quantum events that can move mortality higher (war, pandemic, global catastrophe) are avoided by mankind if possible and, if they happen, still only have a brief impact. The impacted population then typically experiences a long period of recovery, potentially with even lower mortality rates. The events that can move mortality lower in a quantum way (new vaccines, cures for diseases, improved surgical outcomes, greater public safety measures) are highly sought after and, once obtained, create permanent, lasting change in long-term mortality. This drive to survive and thrive is well illustrated by the recent and ongoing shifts in US medical expenses – another important emerging threat.

ESCALATING MEDICAL COSTS

The impact of rising healthcare expenses has been and will continue to be felt around the world, in developed and undeveloped nations alike. Rising healthcare costs are putting a strain on governments worldwide. Nowhere in the world, however, are expenses as high as they are in the United States, where the impact extends into the medical component of workers compensation costs. Although the rate of growth has seen some stability, it still outpaces the US growth rate of inflation. Figure 6 illustrates that per capita spending in the United States in 2010 was over USD8,000. A key driver for higher US costs is that it spends more on hospital care and medical specialists. Hospital costs are 60 percent higher in the United States than in other Organization of Economic Cooperation and Development countries. Spending on the use of specialists is more than two times higher. Forecasters believe this trend will increase.

F-6 | HEALTH EXPENDITURES PER CAPITA: A GLOBAL COMPARISON, 2010



Source: Center for Medicare and Medicaid Services

The US Health Care Cost Institute (HCCI) estimated that in 2013 US healthcare spending rose 3.9 percent per capita per insured. The overall growth rate has stabilized over the past several years, but prices for some services have increased at a faster rate. Hospital spending is on the rise mainly due to hospital consolidation – fewer hospitals leads to higher prices. And spending on the use of specialists has increased by as much as 8 percent.

The cost increases are only expected to worsen. Advancements in sophisticated medical technologies, including specialty drugs and innovative cures, compounded with an aging population are creating a "chicken and egg" scenario that will contribute to the risk of healthcare costs expanding at a more geometric rate.

NEW ECONOMICS ARE CREATING NEW MEDICINE

Through the Affordable Care Act, many measures are being implemented that are expected to have a positive impact on bending the healthcare cost curve downward in the long term. However, the same act removed annual and lifetime limits for medical insurance claims. As a result, the maximum potential loss from a single individual is a new frontier of risk, with new heights being reached each year. This is both a frequency and severity issue.

To illustrate the frequency impact, consider a recent report by Sun Life Financial for its stop-loss business: the number of claims of USD1 million and above increased by 1,000 percent from 2010 to 2013. While there were only two claims in 2010, that number rose to 22 claims in 2013. With respect to severity, the limit for any one person in any year was generally USD2 million prior to 2010. Last year saw multiple claims of more than USD20 million in charges and dozens of more than USD5 million.

With the potential for medical solution providers to earn millions of dollars per patient each year combined with tremendous strides in biotechnology, previously unimagined and uneconomic therapies are becoming not only possible but also potentially pragmatic.

Predictive analytics or predictive medicine uses patient-specific data and enables a more customized, precise approach for patient-specific treatment. With the insight this provides, biotechnology, pharmaceutical and medical device companies can partner to provide better care, improve compliance, lower readmission rates and drive improved outcomes. This can lower unnecessary and ineffective treatments and decrease the overall cost of care. However, taken to an extreme scenario, life science companies could invest in developing much more specific treatments for very small cohorts of affected patients. These focused therapies could be extremely expensive and would be wildly impractical without the intersection of new technology and new economics.

Regenerative medicine is another area undergoing rapid change. Human cells and tissues are being repaired and regrown outside of the body. Three-dimensional printers will create much needed organs for transplant patients using their own cells. Simple organs are already being created. This technology-enabled area of medicine is ground-breaking because it harnesses the body's own ability to heal and can provide potential cures for an enormous array of life-threatening diseases and conditions.

These examples of recent and emerging changes include regulatory, technological and economic disruptive shifts and represent only a portion of the factors affecting any insurer in this space. There is no historical precedent on which to base any forward-looking trends. The impact of these technologies on medical costs in the short term, and on human longevity and reserving in the long term, remains challenging to quantify reliably. However, advances in modeling and analytic methods will provide greater insight than has ever been possible previously.

III. NEW TECHNOLOGIES, NEW LIABILITY RISKS AND EMERGING PRODUCT EXPOSURE

IT IS INCUMBENT UPON INSURERS AND REINSURERS TO HELP ACCELERATE THE COMMERCIALIZATION AND BENEFITS OF THESE INNOVATIONS TO SOCIETY. AT THE SAME TIME, IT IS CRITICAL TO THOROUGHLY UNDERSTAND AND MANAGE THE RISKS.

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

Risk is a major barrier to innovation. Taking a risk, however, is almost always the first step in any type of progress. The productivity of the global economy depends on companies that are willing to find new and better ways of doing things despite the potential perils involved. If they start to be ruled by fear of liability, our global development could be in jeopardy. By helping businesses manage the risks associated with product development, (re)insurers play an important role in stimulating innovation and helping our world move forward in positive ways. From the early days of marine exploration, to the first satellite launch, to the development of state-of-the-art technologies, (re)insurers have provided a critical safety net that has supported and encouraged the creative process. Given the continued transformative potential of emerging technologies such as nanotechnology, 3-D printing, aerial drones and self-driving automobiles, and their applications in virtually every industry, it is incumbent upon insurers and reinsurers to help accelerate the commercialization and benefits of these innovations to society. At the same time, it is critical to thoroughly understand and manage the risks.

In the examples that follow, we focus on technologies that are considered to have wide benefits and for which there are both strong underlying commercial pressures for development, as well as high levels of societal concerns about potential risks and adequate privacy, safety and regulation based on foreseen and unforeseen risks. (Re)insurers then need to attempt to quantify their downside exposures so they can price the foreseen and unforeseen risks correctly and set aside adequate capital to pay future claims; each of which require certain assumptions to be made. Examples of the challenges for each are:

- Foreseen (known) risks – leakage of pollutants or harmful substances caused by the difficulties of proper containment. In modeling, these can be quantified based on similar events in past history.
- Unforeseen risks - the possibility of undesirable misuse of applications or effects that cannot be anticipated at the time of invention. These are problematic risks to model because the quantum is unknown at the initial point in time.
- Both of these risks are made more acute by the rapid speed and complexity of technological development. The growing complexity of new technologies makes them more difficult for individuals, regulatory bodies and (re)insurers to grasp and adequately contemplate.

I. NANOTECHNOLOGY: THE PLASTICS OF THE 21ST CENTURY

Many scientists view nanotechnology as the revolutionary technology of the 21st century. Just as plastics were a pervasive and revolutionary product of the 20th century, nanotechnology products are having widespread use and change our lives in a myriad of ways. This technology has quickly evolved into a global force that is transforming manufacturing, medicine and an ever increasing number of consumer/food goods. The field has become a worldwide market worth an estimated USD1 trillion and is projected to grow at a rate of 16.5 percent through 2020.[15]

Nanotechnology is a generic term for applications that work with matter that is so small that it exists in the atomic and molecular realm. At this size, the substance's physical, chemical and biological properties are different from what they were at the micrometer and larger scales. By harnessing these new properties, researchers have found that they can develop materials, devices and systems that are superior to those in use today and that enhance our lives in almost limitless ways. Nanotechnology currently is being used to strengthen the material used in golf clubs and bicycle frames, to create stain- and water-repellant clothing and to produce wear-resistant paints and coatings. Table 3 illustrates some of the industries and hundreds of consumer products in which nanotechnology is already in use - ranging from automotive, chemical, electronics, medicine and textiles.

[15] MarketWatch Inc.

