THE GENEVA ASSOCIATION

Advancing Accumulation Risk Management in Cyber Insurance

Prerequisites for the development of a sustainable cyber risk insurance market

The Geneva Association

The Geneva Association is the leading international insurance think tank for strategically important insurance and risk management issues. The Geneva Association identifies fundamental trends and strategic issues where insurance plays a substantial role or which influence the insurance sector. Through the development of research programmes, regular publications and the organisation of international meetings, The Geneva Association serves as a catalyst for progress in the understanding of risk and insurance matters and acts as an information creator and disseminator. It is the leading voice of the largest insurance groups worldwide in the dialogue with international institutions. In parallel, it advances—in economic and cultural terms—the development and application of risk management and the understanding of uncertainty in the modern economy.

The Geneva Association membership comprises a statutory maximum of 90 chief executive officers (CEOs) from the world's top insurance and reinsurance companies. It organises international expert networks and manages discussion platforms for senior insurance executives and specialists as well as policymakers, regulators and multilateral organisations.

Established in 1973, The Geneva Association, officially the 'International Association for the Study of Insurance Economics', is based in Zurich, Switzerland and is a non-profit organisation funded by its Members.

Advancing Accumulation Risk Management in Cyber Insurance

Prerequisites for the development of a sustainable cyber risk insurance market

Daniel M. Hofmann, Senior Advisor Insurance Economics, The Geneva Association
Steve Wilson, Senior Advisor Cyber, The Geneva Association

In collaboration with Rachel Anne Carter, Director Cyber, The Geneva Association

The Geneva Association

Talstrasse 70, CH-8001 Zurich | Tel: +41 44 200 49 00 | Fax: +41 44 200 49 99

secretariat@genevaassociation.org www.genevaassociation.org

Photo credits:
Cover page—Shutterstock

August 2018
Advancing Accumulation Risk Management in Cyber Insurance
Prerequisites for the Development of a Sustainable Cyber Risk Insurance Market

Published by The Geneva Association—The International Association for the Study of Insurance Economics.

Contents

Acknowledgements

This report was written under the general guidance of Daniel M. Hofmann, Senior Advisor Insurance Economics, and in close cooperation with Steve Wilson, Senior Advisor to The Geneva Association. Rachel Anne Carter, Director of Cyber, contributed to the writing. Antoine Baronnet, The Geneva Association's Deputy Secretary General supported the project throughout the entire process.

The authors are much obliged to the members of the Cyber Risk Working Group. Their guidance was complemented by input from experts in The Geneva Association's member firms and many insightful discussions with external experts in cyber security, consulting and risk modelling (see Appendix for a complete list). The authors wish to thank all discussion partners for their time spent in contributing to the report. All responsibility for errors and omissions rests, of course, with the authors.

Foreword

Anna Maria D'Hulster

Secretary General,
The Geneva Association

Many threats associated with the digitalized world—cyber risk in short—have steadily moved to centre stage. In a list annually produced by The World Economic Forum, risks related to cyberattacks and data fraud feature among the top five global risks. And a quick search on Google shows about 4.6 million entries for the term 'cyber risk,' ahead of nuclear (3 million) and earthquake (1 million) risks, but well below the roughly 26 million entries each for hurricane and terrorism risks.

Clearly, cyber risk has become a formidable challenge for modern society and the insurance industry. While the cyber insurance market has grown rapidly in recent years from a small base 10 to 15 years ago, there is a risk that future expansion may suffer significant setbacks and that several vulnerabilities may stall expected future growth. One leading industry executive recently opined that "cyber is an accident waiting to happen." Others question its insurability, at least in the absence of necessary conditions to ensure the market's viability and sustainability.

However, expanding the boundaries of insurability and making new risks manageable is not new for insurers. Over centuries, insurers have developed products and services that reflect the changes in the risk landscape brought about by socio-economic transformations, industrial developments and advances in technology. As a result, the industry has many learnings on which to build new business propositions caused by cyber. That said, cyber risk—like the digitalization of economies—is taking us into uncharted territory. Both exposures and threats have distinct characteristics, which give rise to unprecedented challenges.

This report is the first in a series of papers to be published in the next years that explicitly deals with the questions of whether cyber risk can become manageable, whether a sizeable and sustainable insurance market can evolve, and under which (pre-)conditions this will be the case.

For this to happen, three broad prerequisites need to be met. First, there needs to be sufficient resilience at the source of risk for the principles of insurability to apply. This is fundamental for all underwriting, a point to be discussed in our next report. Second, providers of risk protection must be able to achieve an acceptable return on capital. And third, insurance markets need to be able to withstand shocks from extreme events—in the case of cyber, this means absorbing accumulation risk. This concern is widely held across the industry, and it is the reason why we focus in this report on the market's ability to withstand extreme events.

Our findings so far are cautiously optimistic. This report documents that strong progress is being made in data analytics and risk modelling, including the recognition of data and modelling gaps, paving the way for necessary improvements. That said, much more needs to be done for the industry to develop its full role in dealing with rapidly changing and growing threats. We emphasise that, as with all risks of this complexity and scale, the insurance industry can offer only a partial remedy. Other key stakeholders—small and large businesses, technology providers and governments—need to do their part for cyber risk to become manageable in the long run. We offer this report as our first step towards finding solutions, with next constructive steps soon to follow.

Executive summary

In recent years, insurance products offering affirmative cyber coverage (i.e. policies specifically offering cyber risk cover) and premium volumes have expanded sizeably, while loss ratios have compared favourably relative to other product lines. With a constant news stream about data breaches, cyberattacks and viruses, risk awareness in large and small businesses is increasing, and demand for cyber insurance will likely be strong for some time. Keeping up with demand pressure is challenging, and a sustainably growing cyber insurance market should not be taken for granted.

This report identifies three prerequisites that must be met to ensure sustainability. First, customers and insurers must facilitate cyber resilience at the source of risk (this prerequisite will be taken up in a separate report). Second, insurers need to make an acceptable return on capital. And third, the insurance industry needs to be able to withstand major shocks.

While these prerequisites have to be met in many lines of business, cyber risk creates several unprecedented challenges. Exposure bases are hard to define and measure, and they are constantly changing. Historical claims data are scarce and not considered to be well representative of future vulnerabilities. Threats are constantly evolving; they can spread widely and rapidly, and a series of consecutive large events is plausible. A high degree of interconnectivity may result in potentially unbounded impacts. These challenges require that insurers strengthen their core underwriting capabilities, in particular exposure measurement, claims assessment, and accumulation modelling.

Despite the fact that cyber risk is different in many ways, the report finds that insurers have taken several steps to make it manageable. They have played an active role in helping companies build resilience, a trend that is expected to continue. In addition to limiting insured losses, the focus on services to enhance resilience will have wider socio-economic benefits and likely contribute towards containing the spread to cyberattacks in the future.

To better assess future exposures and claims costs developments, leading underwriters are implementing proactive approaches, drawing on a range of internal and external inputs. Some practitioners are talking about 'confinement zones' to capture complex and constantly evolving systems and networks in the corporate world. The often-evoked paucity of data is a clear challenge, but innovative attempts to bypass data limitations are emerging. Advanced techniques (e.g. machine learning, Bayesian hierarchical modelling) can allow for a better measurement and understanding of new technological risks. Specific advances include granular assessments of cloud-related interconnectivity as well as increasingly detailed stochastic scenario assessments for challenges related to malware and excessive reliance on one particular hardware or software (the 'monoculture' dependency).

The advances in accumulation modelling seen so far support a greater understanding of risk interconnectivity, whether on a wide scale or within specific industry segments. This improves the ability of underwriters to accept risk. It is reasonable to assume that market development will continue to benefit from modelling advances. Provided that underwriting discipline is maintained, the report is cautiously optimistic that insurers are well-positioned to ensure the cyber insurance market's viability and achieve sustainable growth in the future.

This cautious optimism in the market's growing capabilities is also underscored by capital levels that currently are sufficient to support cyber risk underwriting in line with limits established by insurers. In addition, governments have started to consider extending, or have started signalling their readiness to extend, existing arrangements for terrorism coverage to include property damage and the related business interruption from events caused by acts of cyberterrorism. While there are still questions about definitions and attribution, the willingness of the public sector to take the cyberterrorism risk off the table will undoubtedly be a meaningful step towards inducing further private capacity to enter—and stay in—the cyber insurance market.

The report identifies four challenges in the context of cyber accumulation risks:

i. A single large event or a series of consecutive events may make affirmative cyber insurance unprofitable;

ii. Insurers and reinsurers (for which risk accumulation may be more pronounced than for primary insurers) could underestimate non-affirmative cyber exposure leading to an unplanned shock from a major event;

iii. Data are of insufficient quality, are incomplete and/or lack the necessary consistency for more advanced modelling techniques; and

iv. Governments fail to provide commensurate frameworks for the sharing of large-scale terrorism-induced losses.

The consequences are manifold should risks associated with these challenges materialise. Insurers and reinsurers could withdraw from the market after unacceptably high losses and fear of repeat events. Growth of the small alternative capital market may be stalled and prevent insurers from accessing needed capacity. (Re)insurers could introduce tighter policy terms and in doing so increase the number of exclusions and/or make buy-backs prohibitively expensive. The lack of confidence in advanced model outputs could stifle growth if models are deemed to be too blunt for insurers to extend portfolios or offer higher coverage levels. This could result in a further constraint on the amount of coverage that insurance markets are willing to provide to larger enterprises. A resultant negative swing in perceptions towards a less profitable and riskier market could subsequently leave the market for small and medium enterprises underdeveloped. A large event may also trigger regulatory intervention with the risk for insurers having to provide cover with uneconomic terms and rates.