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

T-3 | NANOTECHNOLOGY INDUSTRIAL APPLICATIONS

Automotive Lightweight construction; catalysts and painting, tire sensors, windshield and body coatings	**Chemical** Fillers for paints, composite materials, impregnation of papers, adhesives, magnetic fluids
Construction Materials, insulation, flame retardants, surface coatings, mortar	**Cosmetics** Sunscreen, lipsticks, skin creams, toothpaste
Electronics Displays, data memory, laser diodes, fiber optics, optical switches, filters, conductive and antistatic coatings	**Energy** Lighting, fuel cells, solar cells, batteries, capacitors
Engineering Protective coatings for tools and machines, lubricant-free bearings	**Environmental** Environmental monitoring, soil and ground water remediation, toxic exposure sensors, fuel changing catalysts, green chemistry
Food and Drink Packaging, storage life sensors, additives, juice clarifiers	**Household** Ceramic coatings for irons, odor removers, cleaners for glass, ceramics and metals
Medicine Drug delivery systems, contrast medium, rapid testing systems, prostheses and implants, antimicrobial agents, in-body diagnostic systems	**Sports** Ski wax, tennis rackets, golf clubs, tennis balls, antifouling coatings for boats, antifogging coatings for glasses and goggles
Textiles Surface coatings, "smart" clothes (anti-wrinkle, stain resistant, temperature controlled)	**Warfare** Neutralization materials for chemical weapons

Source: Project on Emerging Nanotechnologies in the Science and Technology Innovation Program at the Woodrow Wilson International Center for Scholars, in collaboration with the Virginia Tech Center for Sustainable Nanotechnology.

As with practically all scientific breakthroughs, nanotechnology carries both risks and rewards. While it appears almost certain that the rewards will greatly outweigh the risks, attention must be paid to possible dangers to the well-being and the potential of human latent bodily injury from this new technology. The Project on Emerging Nanotechnologies grouped products according to their potential exposure pathways into the human body from a theoretical perspective, and according to each product's intended use. Based on the study, the number of consumer/industrial products that had the potential for resulting in bodily injury and occupational disease via transdermal, ingestion and inhalation exposure are 496, 129 and 212, respectively.[16]

As optimistic as researchers may be, however, responsible decisions must be made regarding nanotechnology's development and use. Growing evidence suggests that nanoparticles – the basic building blocks of nanotechnology and the tiniest materials ever engineered and produced – may pose environmental, health and safety risks. As such, it appears that the industry is currently caught between stages 2 and 3 of the insurance coverage cycle below:

1. Early study period, currently underway, where insurers and reinsurers study the issue
2. Fear phase, frequently accentuated by unfounded but terrifying rumors. This stage is expected to be short, given the generally benign nature of nanotechnology products
3. Mature phase, where cover routinely is provided either within conventional products or on a standalone basis.

[16] *Nanotechproject.org.*

The (re)insurance industry has a major role to play in helping society capture the benefits of this technology by helping to spread the risks. As it stands today, most global (re)insurers do not differentiate or exclude risks from nano-products. As a result, many in the industry acknowledge that insurance policies and reinsurance agreements in place may already be covering these risks. Rating agency, A.M. Best, in its 2013 briefing, "*Emerging Technologies Pose Significant Risks with Possible Long Tail Losses*," identified the immediate as well as long latent concerns of nanotechnology – even going as far as equating its potential industry impact to asbestos. Nanotechnology risks are covered under a wide variety of covers, including general liability, products liability, workers compensation, professional liability, employment practices liability and directors and officers liability, exposing a broad swath of the industry.

Consequently, if the (re)insurance industry is to continue to support the myriad positive uses of nanotechnology while not incurring major long-term losses, it must have a thorough understanding of how nanomaterials are produced, stored, used and discarded. In addition to the identification and modeling of nano-product accumulations (and their subcomponents throughout the supply chain) on a property/casualty (P&C) portfolio basis, it also is essential for carriers to monitor, manage and control their own exposures. Since losses from nanotechnologies have not materialized, carriers will need to contemplate and integrate an exposure-based modeling approach. Otherwise they could be accumulating multiple years of losses and reserves emanating from the next asbestos-like scenario on their books without realizing it.

As is the case with most emerging areas of risk, nanotechnology challenges insurers and reinsurers with many unknowns. These challenges are further complicated by the fact that few risk-related forecasts have been scientifically confirmed. Many industries are extremely optimistic about the opportunities associated with nanotechnology. If they are not currently exploring its potential, they are likely to do so in the very near future. Because (re)insurers play such a critical part in enabling new and beneficial technologies, it is essential that they work together with manufacturers, the government, scientists and regulatory agencies to identify and quantify nanotechnology's risks. Public response to this new technology, as well as the legal climate, will depend upon how much accurate information is available.

II. THE DAWN OF THE DRONES: THE EVOLVING OPPORTUNITIES AND RISKS OF UNMANNED AERIAL SYSTEMS AND DRIVERLESS CARS

The overall rise of connectivity to a growing number of physical objects will entail additional emerging risks to individuals and companies. Examples include:

- Unmanned Aerial Systems (UAS or drones)
- Driverless vehicles
  - Trains are already in use in London and New York
  - Self-driving cars may soon become more and more prevalent.

If these technologies are implemented and regulated properly, they can lead to notably higher productivity and standards of living. However, if they are not, and the technologies are carried out on a massive global scale and subject to widespread misuse, the consequences could be catastrophic. This would clearly impact the balance sheets of (re)insurance companies and these possibilities need to be considered if these products are to be insured.

UAS/DRONES

Growth projections for the drone or UAS sector are nothing short of phenomenal, as the opportunities and advantages afforded by using this type of machinery in construction, agriculture, energy/utilities, mining, real estate, news media, film production and public safety become increasingly more apparent each passing day. Nevertheless, the potential economic benefits are considered to be vast, expecting to generate an estimated economic benefit of USD82 billion along with 100,000 jobs by 2025.[17] This rapid increase in the number of drones is prompting concerns for:

- Heightened collision risk for commercial airplanes as reports of drones in close proximity continue to make the headlines in the United States and the United Kingdom
- Privacy concerns from remotely controlled autonomous UAS equipped with cameras
- Increased concern of drones being hacked or used as weapons by terrorists.

These are all real risks that need to be addressed by both regulatory agencies and the (re)insurance industry.

Regulators around the world had initially struggled to embrace and regulate this new UAS technology. In regions without adequate oversight, there would be an increased risk for collisions and accidents, thereby resulting in greater loss frequency and severity for (re)insurers. However, some progress is finally being made, as regulators weigh the potential benefits of using drones against issues surrounding public safety, privacy and national security. This is mitigating some of the worst case scenarios in play right now.

Meanwhile, the insurance industry is responding to demand at its own forward-looking pace. (Re)insurers are using their experience of the manned class to assess the risk and/or limit their exposure by selection against size, uses and values of the aircraft, or the type of coverage offered. In March 2015, a Bloomberg article titled "Insurers Step Up for Drone Pilots Unwilling to Wait on FAA Rules" noted that US-based companies interested in UAS operations are obtaining coverage from insurers that are writing their own safety rules for insureds. Despite the US Federal Aviation Administration (FAA) announcing that it intends to issue final regulations for small commercial UAS/drones by mid-2016, until which time none are supposed to fly without a formal waiver, the article stated that several US insurers are already writing policies for drones across the country. The FAA has been highly accommodative to commercial unmanned aircraft operations in US airspace through the granting of over 1,000 Section 333 exemption approvals.

[17] *The Economic Impact of Unmanned Aircraft Systems Integration in the United States, April 2015.*

This exemption provides authorization for certain unmanned aircraft to perform commercial operations. The FAA has also increased the issuance of "blanket" Certificates of Waiver Authorizations for new and novel approaches for inspecting power grids, railroad infrastructure and bridges. UAS risks that can be covered in the market include:

1. Physical loss to UAS/drone itself (airframe, propulsion, operating system, flight controls)
2. Payload (camera equipment, sensors, packages)
3. Ground station control unit
4. Spares and transit coverage
5. Fraud and theft
6. Third party liability (bodily injury and property damage)
7. Product liability (re-seller or manufacturer).

Drones have the potential to become one of the biggest risks for insurers, but also one of the most significant product development areas due to the rapidly expanding usage by companies, as well as the public. Although the insurance industry has begun covering these risks, many manufacturers (some of which are emanating out of less regulated markets such as China) may not be adequately covered. This was evident with Chinese drywall manufacturers who did not have adequate coverage for construction defect. The result was that their liability was shifted to the US-based contractors and distributors. Similarly, we see that the emerging risks associated with UAS and drones will involve highly complex liability scenarios that could encompass all aspects of the global UAS/drone manufacturing and service provider supply chain.

SELF-DRIVING AUTOMOBILES

Technologies that we may take for granted today such as anti-lock braking and airbag systems, driving and parking assistance, hazardous condition traction control and global positioning system routing, may soon all come together and evolve into fully autonomous self-driving automobiles. Self-driving cars are expected to begin commercial production and be in use by 2017. Google, the pioneer in the field, claims it can cut road accidents by eliminating the human driver who gets distracted by text messages or becomes tired. Although safety and efficiency gains have been the most cited and prominent benefits for the rationale for the development of self-driving automobiles, a considerable number of challenges remain.

Different types of technology will be operated in parallel to existing transportation options during their gradual implementation phases. Some key questions that arise are:

- How will autonomous cars interact with human drivers on the road?
- Who will be liable in autonomous car crashes?
- How quickly will the personal liability of the driver shift to the product liability of the manufacturer?
- What if automated systems fail to deliver or simply stop working?
- Will humans be available and have the skills to take over control again as needed?
- What are the increased data/privacy concerns as more sensors and recording devices are used in these vehicles?

It is also possible that some industries or parts of the population will reject this new technology, for economic or privacy reasons or simply a preference. Assuming regulators facilitate wide use of self-driving vehicles and the public accepts them, the speed of their implementation will depend on costs (including insurance), production capacity as well as the pace of transitioning away from current transportation systems. Relative to UAS/drone commercial implementation over the next 10 to 25 years, the shift to fully self-driving cars is expected to be much more gradual, impacting some transport segments quicker than others.

The inevitability of wide-scale autonomous mechanisms including UAS/drones and self-driving cars should not be underestimated. As with any opportunities brought about by advances in technology, they go hand-in-hand with a set of new and little understood risks, to which operators, regulators and the (re)insurance industry are all currently trying to comprehend, embrace and adapt.

Currently there are insufficient precedents set in terms of data, claims and overall knowledge in order to enable underwriters to accurately assess the numerous risks involved in autonomous vehicle operations. However, over the next few years, this data will eventually be generated (beyond these machines and their performance reliability) the hard way – via the emergence of complex litigation, insured and uninsured losses, albeit initially, at the smaller end of the scale.

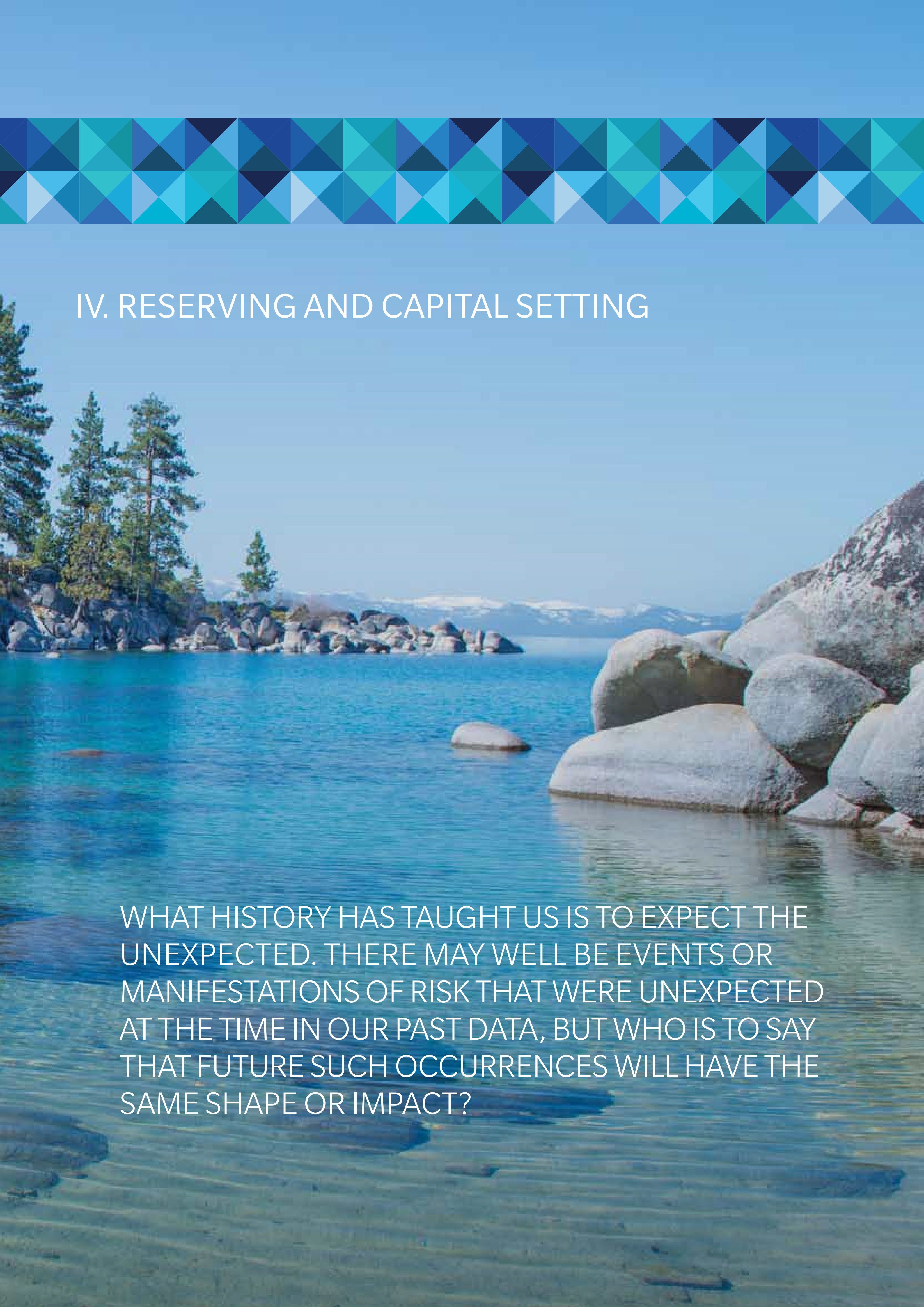
TRACKING AND MODELING NEW INTEGRATED, INTRICATE TECHNOLOGY RISKS

Casualty (re)insurers do not cover standalone emerging risks. A product defect (with recall) or a latent bodily injury resulting from new technological nano-products or UAS risks, could lead to class action lawsuits and ultimately large liability claims including products liability as well as professional liability. This emergent reality, however, is difficult to address. A carrier would need to identify and model several possible epicenters of a liability chain reaction and follow their rapidly spreading implications throughout a portfolio. Without new powerful casualty modeling capabilities as well as highly granular data on the products and subcomponents that each of their insureds manufacture and sell globally, this process would be time-consuming, impossible to complete and likely to miss key threats and underlying exposures.

Because of the complexity and uncertainty involved regarding new technology risks, the degree to which carriers have advanced their risk management practices in this regard notably varies. Until recently, they tended to manage technology liability risks independently and assume the integrated risks either knowingly – or sometimes unknowingly. It is essential that these catastrophe risks be identified, prioritized, accumulated and modeled in their entireties in order for their enterprise level implications to be properly understood and hedged. Recommended steps include:

1. Locate areas of vulnerability to catastrophic technology risk in a portfolio
2. Identify products-centered catastrophe mechanisms and determine how they operate within a portfolio
3. Stochastically model major exposed product-based scenarios having substantial multi-line catastrophe/clash loss potential
4. Formulate a risk management plan to address the full reach of the various scenarios identified.