Of equal importance is the need to maintain underwriting discipline. Cyber risk is not unique in this respect. Historically, many property-casualty classes have suffered when underwriting standards slipped or when prices failed to adequately reflect the cost of risk. Many insurers perceive the current rating environment as soft and likely inadequate should any of the above risks materialise. Furthermore, the growing threat from terrorism adds urgency to such concerns, and the appropriate treatment for this risk in war and terrorism exclusions will be key.

Given the fluid stage of developments, it would be premature to make firm policy recommendations. At this point, the objective should be to 'do no harm.' Prudence suggests refraining from making irreversible decisions, especially when a market is demonstrating high levels of innovation. Policymakers should endeavour to use the market as a discovery mechanism and expect best practices to be adopted quickly by competitors and new market entrants.

There have been a number of policy recommendations under discussion. They include extending the coverage provided by terrorism pools in the countries where cyberterrorism coverage has so far not been offered. Additional governmental backstops related to cyber losses (beyond losses triggered by terrorism) could signal to the market that the public sector too has 'skin in the game' and is prepared to contribute to solutions developed in the private market. To strengthen resilience, cyber security features should be developed and implemented at inception, and security design features should be certified and controlled by authorities. Jointly with IT security providers and insurers, authorities should develop and implement foundational IT and information security standards that facilitate IT security hygiene. Governments could also consider becoming signatories to a 'Digital Geneva Convention,' which would contain the use of cyber weapons by governments.

In the areas of underwriting and risk modelling, insurers should ultimately reduce opacity by standardising event definitions and cyber terminology. In addition, insurers and authorities could work jointly towards data and information sharing that goes beyond mere reporting and one-way notification. And jointly with the industry, authorities could work towards appropriate international frameworks to enable the development and maintenance of standardised databases for cyber incidents similar to databases developed for natural catastrophes.

1. Market characteristics

Triggered by a growing volume of data breaches, hacking attacks and viruses, the cyber insurance market has grown rapidly in recent years. Nevertheless, coverage remains uneven across major markets, with the U.S. accounting for more than 80 per cent of the global market. Similarly, cyber insurance penetration rates are low and unevenly spread across industries, ranging from 5 per cent in the SME segment to up to 75 per cent in the financial sector. In light of growing risk awareness, the demand for cyber insurance will likely continue to increase rapidly in coming years.

1.1 Primary market

In the 20 years since insurers started providing stand-alone cyber insurance, coverages available have expanded from narrow third-party liability covers for hacking, to a wide range of first-party and third-party covers, together with associated services for risk management and post-event remediation. Today, a stand-alone policy (offering only cyber coverage), or affirmative coverage in a package policy (offering coverages for several classes), will typically cover the insured's costs for IT forensics, customer notification, credit monitoring, data recovery and public relations as well as liabilities for costs and damages incurred by third parties (including non-damage business interruption), and insurers will provide—directly or through a technology partner—specialist IT security services.

The development of the market parallels the digitalization of economies, the expansion of the Internet and the increasing losses associated with technological developments. Data breaches have been hitting the headlines for some years, but more recently new threats, such as ransomware, indicate there is a much wider range of potential loss events. McAfee's 2018 report on cybercrime includes some startling statistics: an estimated 4,000 ransomware attacks daily in 2016; 4.8 billion records lost, mostly as a result of data breaches, in the same year; and estimates of between 300,000 and 1 million viruses and other malicious software products being created daily.[1] Reflecting these developments, the cyber insurance market has grown rapidly—over 30 per cent per annum in recent years.[2] In the future, regulations on data privacy and security, rising public awareness and continued high loss frequencies for businesses are expected to continue to drive strong growth in demand.

From information available on U.S. stand-alone cyber policies (which account for around two thirds of the U.S. market), cyber enjoys good loss ratios, with the overall U.S. market reporting 51.4 per cent in 2015, improving to 46.9 per cent in 2016.[3]

Notwithstanding impressive growth rates, total premiums for affirmative cyber coverages (stand-alone and package) are estimated at around less than USD 4 billion globally for 2018, representing around 0.5 per cent of the total global commercial insurance premium. This reflects limited penetration in many countries and industry segments, and low take-up by small and medium-sized enterprises (SMEs). To date, most buyers of cyber insurance have been mid-market and larger corporations, many with internal risk management functions, inhouse IT and increasingly a senior-level Chief Information Security Officer (CISO).

For the largest risks, it is currently possible to purchase in extreme cases coverage of around USD 600 million. This amount is substantially more than was available only a few years ago but it remains less than half that of liability and specialty lines. Furthermore, even such large coverage 'towers' (several stacked policies from a consortium of insurers) are now considered insufficient for the largest of events, with several known losses having exceeded this amount.

Currently, the U.S. accounts for over 85 per cent of global volume but this market is considered far from mature at this stage, with some estimates putting penetration at less than 15 per cent. The primary reason for the larger volume of coverage in the U.S. has been regulations on data privacy and protection. Regulations coming into force in other regions, notably the General Data Protection Regulation (GDPR) in the European Union, are expected to stimulate demand further, as will recent developments in public awareness of the potential for data privacy issues.

1 McAfee and Center for Strategic and International Studies (2018).
2 Aon (2017b).
3 A.M. Best (2017).

The top three industry sectors purchasing cyber are financial institutions, retail and wholesale, and healthcare, reflecting their emphasis on financial transactions and sensitivities of personal data.[4] In 2015, these three sectors accounted for over 60 per cent of the market for stand-alone cyber in the U.S. with market shares of 30 per cent, 21 per cent and 13 per cent for financial institutions, retail and wholesale, and healthcare respectively. As the nature of attacks becomes broader and the prospect of significant disruptions to the operations of all businesses increases, take-up in other industries is expected to increase substantially.

1.2 'Non-affirmative' coverage in other property and casualty lines

While the market provides affirmative coverage in stand-alone and package policies, there is a growing concern for the potential of some cyber events, such as a widespread malware, to cause major losses by triggering coverages in other classes. Most notably, business interruption covers may be triggered as business operations in the vast majority of industries are increasingly dependent on technology, but there is also potential for physical damage, with the possibility of extreme events caused by a cyberterror attack. Considering casualty classes, examples of exposure include Directors' and Officers' policies—where there is potential for claims should a cyber event impair a company's value—and General Liability when third parties are impacted.

The potential for 'non-affirmative' coverages to be triggered presents additional—and potentially significant—challenges for insurers and reinsurers. Not only is there a high degree of uncertainty in the quantitative impact of a large event, but the interpretation of policy language can also be expected to be a major determinant of liability. Policy wordings will likely be tested in the courts, perhaps over several years. Adding to these challenges for the primary insurers, there are risks of misalignment between primary wordings and reinsurance coverages, or reinsurers restricting the cover they provide to the primary insurance market.

Recognising these challenges, some insurers are adapting their policy language to exclude cyber-triggered losses and offering corresponding 'buy-back' endorsements. Currently, these developments are not widespread across jurisdictions.

1.3 Market overview—reinsurance and alternative capital

Around 30 per cent of the market premium is ceded to reinsurers with several reinsurers participating.[5] Reflecting the overall small size of cyber portfolios relative to their overall business volumes, larger reinsurers are currently able to manage their exposures using relatively pragmatic approaches with limited mathematical sophistication. However, growth in the stand-alone cyber business and the exposure to non-affirmative coverages in other lines means that reinsurers will likely face considerable modelling challenges in the future. These challenges include both the granularity of data and the frequency of data submissions from primary insurers. The latter is particularly important to reinsurers, given how quickly the cyber risk landscape is evolving.

Currently, only a very limited role is played by alternative capital. Managers of Insurance Linked Securities (ILS) are not yet confident they can evaluate the risk sufficiently for their investor base, which demands a robust and transparent quantification for the risk premium associated with these instruments. Furthermore, while the ILS market has offered investment options benefiting from little or no correlation to other asset classes, cyber-based securities are different. There are clear connections to the economy: the constant stream of data breaches and ransomware attacks is recognised as a direct economic drag, and a major event, perhaps disrupting one or more industry sectors, could possibly trigger a negative reaction from financial markets.

An Industry Loss Warranty (ILW) index has recently been launched by Property Claim Services (PCS), a provider of independent statistics and measures for the industry in the U.S. This approach, known as 'parametric,' is an encouraging development because determining all costs of the underlying loss and aggregating them into a total

4 Aon (2017b), op. cit.
5 Aon (2017b), op. cit.

cost for an event is subject to numerous challenges and uncertainties—not least extensive legal disputes on the interpretation of non-affirmative coverage. Based on this, a small number of specialist reinsurers are offering ILW-based instruments, which presents some potential for additional retrocession capacity and also the possible novel development of insurers directly purchasing ILW covers to support their own exposure directly.