Ultimately, identifying, managing and modeling technology-based risks require a systematic approach. Those various approaches may differ according to the data they require or by the scenarios being considered as well as any methodologies being contemplated. Some are centered on historical loss experience, yet others are much more exposure-model-based.



IV. RESERVING AND CAPITAL SETTING

WHAT HISTORY HAS TAUGHT US IS TO EXPECT THE UNEXPECTED. THERE MAY WELL BE EVENTS OR MANIFESTATIONS OF RISK THAT WERE UNEXPECTED AT THE TIME IN OUR PAST DATA, BUT WHO IS TO SAY THAT FUTURE SUCH OCCURRENCES WILL HAVE THE SAME SHAPE OR IMPACT?

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

BACKGROUND AND CHALLENGES

Loss reserves are arguably one of the most difficult risks to estimate and monitor. In fact, inadequate pricing and deficient loss reserves have been the leading cause of P&C company impairments. According to A.M. Best, from 1969 to 2009 they triggered approximately 40 percent of all impairments – four times more than those emanating from natural catastrophes.[18] There are many uncertainties in managing long-tailed, heavily legislated lines of business that can be triggered from emerging risks. Unforeseen inflation and anticipated legislative changes over a 10 to 30 year period present many demands. In order to prepare for emerging risk scenarios, future trends and related uncertainties need to be explicitly identified, contemplated and estimated.

The concept of emerging risks is not a new one in the context of (re)insurance; the market has always faced some new challenge as the world around us has changed. Aviation, for example was once considered an emerging risk. Now, it is well understood and the market for risk transfer has been operating for decades. The same will inevitably come to pass for many of the risks discussed in this report. The question is how to try and quantify them and then manage them now while they are less understood.

Reserving has always been the realm of actuaries and the strapline for the actuarial profession for a long time has been "Making Financial Sense of the Future." This ambition to make sense of the future is particularly challenging in the context of reserving and capital setting for emerging risks. Most commonly used reserving techniques rely on the projection of patterns in past data around how claims arrive and are estimated and then paid, to infer what we need to set aside now to meet all of our liabilities. That is perfectly sensible if the past is a good guide to the future. But, in the case of emerging risks, it really is not. What history has taught us is to expect the unexpected. There may well be events or manifestations of risk that were unexpected at the time in our past data, but who is to say that future such occurrences will have the same shape or impact? New and more sophisticated techniques and tools go beyond commonly used reserving methods of the past. Generalized linear modeling (GLM) techniques and tools (such as those incorporated in Guy Carpenter's MetaRisk® Reserve™) can assist in detecting the emergence of new inflation trends as well as other disruptors early on. These tools allow (re)insurers to dynamically stress-test changing inflation scenarios and other emerging claims drivers. Then, capital should be set at a level to mitigate against such surprises and protect the balance sheet.

For many emerging risks discussed in this report the tail will be long so the capital will likely be largely contained in the reserving risk category. Most reserving risk assessments, including those that are incorporating the relatively new GLM techniques, still rely on the use of past data with the associated issues this presents. For these reasons we need to look beyond the traditional actuarial tool kit for solutions.

SIZING THE PROBLEM

There are three main questions to be tackled in sequence:

1. Which emerging risks potentially expose my company?
2. What means do I have to quantify those risks?
3. How are these risks likely to crystalize?

This framework provides an opportunity to categorize risks, identify gaps and decide if, and how, they can be closed. It also offers a way to understand how the financial consequences could become apparent.

[18] A.M. Best Special Report: 1969-2009 Impairment Review.

IDENTIFYING EMERGING RISKS

There are many reports and publications including this one that list and describe emerging risks. These can be helpful but are not some sort of panacea in the identification of risks that could be harmful to (re)insurers. Many risks may not be applicable; the list may not be exhaustive and, of course, will never contain the "unknown unknowns."

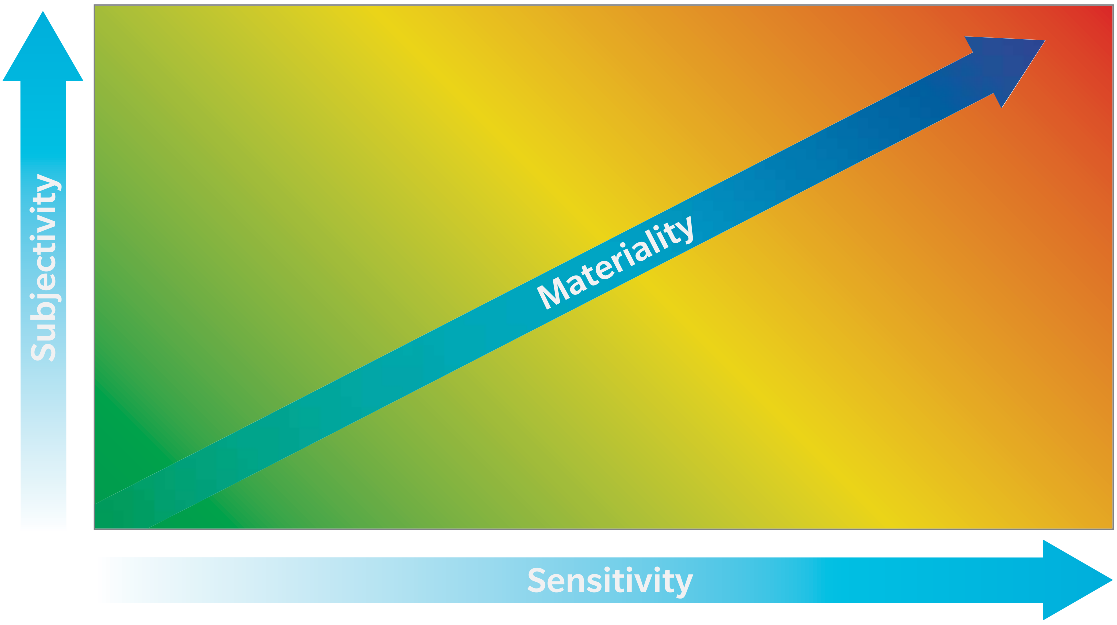
Fortunately, there has been work done on the identification of non-modeled risks in the catastrophe modeling space that can be of use here. The Association of British Insurers in the United Kingdom, in conjunction with the industry, published a report in April 2014[19] detailing a guide to tackling the issue of non-modeled perils. Although the paper focuses necessarily on natural perils, the framework can be adapted to consider emerging risks. The paper advocates an identification process which considers:

- Exposure-based techniques to analyze current and planned exposures
- Claims-based techniques to leverage knowledge contained within existing data
- Expert judgment to gather the opinions of experts for further analysis.

Clearly it is critical to understand the lines of business written to recognize the risks but it is also vital to comprehend the coverage provided for these classes in detail. This may require a detailed analysis of policy wordings, both current and historic, to consider exclusions and coverage scope. It also necessitates a rigorous examination of areas where contracts are silent on coverage because this could lead to implicit inclusion, or at the very least, contract disputes.

Past claims can be of some use. If a risk is indeed already emerging it may be possible to infer trends and make forward-looking projections. Historic data can also be used to identify claims that were unanticipated at the time of writing the business to try to quantify a level of latency associated with different lines of business. It can also be educational to ascertain linkages between lines of business. But, as mentioned before, the past is not necessarily a good guide to the future.

Expert judgment has to be used in the case of emerging risks because, by their very nature, data will be sparse. Not many companies will have the resources or indeed find it practical to have a dedicated group of experts locked in a cupboard with the sole purpose of dreaming up emerging risks and their potential consequences. Most will seek views from experienced claims and underwriting personnel using the latest lists of emerging risks contained in publications, as well as any risks they believe are not captured to elicit their perspective on the likely impact to the business.



[19] Association of British Insurers: Non-Modeled Risk, April 2014.