1.4 Supply and demand

While recognising that no risk class is wholly insurable, on the supply side it is clear that cyber coverage levels are lower than in other classes. The potential size of the largest of claims to an individual insured far exceeds the maximum coverage available in the market, with individual policies limited at roughly USD 600 million. Furthermore, many buyers consider limits on business interruption coverage in stand-alone cyber policies to be too low, and the availability of contingent business interruption is limited. Finally, analyses of accumulation events, such as those provided by Lloyd's and AIR Worldwide in their 2018 study of a cloud failure, indicate insured losses would be in the region of just 20 per cent of total economic losses.[6]

At the macro level, several organisations have estimated total annual economic costs due to cybercrime with, for example, McAfee's current estimate being USD 600 billion.[7] Although not all of the costs in these estimates would typically be insurable, there are serious concerns that the cyber market is covering only a small fraction of losses, with analysis from a number of major studies indicating an insurance gap in the region of 90 per cent for those scenarios.[8]

On the demand side, the awareness of risk is increasing rapidly—CEOs routinely place cyber risk at the top of their concerns, both in the short- and long-term perspective.[9] However, many surveys report that cyber risk is consistently underestimated and that buyers are not aware of what insurers could offer. Consequently, penetration rates vary widely from 75 per cent in large financial institutions to less than 5 per cent in SMEs.[10]

While demand may to some degree be tempered by a lack of understanding of the threats and/or knowledge of the available insurance products, it is nonetheless expected to increase significantly. And as the industry responds, there will inevitably be an increase in accumulation risk exposures. PCS found that 2017 has been the highest loss year to date, with several companies reporting economic losses for individual events to the tune of several hundred million USD, with a handful in excess of USD 1 billion.[11] In many cases, the impacted firms had not purchased coverage to the level of the loss, and so it is to be expected that demand for more 'vertical' coverage (higher limits) will continue to increase strongly. Furthermore, recent trends and the replicating nature of cyber threats would indicate that 2018 and coming years could be worse, and perhaps considerably so. Less likely, but nonetheless plausible, are losses from a cyber catastrophe, impacting both affirmative and non-affirmative covers, which would have a very significant impact on (re)insurers' earnings.

The following chapters explore the industry's progress in underwriting this class for commercial lines and how it is addressing the challenges of managing accumulation risk.

6 Lloyd's and AIR Worldwide (2018).
7 McAfee and Center for Strategic and International Studies (2018), op. cit.
8 The Geneva Association (2018a).
9 KPMG (2017).
10 Aon (2017b), op. cit.
11 See Johansmeyer, (2018).

2. Underwriting and accumulation risk

Cyber risk has several distinct characteristics that differentiate it from other risks. It implies that measurement and modelling approaches that have been developed for other risks (such as natural catastrophes) cannot easily be transferred to cyber risk. This forces underwriters and accumulation modellers to adapt—quite significantly—the technical capabilities that have been developed in those classes. This chapter looks at how insurers, reinsurers and other actors in the industry are responding to these challenges. The discussion is framed in the context of three high-level prerequisites that must be met to ensure the sustainable growth of the cyber risk insurance market. These prerequisites cover the fundamentals of the risk itself, the relevant capabilities of (re)insurers, and the levels of capital needed to support the market and absorb the financial consequences of unexpected extreme events.

2.1 Prerequisites and capabilities

The fundamental prerequisites for a sustainable and effective commercial cyber insurance market can be summarised as follows:

- There needs to be sufficient resilience at the source of the risk for the risk to be insurable;
- The providers of risk protection (i.e. insurers) must be able to make an acceptable return on capital; and
- The available capital must be able to both withstand shocks from accumulation events and provide adequate compensation to insureds in the case of such an event.

The first prerequisite—resilience—is relevant for any risk class to be insurable. If homeowners did not lock their homes, then theft would not be insurable. The first steps in addressing any risk are to assess, measure and manage it. Residual risks (i.e. those that cannot be contained at the source) can then be mitigated through risk transfer mechanisms such as insurance. In the case of cyber risk, resilience is a wide and complex topic and, as can be seen by the current high frequency of events, much needs to be done by technology providers, by technology security companies and by businesses. Unlike traditional risks covered under property and liability lines of business, cyber risk is relatively poorly understood in the business sector, and risk management in this field is evolving at a brisk pace. Insurers can play an important role in helping to develop business-level resilience (see also Chapter 3), and there is a growing number of service companies dedicated to building cyber resilience in conjunction with risk carriers. Many of these offerings are innovative and blend the discipline of systems thinking with technological advances. The focus of this report is on the latter two prerequisites and the consequences for the industry, including primary insurers, reinsurers and alternative capital providers.

The second prerequisite reflects the fact that listed insurance companies must raise capital in a competitive market and must make an adequate return to shareholders. This in turn requires disciplined and effective underwriting to deliver an acceptable loss ratio, the primary driver of earnings performance. So far, the cyber insurance market has reported healthy loss ratios, and participants are generally faring well. This can be attributed in part to the fact that cyber underwriters are leveraging, insofar as is possible, technical capabilities from other more established lines of business. Many cyber underwriters are experienced in the specialty and financial lines markets and are comfortable with complex risks, for example in the drafting of policy wordings where there is potential for intense legal challenge on coverage interpretations. Learnings are also drawn from the property classes with, for example, digital risk assessments being developed that parallel the physical risk assessments long established in property classes. These assessments of a customer's IT security risks are now an integral part of the underwriting process for the major competitors in the market. The use of IT security professionals, either outsourced or in-house, is standard practice for large account risk assessments, while checklists and certifications are applied for smaller accounts where premium levels are not large enough to justify the costs of a bespoke approach.

These parallels have facilitated a quality of underwriting beyond what could be expected for the size and maturity of the cyber insurance market. However, to maintain loss ratios at acceptable levels for the anticipated market growth, underwriters need to continue to develop their technical capabilities in exposure measurement and claims

cost assessment. These are two core technical capabilities in underwriting, and both are being challenged by the distinct characteristics of cyber risk.

The third prerequisite—that the industry must be able to withstand a major shock while offering a meaningful level of coverage to the insured businesses—is at the heart of many concerns about cyber risk. The potential for large losses from extreme events is well established: the extreme scenario of a cyber-triggered act of terrorism, disabling the infrastructure of a major urban area, has been estimated to be able to cause economic losses running into several hundred billion USD or even exceeding one trillion USD,[12] while widespread malware attacks and failure of a cloud provider could lead to losses ranging in the tens of billions, comparable to natural catastrophes.[13,14] For the industry to deal with the accumulation threat, it must develop its capabilities in measuring and modelling this risk, and there must be sufficient capital available to sustain a shock.

The following sections summarise the distinct characteristics of cyber risk and review the industry's progress in developing the core technical capabilities of exposure measurement, claims cost assessment and accumulation modelling in the context of these characteristics. Comparisons are made to the 'traditional' property and casualty classes to help inform how the challenges from cyber impact the underwriting and accumulation modelling processes.

The chapter concludes with a look at the considerations for ensuring that there is sufficient capital available both to absorb a large event and to compensate the firms and organisations requiring risk protection.

2.2 The distinct characteristics of cyber risk

Dealing with a new risk type is not new to the insurance industry, and any developing risk has much uncertainty in the early stages of its evolution. History shows that property and casualty underwriters have typically faced a multitude of challenges as societies, economies and the environment have developed: technological developments of physical assets insured, changing weather patterns, geographical concentrations, industrial diseases, legal and socio-economic trends, and so on. However, digitalization and technological advances have led to unique challenges: levels of interconnectivity of societies and economies are unprecedented, rates of change are daunting, and threats have the potential to replicate across the globe in days or even hours. These create distinct characteristics for cyber risk, which can be summarised as follows:

- Exposure bases are hard to define and measure, and they are constantly changing;
- Historical claims data are scarce and not representative of future vulnerabilities;
- Threats are constantly evolving—they can spread widely and rapidly, and recur;
- A high degree of interconnectivity is leading to potentially unbounded impacts.

2.3 Capability: Exposure measurement

At the very core of underwriting is the need to 'know your exposure.' Broadly defined, exposure is a measure of risk: for example, the value of an insured asset or how much compensation may be paid on a liability policy.

In the property classes, exposures are readily measurable and stable over time. For example, even with trends in urbanisation increasing property concentrations, advances in data capabilities mean that insurers' ability to measure these concentrations has kept pace with these changes. Insurers can gather the exposure data—property values—and furthermore capture the associated key attributes such as geocodes for accurate location, construction details, and so on. This allows insurers to compile a robust exposure base to be used as an input for underwriting analysis and natural catastrophe modelling.

Digitalization brings an entirely new problem: the exposure base is no longer stable, or even measurable, at least based on established analytical and actuarial

12 Lloyd's and Cambridge Centre for Risk Studies (2015).
13 Lloyd's and Cyence (2017).
14 Lloyd's and AIR Worldwide (2018).

techniques. Businesses continually update and introduce new IT systems, often without fully replacing the old, resulting in a system architecture with layers of different technologies. The combination of legacy IT systems with new, highly advanced technologies presents a complex, constantly changing systems landscape. Trying to measure an insured's exposure in a traditional way is inadequate—it is too complicated, too time-consuming, and does not yield sufficient predictive power.

These challenges for the underwriter in the assessment of risk at the individual insured business level are magnified significantly for the accumulation modeller, who needs to understand possible risk aggregations and especially needs data sets of sufficient quality and completeness.

In response to these challenges, data protocols are emerging that combine basic company information (revenue band, industry, number of employees) with digital risk indicators, such as patching frequency and backup procedures. The establishment by Lloyd's in 2016 of a schema for cyber exposure data has provided a much-needed standard for the core features of input data in cyber risk tools and the key attributes to be considered when evaluating cyber risk.[15]

Coupled with this, advanced data analytics are being developed that analyse the characteristics that drive cyber risk. For underwriting individual customers, specialised service providers have developed digital risk assessment tools which measure and assess IT security practices of businesses, providing risk assessment scores and clear benchmarks of standards compared to peers. While these service providers have the potential to offer promising insights into the underlying risk, these tools will take time to mature. Underwriters need to understand the different technical capabilities of these providers, to test their effectiveness and to assess whether the cost of their services is economically viable. All of these validation efforts are challenging, given the highly technical nature of the services offered and the jargon associated with them.

2.4 Capability: Claims costs assessment

The distinct characteristics of cyber risk provide a double challenge in assessing claims costs, a vital part of the underwriting process.