As with any risk identification process one should always have materiality in mind. The list of potential risks may be long so construction of a ranking system can be helpful through the use of materiality matrices. Those risks whose quantification is highly subjective and for which financial results are highly sensitive, should rank highly and receive a much more in-depth assessment.

QUANTIFYING EMERGING RISKS

Once the risks have been identified and ranked, the next step is how to quantify the likely impact on the financial results of the firm. The first and most obvious question is what available quantification techniques are available for each risk on the list. This will depend on the availability of relevant data and commercially produced models.

Where claims or external market data is available the likelihood is that the timespan of datasets will be limited. In this case standard actuarial reserving techniques can exacerbate the problem as there potentially will be no tail to construct a chain ladder-type exercise fully. Looking carefully for any calendar year trends in frequency or severity of claims will pay dividends, as will talking to claims professionals about the likely uncertainty surrounding individual case estimates and obtaining their views on duration to settlement.

For some risks, models may be commercially available. So what do these models typically offer? Well, in short, they might provide the sort of information expected from a catastrophe type model, such as loss amounts with associated return periods and, in some cases, a view on the correlation between lines of business. This helps with best estimate reserving by using the Average Annual Loss (AAL) as an initial loss pick and for capital modeling by using a statistical benchmark such as the 1-in-200 net of reinsurance Value-at-Risk (VaR) amount. What they do not provide in most cases is an estimate of the likely emergence pattern of that risk. This is important for casualty lines and so this is currently a large missing piece of what is a complex jigsaw puzzle.

While these models are helpful as ever, care needs to be taken in their use just "off the shelf." They are all fairly new in their construction and so one must ask:

- What is the data source?
- How has the data source been used in model construction?
- What are the key model assumptions?
- Is expert judgment used in the model methodology or parameterization?
- How are dependencies introduced and parameterized?
- Is my data good enough to produce reliable results?
- How sensitive is model output to the data input and changes in the core assumptions?

Fortunately, these should all be familiar questions as they all need to be addressed whenever using an external model. However, as these models are in their relative infancy, much more care is needed in this validation exercise. Also, it is likely new data and therefore new model versions will follow in the footsteps of the first models quickly as new information emerges. This means results can be volatile as models evolve; so a robust model change policy will be required.

Data quality and availability should also be examined in depth. Because the risks are new, the data may not be captured correctly to power the model, which will lead to further uncertainty and may even preclude the use of a model altogether.

There will be risks on the list for which there is no data and no available model. This absence of information does not mean the industry can just ignore these risks, particularly if they are highly ranked in terms of materiality. Companies do not need to resort to "finger in the air" estimates when they can leverage expert judgment. The use of expert judgment has become much more robust in recent years with the advent of Structured Expert Judgment (SEJ). In fact, SEJ has been used for quantifying many hard to analyze risks such as estimating the probability of volcanic eruptions and cyber aggregations. The process involves taking a panel of experts through a series of interviews to get loss scenarios and estimates of loss quantum and likelihood. These results are used as data points to create a pseudo PML curve which will have a mean estimate for each scenario and also provide a range of estimates which can inform uncertainty.

When it comes to casualty catastrophes or indeed any emerging risk that can be systemic in its effects, it is crucial to consider correlations and dependencies. This is where past data again is not always that useful. While events from emerging risks are scarce in past data for individual lines of business, the instances of a conflagration across lines of business in terms of liability with a simultaneous impact on assets are virtually non-existent. Whatever dependency structure is assumed within an external model or the internal capital model (whether copula-based, using correlation matrices or a risk driver approach) it should be capable of being stressed to reflect that the future could be more unusual than the past.

The key issue in modeling is the timescale over which we realize that the risk is manifesting itself and how this view changes until an ultimate understanding of the loss quantum is reached and all liabilities are discharged. This is the missing dimension from most models but why does it matter? Well, for a natural catastrophe the event usually happens quickly, can be estimated fast and is settled swiftly. An emerging or latent risk can lurk in the balance sheet undiscovered for a long time. Even when discovered it can take even longer to comprehend the full extent of the loss. The best historic example is the liability from exposure to asbestos. The reserves have crept up and up, been impacted by various judicial decisions and are still not fully concluded in many cases and jurisdictions. It could be presumed that as long as there is an estimate about the potential overall quantum of loss, and capital is held to back that ultimate liability at inception, then it should not really matter whether the realization of the loss is tomorrow or 20 years in the future. But, that would be wrong as we now explain.

THE CRYSTALIZATION OF EMERGING RISKS

As discussed in the Executive Summary of this report, the term "crystalization of risk" refers to the timescale over which we realize that the risk is manifesting itself and how this view changes until ultimate understanding of quantum is reached and all liabilities are discharged. The "Reserving Risks" section in last year's report, *Ahead of the Curve: Understanding Emerging Risks* looked at how information emerges in the presence of reserving cycles. The profit or loss in any particular financial year is made up of not only the profit or loss from the same accident year but also any recognized changes in the reserves on prior years.

A big movement in prior year reserves in any one financial year particularly from an unanticipated source of risk can cause a sharp drop in share price and an increase in regulatory scrutiny. In addition a small drip, drip of increasing reserves in consecutive financial years can also make shareholders, analysts and regulators nervous about where the deterioration will stop and question whether they can have any confidence in a company's reserving process.

Such reserving increases can certainly erode the available surplus but should they also lead to a reexamination of the required capital, as they can be an additional item of information that would have changed the perspective at the time the capital was set? This is a somewhat philosophical question; a company can set capital aside initially to protect against extreme eventualities akin to a certain amount of water in a bucket, then someone trips and spills half the contents of the bucket due to something everyone thought was unlikely to happen. Does it make one think there should have been a bigger bucket when one sees what is left?

In a Solvency II world, capital (the solvency capital requirement (SCR)) is set as the change in a firm's own funds (assets less liabilities) at a 99.5% confidence level over a 1-year time horizon. Setting this out as an equation, it looks like:

$$\text{SCR} = \text{Change}\ (A - L)\ @\ \text{VaR}\ 99.5\%$$

Expanding the L (in Solvency II, liabilities are actually the sum of the Best Estimate and the Risk Margin), the equation becomes:

$$\text{SCR} = \text{Change}\ (A - (BE + RM))\ @\text{VaR}\ 99.5\%$$

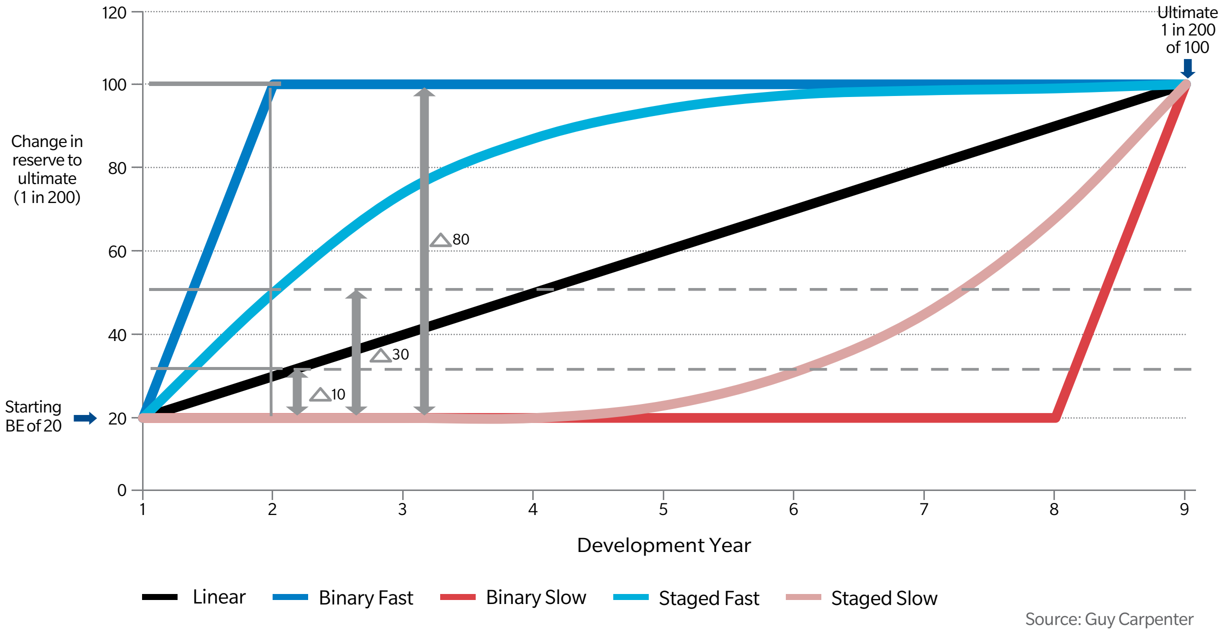
The Risk Margin is actually defined as an amount that a third party would require in order to accept the transfer of the liabilities over and above the best estimate. This is effectively the cost of the capital required to run-off the portfolio (i.e. the sum of the future SCRs calculated at each future point in time until the portfolio is fully run-off and discounted back at the risk-free rate).

So, roughly translated, the SCR is actually a reflection of how much surplus can change in a year, which in turn, is influenced by a firm's view of risk at each point in time. For emerging risks that view can change fast, and presents issues as to how it should be reflected in the calculation of the risk margin and hence the SCR.

The discounting implicit in the Risk Margin calculation can be influential for emerging risks as well. What if a known or suspected risk is long-tailed but there is uncertainty in the way that it is likely to run-off? The model suggests that the ultimate 1-in-200-year loss is 100. However, it does not show either when that 100 could manifest itself or what inflationary influences may act on that 100 if it is presented in today's values but may settle way into the future.

The chart on the next page attempts to illustrate this issue. Suppose the best estimate is 20 and the assessment from modeling is that the 1-in-200-year ultimate loss is 100. If all else stays the same and with the simplifying assumption that the yield curve stays flat, one can say that the sum of the 1-year SCRs approximated the difference between 100 and 20 (i.e. 80). Yet, because of the discounting, when in time the change in own funds is recognized, is important. The black line represents a linear recognition pattern so the 1-year SCRs are all equal with increments of 10. The blue line represents a Binary Fast recognition so the first year SCR is 80 and the remaining years' SCR are zero. This means that the deterioration is recognized quickly. The red line again shows binary recognition but with a slow pattern as the movement is only occurring toward the end of the liabilities' life. The two curves in light blue and light red represent less severe versions of the binary forms.

F-7 | RECOGNITION PATH TO THE 1 IN 200 ULTIMATE POSITION



Source: Guy Carpenter

Consider which lines of business could have these sorts of recognition patterns. The Binary Fast line is analogous to property cat for example. The loss would be known and reserved for in a short space of time so the one-year change in own funds would be large and thereafter would be zero or minimal. The linear recognition line could be representative of an annuity business with a creeping change in longevity assumptions as improving mortality tables are released each year. The Binary Slow line could equally apply to some sort of life time annuity provision where there was a one-off, overnight huge medical advance such as a cure for cancer. Most types of business will be something in between the envelopes provided by the staged-fast and staged-slow curves.

The table below shows a simplified example of how the recognition of the journey to 100 makes a difference to the value of the risk margin when the two recognition extremes Binary Fast and Binary Slow are examined using a flat risk-free yield curve of 3 percent.

T-4 | JOURNEY TO 100

Recognition year	Binary fast one-year change	Binary fast cost of capital (@ 6%)	Binary fast discounted cost of capital (@ 3%)	Binary slow one-year change	Binary slow cost of capital (@ 6%)	Binary slow discounted cost of capital (@ 3%)
0	0.00	0.00	0.00	0.00	0.00	0.00
1	80.00	4.80	4.66	0.00	0.00	0.00
2	0.00	0.00	0.00	0.00	0.00	0.00
3	0.00	0.00	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.00	0.00	0.00
6	0.00	0.00	0.00	0.00	0.00	0.00
7	0.00	0.00	0.00	0.00	0.00	0.00
8	0.00	0.00	0.00	80.0	4.80	3.79
Total	**80.00**	**4.80**	**4.66**	**80.0**	**4.80**	**3.79**

Source: Guy Carpenter

For Binary Fast, the effect of discounting is minimal, taking the cost of capital from 4.8 down to 4.66. For Binary Slow, it is much more significant, taking it to 3.79, which represents a 21 percent reduction.

The point of this simplified exercise is to illustrate that for emerging risks it is very unclear exactly how they will be recognized. Subsequently, as well as quantum we need to consider timing carefully, as this can be influential on the size of the risk margin and hence surplus.

CONCLUSION

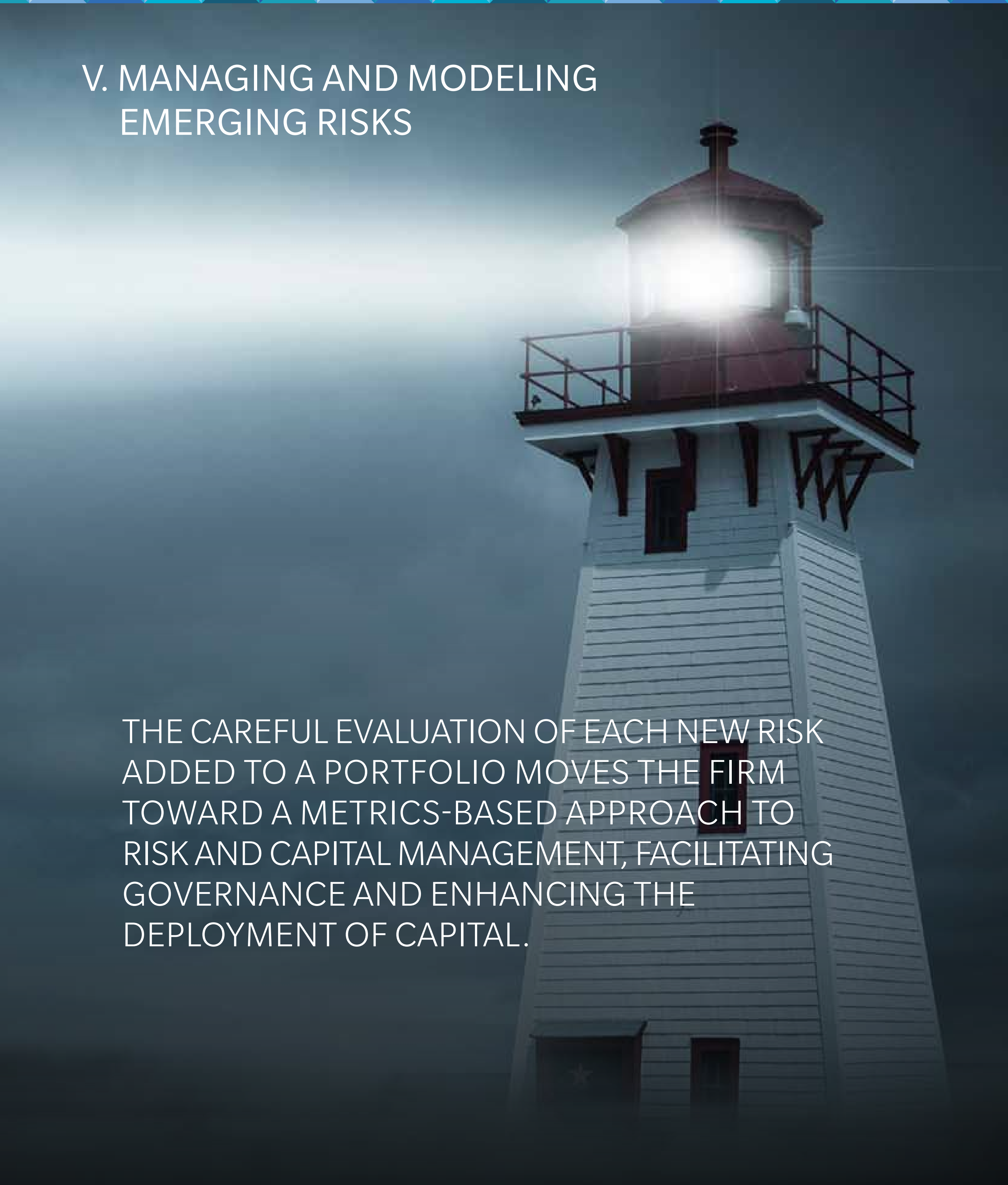
The obvious response to the issues emerging risks provide is to make sure reserves and capital position are more than robust enough for any eventuality – however remote – and then release them when the risks fail to materialize. But, there are many arguments against this as a practical strategy:

- Best estimate reserves are meant to be just that – a "best estimate" without any margins at least in a regulatory sense.
- Holding reserves or capital much higher than necessary in most instances can put a firm at a commercial disadvantage to its peers both from a pure results perspective (unless the upside or releases are consistent over time) and from a return on capital perspective.
- With these sorts of risks, which can have a long period of latency, it may never be clear when it is safe to release reserves or capital held.