First, historical claims data are generally sparse. Only a handful of insurers have a long enough and sufficiently broad history to assemble a database with enough credibility to carry out conventional analytical techniques. Second, threats are changing rapidly. 2017 experienced the greatest amount of cyber losses to date, with a range of attacks from widespread hardware flaws to innovative malware attacks. The dynamic features of cyber threats are exacerbated by the rapidity with which the Internet can spread knowledge, including allowing criminal actors to benefit from highly sophisticated state-developed software. The 'dark web' has facilitated the growth of black market digital ecosystems, spreading knowledge amongst bad adversaries. For example, ransomware is widely available—even offered as a service—with cryptocurrencies offering shelter for malicious actors. Threats spread and replicate across the globe and, unlike natural catastrophes, can endlessly adapt and recur with alarming frequency. So even with a credible volume of historical claims data, its predictive power is questionable.

In the last 20 to 30 years, actuarial techniques in property-casualty classes have become increasingly sophisticated in assessing key claims metrics, such as claims costs and frequencies measured with reference to the exposure base. These techniques originated in classes with large claims volumes where it is possible to 'slice and dice' claims data and where trends are measured over multi-year periods. For example, motor insurance rates depend on variables such as age of driver, size of engine, location, and so on; and there is a well-defined and stable exposure base—the number of vehicles in the portfolio. Similarly, workers' compensation claims costs are analysed by type of injury and referenced against payrolls; property classes have well-defined perils—fire, theft and weather—to be referenced against property values.

15 A collaboration with Lloyd's Market Association, AIR Worldwide, Cambridge Centre for Risk Studies, and RMS, has sought to establish a common core schema for cyber exposure data and common core features for input data used in cyber risk tools in the market in relation to both key attributes that should be considered when evaluating cyber risk and the way in which this information should be collected in line with existing industry-standard codes. See https://www.lloyds.com/market-resources/data-and-research/cyber-core-data-requirements.

Limited data volumes and ever-changing threats—compounded by uncertain exposure—render these traditional actuarial methods for analysing claims costs unfit for purpose. Cyber underwriters appreciate that fitting trend curves to the claims experience of the last few years cannot be a reliable guide to future claims costs. This is a lesson driven home by natural catastrophes, and it motivated the development and widespread use of forward-looking catastrophe modelling.

In response to this double challenge from limited claims data and constantly evolving threats, leading underwriting organisations are implementing proactive approaches to assess the likely rate of change in future developments. Earlier tools, such as emerging 'risk radars', had similar aims, but they tended to focus on risks that developed over multi-year timescales. An example is the impact of climate change on weather patterns, whereas cyber risk evolves much faster at the pace of the digital world. It is now generally accepted practice for (re)insurers to draw on a range of inputs, such as publications from researchers, specialist modelling firms, and cyber security companies. In conjunction with external inputs, underwriters and accumulation modellers may conduct their own research and discuss trends with in-house cyber security experts. In larger insurance companies, the traditional risk engineering function is evolving to include cyber and technology skills.

The common thread in these developments in exposure measurement and claims cost assessment is the shift from an essentially 'physical' world to a 'digital' world. Just as societies, industry and commerce are evolving, underwriting and the broader insurance value chain must also evolve. This evolution is not only changing the way underwriting is done but also the skill set of the underwriting function. In addition to requiring greater analytical skills, the underwriting profile must include a deeper understanding of data sciences and much greater familiarity with the technologies at the source of the underlying risk. In turn, this shift in required skill sets may be creating talent shortages in the industry.

2.5 Capability: Accumulation modelling

Model development—is it fast enough?

Discussions with leading insurers, reinsurers and specialist modellers reveal a highly active field of development with data analytics, machine learning and other technological advances leading to a fast-moving model landscape.

Currently, (re)insurers rely on pragmatic—but solid—methodologies that assess proportions of total limits at risk against the currently known major scenarios of data breaches, cloud outage, widespread malware, and disruption to critical infrastructure. These deterministic, scenario-driven methods, with expert judgement applied, provide a working solution while more sophisticated and insightful models are being developed. Tangible progress is being made, but unsurprisingly, given the uncertainties in this area, there is a divergence of views as to the time it will take for models to achieve a mature state.

- ***For the bears***, the challenges of modelling cyber accumulations are highly significant and will take a decade or more to overcome. Data challenges are great, and even with technological advances in data gathering, data sets will be neither robust nor complete. Should this view prevail, capital providers, whether traditional or alternative, may be unwilling to provide funds at the levels needed to support expected market growth.

- ***The bulls***, however, hold the view that advances in technologies will provide the capabilities to understand and measure these new technological risks. In this view, data, far from being scarce, is abundant and it is only a matter of how to extract, capture and utilise it. Decades of experience in modelling natural catastrophe risk, although not directly transferable, provides a solid base on which the cyber modellers can build. New techniques are emerging that harness all the computational power of today's data processing and analytical tools, and so shorten the duration of the learning curve for cyber risk, with maturity perhaps around five years away.

Both views have their proponents, and both have compelling arguments. What is clear is that the modellers have decades of experience on which to build, and many new advanced technologies in their toolbox, while the subject of their modelling is a fast-moving and unpredictable target.

Unique characteristics, unique challenges

Cyber accumulation modellers, like individual risk underwriters, must deal with the idiosyncratic features of measuring exposures for cyber risk and assessing claims that may arise from these exposures. But over and above these challenges lies a unique problem: how to understand and measure the aggregation of risk in the hyperconnected digital world.

A property catastrophe model bases its accumulated exposures on a geographical 'footprint.' Within the footprint, total property values can be calculated, and properties assigned relevant data attributes to predict their vulnerability to loss. Loss event scenarios simulating a natural catastrophe, such as a windstorm, are then run against this exposure base. The footprint is intuitive and conceptually well understood (if not to say simple), and advances in the capture of data and relevant data attributes, such as geocodes and construction types, facilitate the production of highly granular databases. Modellers have turned to the sciences of meteorology and seismology for event scenarios and, aided by vast advances in computing power, are able to run thousands of scenarios across these granular exposures, with the outputs being probabilistic descriptions of potential event impacts.

It has taken property catastrophe modelling around 25 to 30 years to mature, and model builders have been able to benefit from decades and often centuries of observations detailing which perils and regions should be focused on. Probabilistic catastrophe models are now commonplace, enabling risk measures to be estimated with sufficient robustness for a range of capital providers to accept catastrophe risk with more confidence than before models became available.

For cyber risk, it is a challenge to even define a 'footprint,' let alone measure the exposure within it. Some leading practitioners talk of a 'confinement zone' to reflect complex and constantly evolving corporate systems and networks, both internal and external. Supply chains have become increasingly digitalized and, with the range of cloud-based services extending further along the value chain, aggregations 'in the cloud' lie both within and across industries. While specialised industry-specific software tools connect actors in one industry sector, more generic technologies are utilised across multiple sectors and, with the Internet of Things, connections reach into the homes of hundreds of millions of individuals. These varied connecting threads and digital 'monocultures' create an exposure base that is largely opaque, lacks hard boundaries and enables threats to permeate across sectors and countries.

Notwithstanding the above challenges, an annual study by Verizon, based on a set of nine common attack patterns and an extensive event database, shows that historically, attacks have tended to cluster by industry sector.[16] This is promising and suggests that the 'footprint' problem is not intractable, while recognising there is potential for cross-industry attacks as discussed below.

As with primary underwriting discussed earlier, the threats to the exposures are equally hard to determine. To the natural catastrophe modeller, even the strongest meteorological trends and fluctuations lead to only gradual changes in model parameters: the number of named storms in the hurricane season may be volatile but it is certain that the threat is a storm. Cyber threats—such as breaches, malware, and ransomware—are themselves evolving with thousands of attacks daily, millions of new viruses developed, and billions of records compromised annually.[17]

Dealing with interconnectivity

This high level of interconnectivity of cyber risk is widely recognised as one of its most concerning aspects. Interconnectivity arises in several ways—businesses interact in the digital world and so create connections between themselves, with the cloud being the most notable development in this regard. Cloud service providers (CSPs) now connect many commercial organisations that would otherwise have little or no dependency. Further, commercial entities often use common software—for example operating systems, accounting systems in their back office or systems for customer relationship management—or common hardware. These 'monocultures' create connecting threads both across and within industry sectors and present unprecedented challenges for risk assessment.

16 Verizon (2018).
17 McAfee and Center for Strategic & International Studies (2018).

Two scenarios that aim to encapsulate the potential for digital interconnections to give rise to substantial risk aggregations were defined and researched in 2017 by Lloyd's, in conjunction with Cyence.[18] These are a mass vulnerability attack and the hacking of a cloud service provider. After the mega-catastrophe of a terrorist attack on critical infrastructure, these two scenarios are currently considered to be the major accumulation threats.[19] Research continues to be active, with a more recent publication by Lloyd's and AIR Worldwide digging deeper into a 'cloud down' scenario and offering insights into potential solutions to this problem.[20]

It is not new that the growth in cloud computing is a major factor in the increased levels of interconnectivity in today's digital economies. In 2014, Zurich Insurance warned that cloud computing risks had parallels with the complex feedback loops introduced by derivatives and securitisation to the financial world, which ultimately exacerbated the financial crisis of 2008.[21] Certainly, increasing levels of cloud usage create a complex network of digital supply chains and, as has been learned in the physical world, for example in the Thai floods of 2011, complex supply chain networks may have embedded concentration points, creating the potential for system-wide 'single point of failure' losses. Today, cloud data backups are ubiquitous for both individuals and businesses. Furthermore, the range of cloud service models available means that the commercial sector has many options on how it can utilise the cloud—from a thin interface accessing software provided by the CSP, through to developing and managing operating systems and applications themselves on a platform provided by the CSP.