A more pragmatic approach is to follow the advice provided here. Identify the risks, rank them in terms of materiality, quantify them if possible, create loadings where it is not possible, be mindful of recognition patterns and stress the impact of changing initial assumptions.

Finally, models for emerging risks are in their infancy but are likely to improve rapidly over time where demand is present and data becomes available. Eventually some emerging risks can become business as usual if the past is anything to go by.

V. MANAGING AND MODELING EMERGING RISKS



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 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. Furthermore, the various disaster scenarios with which carriers are being increasingly confronted needs to be prioritized and synthesized within their enterprise risk management (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, 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 technological category. Here, new data and modeling applications are being synthesized and adapted within existing model frameworks allowing carriers to better underwrite and manage these risks. Other applications involve the identification and quantification of emerging "aggregating" exposure concentrations such as those resulting from global supply chain dynamics. 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 property 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 credible views of overall risk and the ever increasing number of emerging perils and cat risks.

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, 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 typically been the industry practice.

However, as the level of sophistication and tools for deterministic modeling capabilities increases, the next question that arises involves the more challenging leap toward a more probabilistic and holistic model approach. It is important to note that the A.M. Best rating agency introduced deterministic casualty catastrophe loss scenario modeling questions into its 2014 Supplemental Rating Questionnaire (SRQ). A.M. Best defines casualty catastrophes as "events, activities or products that result in a number of lawsuits from multiple plaintiffs alleging damages that impact multiple insureds, coverages and/or time periods." Scenarios need to be identified uniquely by each carrier based on what it views its exposure to emerging casualty risk(s) to be. The expectation is that more sophisticated data, modeling and responses will be required going forward.

The availability of essential insured-level data on emerging and casualty catastrophe risks remains an important challenge that many carriers continue to work toward 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 requires exposure data related to the particular industries covered by their insureds within the portfolio. The variety of models that is beginning to emerge in this area differ according to the data they require, the approach taken as well as the specific scenario set(s) on which the development is focused. Some are taking a highly granular, data-intensive, bottom-up approach; whereas others may be contemplating a more general top-down attitude to the exposure data required. Some are loss experience-based and are considering an integrated historical event set, yet others are much more exposure-based.

The exposure-based models (such as Praedicat's CoMeta™) are dependent on generally accepted scientific and mass tort data. They also operate under the fundamental assumption that past losses and patterns may not necessarily be indicative and directly applicable to future emerging threats. As a result they tend to focus predominantly on products-based liability scenarios and their latent impact on bodily injury.

FORCAS℠: GUY CARPENTER'S CASUALTY CAT MODELING PLATFORM APPROACH

The major difficulties in modeling casualty catastrophes come from both predicting future loss drivers and identifying exposure concentrations. In property catastrophes, there are only a handful of natural disasters that can occur, and when they do, the damage is generally restricted to a single geographical area. As discussed in the previous sections of this report, the man-made disasters that will drive casualty catastrophes of the future could come from one of hundreds of increasing emerging risks that can span areas such as nanotechnology, genetically modified organisms or cyber-attacks that would be unknown perils to risk managers of the past. Furthermore, the damage and liability from these perils will not be contained to one geographical region or even one industry but will spread across regions and industries according to complex interrelationships that are likely unique to that specific peril. A casualty catastrophe model must therefore contemplate these complexities at the basic level. This marks an important distinction from property catastrophe modeling, where the loss drivers and exposure concentrations are generally well understood.

Casualty exposure concentrations can be geographical, they can be industry-linked or they can be linked through a supply chain:

- Geographical link - comes largely from different litigious environments. A recall on baby formula is likely to be a catastrophic exposure in the United States, but may not be so in other regions.
- Industry link - will be driven by economic conditions, where decreased prosperity of a given industry could lead to multiple shareholder lawsuits occurring at the same time. This is commonly seen in the financial sector, and it is usually the result of a failed industry practice.
- Supply chain link - recognizes the connection between inputs and outputs. If a rubber manufacturer produces defective rubber, these liabilities will flow up the supply chain to industries that use rubber as an input, such as the automobile industry.

GC ForCas has been developed as a platform with model components to cover US commercial lines losses resulting from casualty catastrophes, taking into consideration many of the issues we just outlined above. GC ForCas is an experience-based model that groups historic losses into four main perils, or modules: Sudden Disasters (e.g., Deepwater Horizon), Financial Institutions (e.g., Subprime Crisis), Cyber (all released in the first half of 2015) and Products (e.g., Asbestos) (currently in development). GC ForCas leverages a variety of industry sources to model loss scenarios and line of business dependencies. Through the modeling process, industry portfolio concentrations will be uncovered by mapping exposures and analyzing the interrelationships among those industries. The utilization of historical loss data eliminates the need to estimate these portfolio concentrations through another proxy such as supply chain.

T-5 | EXAMPLE OF CONDITIONAL RELATIONSHIP BETWEEN STANDARD INDUSTRY CLASSIFICATIONS

Probability of a loss in subsequent industry (vertical axis) given a loss in base industry (horizontal axis)

SIC description	2 Dig SIC	28	73	91	49	37
Chemicals and allied products	28		20%	31%	31%	45%
Business services	73	10%		23%	13%	18%
Executive & general government	91	19%	30%		13%	9%
Electric, gas and sanitary services	49	24%	20%	15%		45%
Transportation equipment	37	24%	20%	8%	31%	

Source: Guy Carpenter

The Sudden Disaster and Financial Institutions modules produce catastrophe loss distributions by line of business and by industry, which are to be viewed as an additional load to the non-catastrophe loss in an insurance company's portfolio. These loss distributions reflect an individual company's limits profile as well as its market share at the line of business/industry type level.