Until recently, the interconnectivity associated with clouds seemed an intractable problem for risk accumulation modellers. However, advances in capabilities to map CSP networks are now yielding much greater transparency. At least one modelling specialist has introduced an approach to trace the CSP networks and other digital relationships of an insured business and enable insurers to determine their specific exposure to a potential CSP failure. The approach, developed with technology firms, uses publicly accessible digital information to identify connections between firms and their cloud providers. With this detailed digital map it is possible to assess the impact on a business of a specific cloud outage or failure, a significant step in understanding the risks associated with cloud interconnections.

This innovation leverages technology to address a challenge generated by technology and, as such, illustrates how new ways of thinking are emerging to meet the challenges of cyber risk. It also offers the potential for primary insurers to move away from an averaging, market-share approach, which may hide major unplanned risk concentrations. This is a significant step forward in both understanding the risk overall and enabling a more detailed assessment of the risks in the portfolio.

Novel approaches are also emerging to address the unique challenges from widespread malware attacks. For example, the modelling firm RMS has been looking at the link between modelling of pandemic and cyber risks and is exploring similarities between the mathematics of epidemiology and the spread of viruses, worms and malware through computer systems. In analysing the mathematics of patterns of the spread of disease and pandemics, one can start to see the emergence of similar patterns in the way that computers and IT systems can be affected by malware, worms and other viruses. Understanding these patterns enables the modelling of such risks and a 'footprint' which can be adapted specifically to the cyber space. The pandemic models can thus start to inform and assist in the enhancement of cyber models. The information about the spread of the cyber virus, worm or malware can be combined with information about the behaviour of computer systems and their operability and functionality at other times. Although a framework is starting to develop to assist with interconnectivity, there is still a high level of uncertainty and lack of ability for the models to be calibrated over time to achieve their objectives of enabling the cyber insurance market to grow sustainably.

Furthermore, there is around 20 years' historical experience of malware attacks. While recognising that malware evolves as the systems it targets evolve, the growing volume of empirical data is enabling modellers

18 Lloyd's and Cyence, op. cit.
19 Lloyd's and Cambridge Centre for Risk Studies, op. cit.
20 Lloyd's and AIR Worldwide, op. cit.
21 Zurich Insurance and Atlantic Council (2014).

to understand the nature of this threat vector. The motivations and capabilities of the threat actors are a first step; whether the attack is for financial gain or (politically motivated) disruption will have a significant bearing on the footprint (the latter tending to be much wider).

Deepening the knowledge in this area can also cause risk concentrations to surface for particular insurers. For example, an insurer focused on a target industry sector could be especially vulnerable if that sector relies widely on a single common software package. (Losses that are perceived to be idiosyncratic to a specific insurer should be of special concern to underwriters and senior management as this can have a damaging impact on the credibility of that insurer). Hence, efforts to increase the level of granularity in the understanding of attacks are a priority for the modelling companies in supporting the industry.

In parallel to this, the growing volume of data provides greater appreciation of the nature of vulnerabilities, essentially the importance of strength in IT security. Patching cadence, susceptibility to social engineering, asset attractiveness and so on are all elements in developing models with a hierarchy of risk to enable better identification of major exposures. Insurers with larger market shares have data volumes that are sufficiently credible to help identify 'blind spots' which may be present in external scanning techniques and that could be vital to anticipating major trends.

From deterministic to probabilistic

Various reports covering major accumulation scenarios and the work being done internally by (re)insurers indicate progress is also being made in understanding the potential severity of major events, which is central to managing accumulation risks. As a leading underwriter said, "it is most likely not possible to consider all the ways hackers can attack, or how technology can fail, but by running unlikely assumptions against the portfolio, it is possible to determine a worst case."

But only being able to estimate the severity of events is not sufficient, and managing accumulations to worst-case scenarios will lead to a conservative position on risk acceptance, potentially limiting capital allocated to this market. Not allowing for the probability dimension also means it is not possible to adequately determine expected losses—the mean—and the volatility around the mean, both needed to determine an adequate price of risk from the standpoint of investors, which is an important prerequisite for the involvement of alternative capital. There is a need to improve the quality of the estimates of the probability of extreme events—the 'return period' in the industry's vernacular.[22] Ultimately, reliable probability distributions need to be an essential component of modelling for insurers and reinsurers—and especially for alternative capital providers.

Extreme events are by their nature few and far between, which makes for limited 'data points.' Modellers of natural catastrophes have addressed this challenge for many natural perils by reference to relevant sciences, such as meteorology and seismology. This has served well for perils such as windstorms. Today, the impact of hurricanes making landfall on the U.S. mainland in any season, although subject to intrinsic volatility, can be modelled with sufficient confidence to influence how insurers write business and structure their reinsurance protection. Likewise, reinsurers and the ILS market can assess the potential impacts on their portfolios and, for the latter, determine an adequate risk premium. This is key for the ILS market if it is to attract investors without specialist insurance knowledge.

For the cyber modeller, there is no analogous hazard science to draw on that can provide key parameters or expected relationships. Exposures are dynamic, and with threats constantly emerging, assessing event frequency is a formidable challenge.

To address these challenges, modellers are adopting multi-dimensional exposure bases, developed on new data standards, such as the Lloyd's common core schema for cyber exposure data mentioned earlier. As well as basic statistics about businesses, such as turnover and industry, these include measures of cyber security effectiveness, which is identified as a key data attribute for exposure measurement. These enriched data sets offer more predictive power when used with the techniques described below.

22 Return period, e.g. a '1 in 200-year event,' is used to express more intuitively the probability of that event (0.005 or 0.5 per cent in the case of a 1 in 200-year return period).

Regarding claims, although empirical data are often claimed to be scarce, there are substantial volumes of data on data breaches, and the growing number of significant actual events or 'near misses'—such as the ransomware attack WannaCry, the Dyn distributed denial of service attack, and system flaws such as Meltdown—provide valuable data points that underwriters and modellers can utilise to adapt and test their models. In an academic approach, Wheatley and co-authors have shown that despite the rapidly changing context and the short history of data breaches, statistical models can be derived (with the help of informed distribution fitting) that allow for a novel understanding of cyber risk.[23]

Counterfactual analysis, the discipline of reimagining historical events how they might have been or how they may differ should a similar event occur in the future, is another technique adding to the understanding of potential accumulations. The purpose of this approach is to widen the data set from merely historical data to include 'possible' plausible histories.[24] A transparent and well-structured analysis may provide a richer texture to data-poor models, and so-called 'downward counterfactuals' (where worse outcomes are imagined) can contribute to a better understanding of likely extreme loss scenarios.

In the light of these approaches, the often evoked paucity of data is a clear challenge, but innovative attempts to bypass data limitations are emerging.

Assessing the relationship between claims frequencies and multi-dimension exposure bases is a complex challenge, eluding conventional mathematical regression techniques, and it is here that actuaries and data scientists have brought into play techniques from other mathematical fields made possible by advances in machine learning. Decision tree algorithms, and the Random Forest approach, for example, are being used by some modelling specialists to predict outcomes from enriched exposure data.

With these developments to address the challenges of the dynamic exposure base and the limitations in historical claims data, cyber catastrophe models are progressing beyond the pragmatic 'stacking of limits' methods and are starting to have many of the qualities of their natural catastrophe counterparts, such as objective measures and the ability to stress test many scenarios.

More to be done

The progress made, for example in mapping cloud-related interconnectivity or using machine learning on more complex data sets, is encouraging in and of itself. But, just as importantly, it is an indication of how new technologies can be deployed to meet the challenges of technological risks and it offers some comfort that cyber accumulation risk can ultimately be well-modelled.

However, accumulation models for cyber are still work in progress. The modelling of the threat of widespread malware impacting many organisations in many countries is, as yet, not mature. This is hardly surprising given its sinister nature and the wide variety of potential variants, as has been seen in 2017. Furthermore, a sophisticated and determined attacker could execute repeat attacks resulting in multiple loss events, wreaking havoc on businesses and the insurance industry.

The potential for a large cyber-triggered event to have considerable impact on non-affirmative coverages is now recognised across the industry, and much is being done to quantify this. Although insurers' historical loss statistics for 'non-cyber' coverages do not include any material cyber losses (and neither does the pricing, which is a further consideration), a body of man-made disaster scenarios has been developed over many years. Covering many events, such as aviation disasters, oil rig explosions, chemical plant and power grid failures, these scenarios can readily provide a sense of the scale of a cyber-triggered event. Insurers are able to leverage the extensive modelling work that has already been done for these man-made catastrophes but with a recalibration for cyber as a loss driver. This will further enable strategic discussion on risk mitigation, engineering, pricing, and reinsurance buying.

23 Wheatley. et al. (2016).
24 Lloyd's and RMS (2017).

This is a complex process, however, and from the insurance industry's standpoint, there are further layers of uncertainty as to how legal systems in various jurisdictions will interpret policy wordings following a cyber event. A full and robust assessment of these exposures is essential to provide confidence to the boards of (re)insurers and investors.

With respect to data, the current situation seems to be considerably better than some would state. However, the level of granularity of exposure data, and the need to ensure it is sufficiently complete when aggregated for accumulation models, means it will take time to reach standards comparable to equivalents in natural catastrophe modelling.

2.6 Capital availability

Despite its rapid growth, the market for affirmative cyber cover is still a fraction of the size of other commercial lines; total global premiums of under USD 4 billion represent less than 1 per cent of global commercial property premiums. At this level, for a large insurer, and considering the specific policy limits imposed, the overall balance sheet is unlikely to be significantly impacted by losses from a major event that arise on its affirmative portfolio. Some smaller insurers may be less insulated since even a small cyber portfolio could represent a significant amount of limit exposed to an unidentified concentration, and it is plausible that some players may have overweighted their aggregate cyber exposure. This means that for the time being, larger (re) insurers can rely on the more pragmatic, deterministic approaches to accumulation management, giving time for the modelling discipline to progress. Moreover, there is currently a strong inflow of new entrants, perhaps drawn to the attractive loss ratios and promising growth prospects, although this may present risks to the underwriting discipline so far demonstrated by market participants.