T-6 | FINANCIAL INSTITUTIONS: LOSS DISTRIBUTIONS

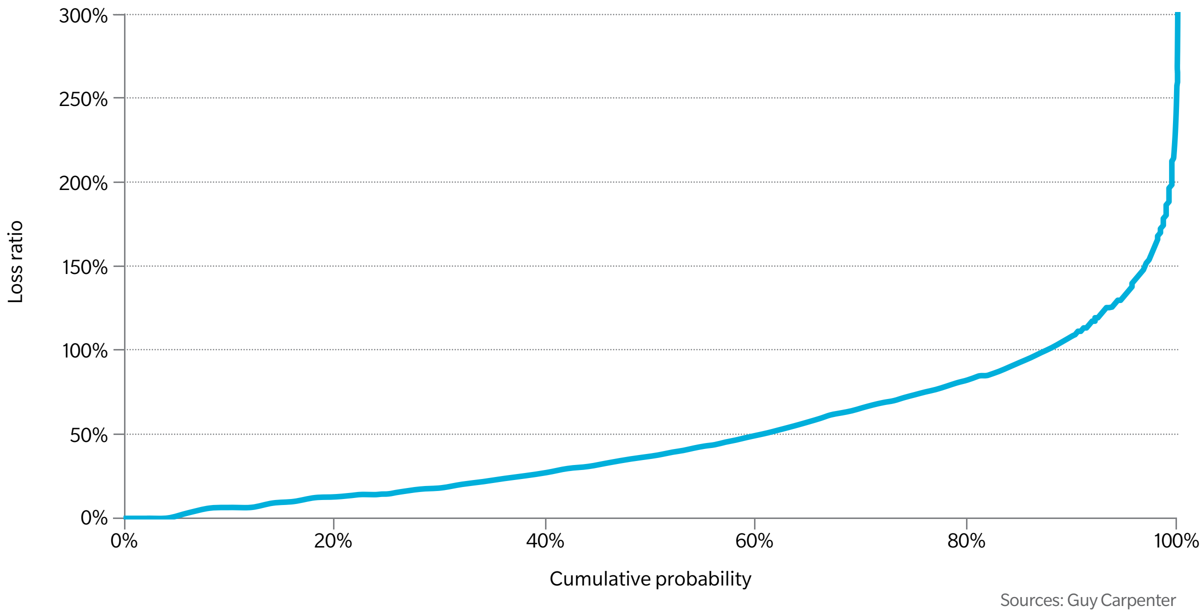
	Mean StdDev CV	78.1M 88.5M 0.96	18.4M 32.9M 1.51	47.2M 52.7M 0.94	0.8M 3.4M 3.44	10.4M 23.4M 1.90	1.1M 6.1M 4.52	0.2M 1.8M 8.21
Probability	**Return period**	**Company annual**	**FI E&O/ D&O**	**D&O**	**E&O**	**Other liabilities**	**Excess casualty**	**Fidelity surety**
			Value at Risk (VaR)					
80.0%	5	120.7M	27.4M	78.3M	0.0M	16.9M	0.0M	0.0M
90.0%	10	176.0M	50.7M	113.2M	1.7M	34.4M	0.0M	0.0M
95.0%	20	221.7M	67.9M	140.8M	4.0M	50.7M	0.0M	0.0M
97.0%	33	324.2M	115.5M	176.3M	10.5M	76.7M	18.5M	0.0M
98.0%	50	360.7M	128.9M	203.4M	12.7M	87.3M	21.1M	0.0M
99.0%	100	408.9M	155.9M	232.4M	16.1M	105.2M	23.5M	9.3M
99.5%	200	456.0M	215.2M	259.2M	21.1M	139.2M	42.3M	16.9M
99.6%	250	501.6M	221.3M	281.8M	24.1M	149.2M	63.3M	17.5M
99.8%	500	631.3M	239.8M	315.5M	28.3M	171.0M	63.3M	21.1M
99.9%	1000	714.2M	246.8M	361.7M	33.0M	174.7M	63.3M	24.5M

Note: Mean statistics by line sum to equal the total mean. VaR statistics will not sum to total due to diversification benefits at both ends of the distribution. The VaR statistics by line can still show the relative contribution of each line to the total.

Source: Guy Carpenter

The GC ForCas^{SM} Cyber component has been developed to examine cyber liability risk, both first and third party coverages, at the portfolio level. Events may include data breach/privacy liability, network security liability, business interruption and data asset protection, among others. The Cyber module produces a ground-up loss ratio distribution for a cyber liability portfolio. This distribution is the product of a frequency/severity analysis that reflects individual risk detail such as limit, attachment, parent company type (public or private), industry code and parent/company revenue within the portfolio.

F-8 | GROUND-UP LOSS RATIO DISTRIBUTION



Sources: Guy Carpenter

INTEGRATING & SYNTHESIZING NEW EMERGING RISKS – WITHIN THE ERM FRAMEWORK

One purpose of ERM is 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, a robust ERM methodology would use a holistic approach to risk and capital management where threats are identified and monitored, all action plans are developed and risks are measured.

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. 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 an ERM approach, 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 datasets and the development of new technology is beginning to enable (re)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.

Proper enterprise risk management 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® 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, these models can facilitate comparisons of a company's risk profile to that of its peers and peer composites.

VI. CONCLUSION

With the world rapidly changing and evolving, what was the case 10 years ago is not the case today and will not be 10 years from now. As discussed in detail in this report, new technologies can impact people in their everyday lives through the products we use, how long we live, how much we spend to keep ourselves healthy and where our information is stored. All of these carry inherent risks that are new to the world and that may not be a part of the historical dataset upon which (re)insurers rely for pricing and/or establishing proper risk controls.

In our Emerging Risks series that started two years ago and continues with this report, Guy Carpenter has sought to bring some element of clarity to what those risks are and, more importantly, how the (re)insurance industry would benefit by understanding and quantifying its exposures to these risks in order to mitigate capital depletion.

There are many challenges in creating a probabilistic data set that attempts to quantify unforeseen loss, unforeseen change in life expectancy or the unforeseen increase in medical costs and the impact these may have on (re)insurers.

(Re)insurers that innovate by anticipating the risks of new technologies, developing new products in response to those threats and solving for how to manage these exposures are likely to translate risk into opportunity.

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

Contributors

William Garland
Managing Director

Mike Brown
Managing Director

Victoria Jenkins
Managing Director

Emil Metropoulos
Senior Vice President

Jeremy Platt
Senior Vice President

David Rains
Managing Director

Christopher Ross
Managing Director

Jiyang Song
Senior Vice President

Morley Speed
Managing Director

Christopher Wetzel
Assistant Vice President

Contact Us

For additional information on Guy Carpenter solutions, please contact your representative or visit your local office or guycarp.com.

For media or general inquiries:

Missy DeAngelis
missy.deangelis@guycarp.com
+1 917 937 3118

Jennifer Ainslie
jennifer.ainslie@guycarp.com
+44 207 357 2058

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; public sector; 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 modelling 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 people. Marsh is a leader in insurance broking and risk management; Guy Carpenter is a leader in providing risk and reinsurance intermediary services; Mercer is a leader in talent, health, retirement, and investment consulting; and Oliver Wyman is a leader in management consulting. With annual revenue of $13 billion and 57,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 130 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information and follow us on LinkedIn and Twitter @MMC_Global.

*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.

DISCLAIMER

The data and analysis provided by Guy Carpenter herein or in connection herewith are provided "as is", without warranty of any kind whether express or implied. The analysis is based upon data provided by the company or obtained from external sources, the accuracy of which has not been independently verified by Guy Carpenter. Neither Guy Carpenter, its affiliates nor their officers, directors, agents, modelers, or subcontractors (collectively, "Providers") guarantee or warrant the correctness, completeness, currentness, merchantability, or fitness for a particular purpose of such data and analysis. The data and analysis is intended to be used solely for the purpose of the company internal evaluation and the company shall not disclose the analysis to any third party, except its reinsurers, auditors, rating agencies and regulators, without Guy Carpenter's prior written consent. In the event that the company discloses the data and analysis or any portion thereof, to any permissible third party, the company shall adopt the data and analysis as its own. In no event will any Provider be liable for loss of profits or any other indirect, special, incidental and/or consequential damage of any kind howsoever incurred or designated, arising from any use of the data and analysis provided herein or in connection herewith.

Statements or analysis concerning or incorporating tax, accounting, regulatory or legal matters should be understood to be general observations or applications based solely on our experience as reinsurance brokers and risk consultants and may not be relied upon as tax, accounting, regulatory or legal advice, which we are not authorized to provide. All such matters should be reviewed with the client's own qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise.

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Guy Carpenter & Company, LLC, except that clients of Guy Carpenter & Company, LLC need not obtain such permission when using this report for their internal purposes.

The trademarks and service marks contained herein are the property of their respective owners.

Guy Carpenter Report

MARSH & McLENNAN COMPANIES

Executive Summary
Cyber
Life/Health/Longevity
New Technologies
Reserving/Capital Setting
Managing/Modeling Risks
Conclusion

GUY CARPENTER

M2450.9.15.900K | EMERGING RISKS REPORT | | GUYCARP.COM