Against the backdrop of these developments, it is fair to say that capital is currently not a constraint to the growth of the cyber insurance market. However, penetration rates are low, and total available coverage for large customers falls short of demand. As the high-profile nature of major events and data-related issues make customers increasingly aware of the potential consequences of a cyberattack, and as much tighter data regulations take effect, one can expect very significant growth in the demand for cyber coverage. The industry needs to be able to respond to this. It will require more capital allocated to cyber, but also an increase in the amount of technical talent available to underwrite this business. A talent bottleneck could stall growth or, even worse, the market could stray from its disciplined approach to underwriting.

Should a catastrophic event occur, there is a clear potential for high losses across many portfolios—certainly outstripping the premiums earned on the affirmative covers. In such a scenario, demand will rise substantially as businesses already suffering from the impact of the event seek to protect themselves. At the same time, supply will likely drop as insurers withdraw from the market. In this scenario, there may be a view that there will be a strong inflow of new capital to the market, as has often been seen in the aftermath of large natural catastrophes. However, the potential for consecutive and potentially large cyber events could deter investors from entering the market.

Alternative risk transfer

Several other classes, largely with natural catastrophe exposure but also some life and motor liability classes, attract additional capital through securitised instruments. These ILS have developed over the last 20 years and bring non-insurance capital to the insurance market.

In recent years, the amount of ILS capital has risen steadily as investors from outside the insurance industry have become more familiar with ILS products and as their performance has built confidence in the risk-return dynamics of such instruments.

While recognising that the capital markets are constantly looking for new investment opportunities, it will likely take some time for cyber-based instruments to enter the ILS mainstream for the following two reasons:

- First, there is a high level of uncertainty around the potential size and nature of a large event and a lack of maturity of probabilistic models supplied by model vendors, which are needed to provide quantification on the severity and probability of large events. The growth of the ILS market has been predicated on a rigorous analytical discipline, and ILS managers—and their customers—typically have high requirements when measuring and assessing the appropriate risk premium. Although probabilistic models are now appearing, the ILS market will likely require more maturity.

- Second, the interest from ILS capital providers may be muted since cyber accumulation risk, unlike natural catastrophe risk, is unlikely to have a low—or even any—correlation with other financial asset classes. The constant stream of data breaches and ransomware attacks is a recognised economic drag, adding to the cost base of many industries and showing how cyber risk is inextricably linked to the economy. The economic impact of a major event has yet to be experienced—perhaps disrupting a major industry sector—and the reaction from financial markets has yet to be seen, but there may well be some positive correlation, perhaps to a significant degree.

This is not to preclude the possibility that some ILS managers will look to develop products despite the current limits to quantification if there are investors with a corresponding risk appetite.

Industry Loss Warranties (ILWs) are parametric instruments that can enable risk transfer to both traditional (re)insurers and alternative capital providers. An ILW contract offers protection based on the total loss arising from an event to the entire insurance industry, rather than the losses of the party purchasing the contract, with the industry loss forming the base for payouts being independently assessed.[25] For many reasons, ILWs are easier to design, more flexible and less prone to moral hazard. They lend themselves to standardisation, which helps in avoiding many of the administrative complications of mainstream reinsurance programmes. However, there is basis risk, as a result of the mismatch between the buyer's losses and the protection purchased if the buyer's book of business and the reported industry-wide losses are not perfectly correlated. Providers of ILW contracts are typically familiar with the risk profiles of the insurance markets, being either market participants or specialist hedge funds. As such, providers of ILW contracts tend to have a greater appetite for new or difficult risks and hence could have more appetite for cyber accumulation risk. At the time of writing there are two providers in the market, with the loss estimates for these contracts being based on the PCS cyber ILW index launched in September 2017, and there are a number of potential buyers, including some primary insurers.

Pools and backstops

For a quarter of a century, the use of pool arrangements with governmental support has been successful in securing additional capacity in areas with extreme event potential, such as terrorism, nuclear and natural catastrophes. In the man-made catastrophe space, a number of the pools that were initially established to provide a backstop against terrorism losses are now evolving to include cover for events caused by cyberterrorism. To cite just a few examples: Pool Re, the government-backed entity set up in the U.K. in the early 1990s has extended its cover, effective April 2018, to include material damage and business interruption from cyber-triggered acts of terrorism. In the U.S., authorities clarified that stand-alone (or affirmative) cyber liability policies will be included under the Terrorism Risk Insurance Act (TRIA) of 2002, as amended in 2015.[26] France, Belgium, Spain and South Africa have also included cyberterrorism coverage, and similar developments are under way in Australia.

On a global level, the International Forum for Terrorism (Re) Insurance Pools (IFTRIP) was established in 2015. It provides a mechanism for individual government pools to collaborate more closely on issues of concern to the pools as a whole. Although involvement on cyber insurance to date has been limited, there appears to be potential to provide coverage for the top layer of cyber threats through its member pools.

As well as providing capacity for a major event, several further benefits for a government-backed pool have been cited, for example in a report on the insurability of cyber risk.[27] These include improvements in data availability, improvements in risk diversification, and better representation of the interested parties (insureds, insurers and reinsurers) with governments and authorities. These benefits are tempered by some negatives—a pool is essentially a market intervention—including less differentiation in the market and reduced incentives for innovation.

Given the critical importance of cyber security to the private and public sectors, and the risk to critical infrastructure, there are strong arguments for governments to help insurers provide risk protection. Furthermore, this would harmonise with governmental activity in the area of cyber resilience.

25 Property Claims Services (PCS), a division of the Insurance Services Office (ISO), is usually the source for loss estimates in the U.S.; SIGMA, a division of Swiss Re and Munich Re's NatCAT Service, for non-U.S. business.
26 See Aon (2017a) for background.
27 Eling and Wirfs (2016).

Dealing with cyber acts of terrorism and war

The challenge in differentiating a cyber event from cyberterrorism is attribution. Terrorism pools covering cyberterrorism differ as to how they attribute acts of cyberterrorism. Even pools with strict procedures are employing a case-by-case approach. The determination is likely to be dependent on the strength of the links between the attacker and a terrorism organisation. This is an imperfect system. Even where cyberterrorism is insured by a pool, challenges exist and attribution remains subjective. The difficulties in the attribution or certification can conflate the issue of coverage. Insurers and pools may disagree about the allocation of losses between them. As summarised in the table, a number of terror pools currently cover cyberterrorism or are at different stages of expanding to incorporate such cover.

	Coverage	Criteria
USA	All lines	1. 'Act of terrorism' has occurred and was violent or dangerous to human life or property. 2. Losses must exceed USD 5 million in the aggregate before certification. 3. Certified as an 'act of terrorism' by three government agencies. 4. To activate programme, aggregate industry losses must exceed USD 160 million. 5. Payments will be made by the insurer and TRIA. Lines covered: Commercial property, casualty liability, workers compensation.
BEL	All lines	No specific process for cyberterrorism; standard procedure as applied to an 'act of terrorism'.
ESP	All lines	Cyberterrorism is treated as an 'extraordinary risk' for which coverage may be applied. The challenge is lack of a clear procedure in place to differentiate between a standard cyber event and a cyberterrorism event. Lines covered: residential property, commercial property, industrial property, civil works, motor, railway, life, personal accident and business interruption.
FRA	Property damage Business interruption	1. Cyberattack must result in a strong violation of public order. 2. Cover limited to policy terms, conditions and limits under property insurance policy as ceded to the French pool (GAREAT).
GBR	Property damage Business interruption	1. Certification that 'an act of cyberterrorism' and loss to commercial property or business interruption have occurred. 2. Pool Re refers the matter to the government to also certify that the event was an act of terrorism. 3. Once both Pool Re and the government have certified, Pool Re can pay out claims.
ZAF	Property damage	No specific process for cyberterrorism; standard procedure as applied to an 'act of terrorism'.
AUS	Under review	Extension of pool to include cyberterrorism is a key area for analysis in the 2018 triennial review. Lines that may cover cyberterrorism in the future are property damage and business interruption.

3. Enabling cyber resilience

In the digital economy, finely-tuned and highly complex just-in-time supply chains are susceptible to disruptions of IT infrastructures. An insurer's loss compensation to one affected link in the supply chain does nothing to lessen the harm caused further down the chain or at the customer endpoint. And if the frequency of claims cannot be contained, then 'day-to-day' losses will in effect become uninsurable, as there is no economic logic or business rationale to insure events that are highly likely to happen.[28] *It is therefore in the best interest of corporations and insurers to avoid disruptions as much as possible. In that sense, business resilience is a prerequisite for any insurance market. This cannot happen in isolation. Other stakeholders—technology providers and governments—must also contribute. This chapter will refer only to a few key concepts.*

3.1 The role of the corporate sector

Many studies have documented the reasons why corporations fail to properly address cyber risk management. The challenge is to consider the true complexity of organisations: the unseen interdependencies between people, processes and data, as well as supporting technologies. While the scale, scope and complexity of businesses vary widely depending on the industry (whether manufacturing or services), all include the above four components. The synthesis of these components needs rigorous quantitative techniques, such as systems engineering, which was developed to manage large, complex systems (the International Space Station being an example that has passed the test of time). The prevailing qualitative approaches are increasingly recognised to be only partially adequate against sophisticated and determined adversaries.[29] From such a comprehensive perspective, cyber resilience is more than just 'being prepared in the face of adversity.'

Done properly, resilient businesses share common characteristics.[30] They rely on more secure processes and systems; they have implemented strong controls; and they have harnessed the powers of digitalization to automatically analyse the risk environment, detect deviations from the norm and initiate corrective action. Resilient businesses that control risk at the source are also more likely to reduce the potential for moral hazard, which is an important prerequisite for insurers to provide coverage. Most important, however, is the implementation of a solid risk culture encompassing all levels of management and all departments in the organisation. Collective efforts are needed to combat the threats, and everyone has a role to play in minimising the 'human errors' which often provide a gateway that can be exploited by cyber adversaries.

3.2 Technology providers

If the use of technology causes problems, can investments in even more technology deliver a solution? There are indeed many good reasons why firms should spend more on application and data layers and why they should step up investments in technology. However, throwing money at a problem may not always produce the desired results. Firms are indeed investing on a large scale, but much of it may be "misdirected toward security capabilities that fail to deliver the greatest efficiency and effectiveness."[31] Therefore, technology must be complemented by human intelligence because "it is not the number of technologies that make an enterprise resilient, the key is how well the enterprise utilizes those technologies."[32]

This assigns an important and, in many ways, new role to technology providers. As a recent report states, technology players should not only limit themselves to innovation, they should also become "stakeholders in shaping the future of risk mitigation. The technology industry has deep knowledge, data science and related

28 Hiscox (2018) reports cyber loss frequencies at around 50 per cent, rendering the cost of claims effectively a tax on business, which could make it a real concern.

29 The systems engineering approach with respect to cyber risk is in use, for instance, in The Institution of Engineering and Technology's 'Code of Practice: Cyber Security for Ships,' available at https://www.theiet.org/resources/standards/cyberships-cop.cfm?

30 Allianz (2015), Cisco (2016), and PwC (2015) have good introductions to cyber resilience. The World Economic Forum (2017a) provides a comprehensive cyber resilience checklist for boards of directors.

31 Ponemon (2017).

32 Symantec (2014b).

risk expertise. As experts in this area, the industry's players have the opportunity and responsibility to take on a larger role in supporting the development of risk mitigation solutions."[33] This implies that security has to be built in at the very first stages of hardware and software development and that appropriate cyber hygiene must be promoted and adhered to at all subsequent stages and by all users. Security by design will be a particularly important feature in the future Internet of Things (IoT) environments, in which any device will be linked to a multitude of other devices.

3.3 Governments

Governments enter on both sides of the cyber risk equation. First, some governments have tools to engage in a broad spectrum of malicious and hostile activities, ranging from interfering with social media, espionage, sabotage and outright cyber warfare, and some have actively engaged in all of them. Second, and more important for the purpose of this report, they are also targets for malicious attacks. And just as the private sector, governments can be victims of malfunctioning hardware and software and suffer adverse consequences of negligent or malicious employee behaviour. In fact, industry observers believe that "the public sector faces more security incidents and data breaches than any other sector."[34]

Given that the public sector collects and stores large volumes of sensitive data (about individuals but also about procurement programmes) it must take utmost care to ensure the integrity of data stored in its systems. And since it is subject to the same incident patterns and potentially targeted attacks, it must use the same response toolkit applied by the private sector. Government agencies must deploy forward-looking risk management to make the public sector more resilient in cyberspace.[35]

3.4 The role of insurers

If the resilience prerequisites are in place, the contribution of insurers in the cyber risk space is not any different from the fundamental role the industry plays in our economies and societies. To absorb the financial consequences of risk, insurers must properly assess and adequately price the risk underlying an insurance transaction. In market economies, prices are signalling devices for the allocation of scarce resources and production factors. And by putting a price on risk, including cyber risk, insurers contribute to the efficient working of our economies.

However, loss absorption based on risk-commensurate pricing is only one part of insurers' contribution to the mitigation of cyber risk. Equally important are their contributions before, during and after cyber events. This includes educating customers about risks and vulnerabilities, helping them in managing risks, and promoting cyber resilience. For these reasons, insurers are increasingly offering a wide range of services along the entire value chain. This is also true, and likely to grow in importance, in the line of cyber risk insurance.[36]

Other parties (such as consultants) also provide valuable insights for the mitigation of cyber risk and the strengthening of cyber resilience. A veritable flood of publications attests to their productivity. But the contribution of insurers is different in one fundamental point: insurers are absorbing policyholder risks on their own balance sheets. And by putting capital at risk, insurers have 'skin in the game' on behalf of their customers. This will arguably go a long way towards aligning the interests of policyholders and insurers and making the insurance offering an effective risk mitigation tool.

33 World Economic Forum (2017b).
34 Verizon (2015).
35 Eggers (2016).
36 See The Geneva Association (2018b) for a detailed analysis of insurers' service offerings in the cyber space.

4. Policy implications

As stated in Chapter 2, the sustainable growth of the cyber risk insurance market must build on three prerequisites. These requirements have implications for practices implemented by insurers, as well as policies governing the functioning of financial markets in general and insurance markets in particular. This chapter provides a preliminary overview of policy issues, mainly triggered by the insights gained from the treatment of accumulation risk.

Given the fluid stage of market developments, it would be premature to make firm policy recommendations. At this point, the objective should be to 'do no harm.' Prudence suggests to refrain from making irreversible decisions. Policymakers should rather endeavour to use the market as a discovery mechanism and expect best practices to be adopted quickly by competitors and new market entrants. These practices are likely to go a long way towards dealing with the issues discussed in this paper.

In line with the three prerequisites, there are several policy measures that are likely to bring the insurability of cyber risk within reach, and deliver risk models that can serve as a basis for capital allocation.

4.1 Strengthen risk modelling and facilitate policyholder access

- Insurers could reduce opacity by standardising event definitions. This would clarify the nature of the insurance offering, which could reduce what is perceived as high (and probably unnecessary) product complexity.
- To reduce market barriers, special attention could be given to the needs of small and medium enterprises (SMEs) with the objective to make cyber insurance products better accessible and more affordable.
- Insurers and authorities could work jointly towards data and information sharing that goes beyond mere reporting and one-way notification. Such two-way intelligence sharing should be efficient, secure and robust. Public-private information sharing should also be transparent and not give rise to an additional risk of enforcement actions or liability claims as a result of cyberattacks.
- Jointly with the industry, authorities could work towards appropriate international frameworks to enable the development and maintenance of standardised databases for cyber incidents similar to the databases developed for natural catastrophes. They could build on work done by the CRO Forum which has defined a standardised insurance classification for the monitoring of cyber risk.[37]

4.2 Strengthen resilience at the source of risk

Despite recent widespread data breaches and ransomware attacks, take-up rates of cyber insurance remain at relatively low levels—less than 15 per cent.[38] Many customers, particularly in the SME segment, continue to be unaware of risks and available cover. Some lack of sophistication may be due to buyers' ignorance, but insurers also seem to carry some of the blame for the observed underinsurance. Only 13 per cent of brokers polled by the CIAB said that insurers gave adequate clarity on policy coverages and exclusions.

These data points indicate that proactive measures by the insurance industry to increase risk awareness and induce corporations to engage in cyber risk management would go a long way towards reducing underinsurance. Moreover, if one accepts that using insurance is a signalling device for the pricing of risk, a growing cyber insurance market would contribute to a better use of resources and thereby increase overall economic efficiency. The policy measures to be vetted could include a number of initiatives:

- Cyber security features should be developed and implemented at inception, and security design features should be certified and controlled by official authorities.
- Authorities could enforce measures to ensure the cyber ecosystem does not fall into a monoculture trap (such as broad-based reliance on one single piece of hardware or on one operating system).

37 CRO Forum (2018).
38 According to a recent survey for the U.S. market; see CIAB (2017).

- Jointly with IT security providers and insurers, authorities should develop and implement minimal IT and information security standards. Standards should be risk-adequate and principles-based, and they should include some degree of international coordination and cooperation among national and regional supervisors.

- Governments could consider becoming signatories to a 'Digital Geneva Convention', which would contain—similar to agreements governing the non-proliferation of nuclear weapons—the use of cyber weapons by governments.[39]

4.3 Facilitate market-based access to capital

Publicly-listed insurance companies must compete for capital against other listed financial and non-financial corporations. Policymakers should therefore ensure that insurers are not burdened with capital requirements that artificially depress the returns on equity capital provided by shareholders. Capital requirements should be comparable across industries while being mindful of the risks and complexities inherent in the insurance business. The proportionality principle must apply.

The requirement that insurers should be able to earn risk-commensurate returns on capital also has implications for underwriting. Regulation should instil prudent and disciplined underwriting and not interfere with the need for the risk-based pricing of cyber risk.

4.4 Facilitate access to sufficient capital

While access to sufficient capacity does not seem to be an issue at this time, current trends make it likely that the industry must eventually absorb large, unexpected losses. This makes access to capital sufficient to absorb such losses paramount. In consultation with the industry, supervisors should therefore start thinking about the adequacy of stress tests applied under current solvency regimes.

There are many good reasons to assume that strengthened capital requirements may not be the appropriate response to the cyber risk challenge. This makes it imperative to explore other policy and regulatory measures to ensure the insurability of cyber risk. They could include:

- Pooling solutions to include cyberterrorism. For more than a century, government-sponsored pooling schemes have demonstrated their usefulness for other seemingly uninsurable risks, such as nuclear and terrorism risks.

- Broad governmental backstops related to cyber losses (in addition to losses triggered by terrorism). Such backstops could signal to the market that governments too have 'skin in the game' and are prepared to contribute to solutions developed by private market participants. Governmental backstops could thus be seen as providing confidence to the market, thus potentially unlocking capacity that otherwise would remain on the sideline.

39 Such a non-proliferation convention was recently proposed by Microsoft (2017).

5. Summary and scorecard

Although cyber is different in many ways, the (re)insurance industry has taken several steps towards making the risk manageable. Insurers and reinsurers have demonstrated they can successfully underwrite cyber risk. Underwriting discipline is strong and, given the absence of large events, this has resulted in good profitability.

Table 5.1 provides a summary of the industry's progress in developing the technical capabilities of exposure measurement, claims cost assessment and accumulation modelling to handle the distinct characteristics of cyber risk, namely:

- Exposure bases are hard to define and measure, and they are constantly changing;
- Historical claims data are scarce and not representative of future vulnerabilities;
- Threats are constantly evolving—they can spread widely and rapidly, and recur;
- A high degree of interconnectivity is leading to potentially unbounded impacts.

In accumulation modelling, the developments have been fast and extensive. Models range from pragmatic approaches—which provide comfort for worst-case exposures—through to technically and mathematically advanced approaches. Specific advances include granular assessments of cloud-related interconnectivity challenges and increasingly detailed stochastic scenario assessments for malware/monoculture challenges.

Table 5.1 Challenges and responses in the cyber insurance market

Cyber characteristic	Capabilities impacted	Industry response	Ongoing issues
Exposures hard to define and measure; constantly changing.	Exposure measurement.	Establishment of core data schema; Digital risk assessments at the insured level.	Technical nature of exposures very different from other classes—difficult to learn and creates talent issues.
Claims data scarce and not representative of future vulnerabilities.	Claims assessment; Modelling.	Utilise breach data and publicly available data on major events to generate scenarios.	Insurers may be wrong-footed by unseen threats or trends deviating from expectations.
Threats evolve constantly, spread widely and rapidly, and can recur.	Claims assessment; Modelling.	Forward-looking threat assessments including external expert inputs; Develop in-house technical know-how.	
Highly interconnected with potentially unbounded exposure.	Accumulation modelling.	Mapping cloud and digital supply chains; Machine learning (ML) for complex relationships between exposure and claims.	Malware still a major threat; Non-affirmative cover exposure not assessed; Yet to assess ML effectiveness.

Paucity of data, whilst undoubtedly considered an issue, may be more manageable than is generally thought. There are innovative approaches to bypass limitations and wider mathematical methodologies being deployed to analyse the data gathered. However, even the most advanced model needs data that is of robust quality and, for accumulation models in particular, ensuring completeness of data is a key challenge. Many jurisdictions do not have the same level of reporting requirements for data breaches as in Europe and the U.S., hindering efforts to compile a global picture of cyber losses.

The advances in modelling support a greater understanding of risk interconnectivity, whether wide-scale in nature through cross-cutting digital 'monocultures' or because of businesses' digital interactions and supply chains. The more granular understanding not only supports a better assessment of overall exposures but, importantly, improves underwriters' ability to understand their portfolio concentrations and so helps to widen the volume and variety of coverage levels they can provide.

Although developments in the industry's capabilities are encouraging, a note of caution is appropriate. The history of cyber risk is short, and the market has yet to experience a major adverse event. It is vulnerable to risks, and without due attention there is a potential of slipping into undisciplined underwriting.

A single major event, or a series of consecutive events, could render the market unprofitable. Likewise, underestimation of exposure, especially non-affirmative, could result in significant, unanticipated losses. Lack of discipline in policy wording, especially to control exposure to acts of terrorism, is a key concern. Under such scenarios, a sizeable withdrawal of market capacity could ensue, with tighter policy conditions, wider exclusions, and price hikes in cyber-specific covers. Such a setback could have potentially significant negative impacts on business confidence and the wider economy.

References

Allianz (2015) *A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, available at https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

A.M. Best (2017) *Cyber Line Expected to be One of the Leading P/C Growth Areas*, Best's Special Report, available at http://www.bestweek.com/europe/promo/CyberLinePCGrowthAreas.pdf.

Aon (2017a) *U.S. Treasury Makes Standalone Cyber Insurance Policies More Valuable*, available at http://www.aon.com/attachments/risk-services/cyber/TRIA-2017Update.pdf

Aon (2017b) *Global Cyber Market Overview: Uncovering the Hidden Opportunities*, available at http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf.

Cisco (2016) *Cyber Resilience: Safeguarding the Digital Organization*, available at https://static.ziftsolutions.com/files/ff8081815a29e70c015a43528326532d/cyber%20resilience%20white-paper-c11-736966%20(1).pdf.

CIAB, The Council of Insurance Agents & Brokers (2017), *Cyber Insurance Market Watch Survey*, December edition, available at https://www.ciab.com/topic/cyber-survey/.

CRO Forum (2018) *Supporting On-going Capture and Sharing of Digital Event Data*, available at https://www.thecroforum.org/2018/02/21/supporting-on-going-capture-and-sharing-of-digital-event-data/

Eggers, W.D. (2016) Government's Cyber Challenge: Protecting Sensitive Data for the Public Good, Deloitte Review, Issue 19, pp. 139-55, available at https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html.

Eling, M. and Wirfs, J.H. (2016) *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class*, available at https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

The Geneva Association (2018a) *Understanding and Addressing Global Insurance Protection Gaps*, available at https://www.genevaassociation.org/research-topics/protection-gap/understanding-and-addressing-global-insurance-protection-gaps.

The Geneva Association (2018b) *Cyber Insurance as a Risk Mitigation Strategy*, available at https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

Hiscox (2018) *Cyber Readiness Report*, available at https://www.hiscox.de/hiscox-cyber-readiness-report/.

Johansmeyer, T. (2018) *Unleashing the Potential of the Cyber Insurance Market*, presentation to OECD conference, Paris, available at http://www.oecd.org/daf/fin/insurance/Presentations-Conference-cyber-insurance-market.pdf.

KPMG (2017) *Cybercrime Survey Report: Insights and Perspectives*, available at https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf.

Lloyd's and AIR Worldwide (2018) *Cloud Down: Impacts on the US Economy*, available at https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down?utm_source=Presentation_screens&utm_medium=Presentation_screens&utm_campaign=emergingrisks_clouddown.

Lloyd's and Cambridge Centre for Risk Studies (2015) *Business Blackout: The Insurance Implications of a Cyberattack on the U.S. Power Grid*, available at https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/space-and-technology/lloyds-business-blackout-scenario/.

Lloyd's and Cyence (2017) *Counting the Cost: Cyber Exposure Decoded*, available at https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost.

Lloyd's and RMS (2017) *Reimagining History: Counter Factual Risk Analysis*, available at https://www.lloyds.com/news-and-risk-insight/press-releases/2017/10/what-if.

McAfee and Center for Strategic & International Studies (2018) *Economic Impact of Cybercrime— No Slowing Down*, available at https://www.csis.org/analysis/economic-impact-cybercrime.

Microsoft (2017) *A Digital Geneva Convention to Protect Cyberspace: Microsoft Policy Papers*, available at https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

Ponemon Institute (2017) *Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference*, available at https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

PwC (2015) *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*, available at https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

Symantec (2014) *A Manifesto for Cyber Resilience*, available at https://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf.

Symantec (2014b) *The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence*, available at https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilient-enterprise-wp-21332471-en-us.pdf.

Verizon (2015) *Data Breach Investigations Report*, available at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf.

Verizon (2018) *Data Breach Investigations Report: Tales of Dirty Deeds and Unscrupulous Activities*, available at https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

Wheatley, S., Maillart, T. and Sornette, D. (2016) *The Extreme Risk of Personal Data Breaches and the Erosion of Privacy*, ETH Zurich, Department of Management, Technology and Economics, published in *The European Physical Journal B*, 89(7), available at https://link.springer.com/article/10.1140/epjb/e2015-60754-4.

World Economic Forum (2017a) *Advancing Cyber Resilience: Principles and Tools for Boards*, available at http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

World Economic Forum (2017b) *Mitigating Risks in the Innovation Economy: How Emerging Technologies Are Changing the Risk Landscape*, available at http://www3.weforum.org/-docs/WEF_Mitigating_Risks_Innovation_Economy_report_2017.pdf

Zurich Insurance and Atlantic Council (2014) *Beyond Data Breaches: Global Interconnections of Cyber Risk*, available at https://www.files.ethz.ch/isn/182163/Zurich_Cyber_Risk_April_2014.pdf.

Appendix

(Status June 1, 2018)

A.1 Members of The Geneva Association's Cyber Risk Working Group

Tracie Grella, AIG
Catharina Richter, Allianz (until January 2018)
Henning Schult, Allianz
Patrick Smolka, HDI (until January 2018)
Philipp Lienau, HDI
Alain Lessard, Intact Financial
Keith Smith, Lloyd's
Daljit Barn, Munich Re
Chris McEvoy, Partner Re
Eric Durand, Swiss Re
Ryusuke Yoshida, Tokio Marine
Regina O'Connor, XL Catlin
Mark Radice, Zurich Insurance Group (until April 2018)
Mark Bannon, Zurich Insurance Group

A.2 Cyber experts in The Geneva Association members' firms

Anthony Shapella, AIG
Jenny Soubra, Allianz
Sebastian Wendler, HDI
Caroline Dunn, Lloyd's
David Clousten, Lloyd's
Holger Glaab, Munich Re
François Bisson, Swiss Re
John Coletti, XL Catlin
Vinita Saxena, XL Catlin
James Tuplin, XL Catlin
Lori Bailey, Zurich Insurance Group
Stephan von Watzdorf, Zurich Insurance Group

A.3 Experts consulted in other organisations

Mark Banks, AIR Worldwide
Scott Stransky, AIR Worldwide
Visesh Gosrani, Cyence
Jonathan Cunnison, RJD Technology
Russell Searle, RJD Technology
Tom Harvey, RMS
Gordon Woo, RMS
Tom Johansmeyer, PCS
Geoff Riddell, Pool Re
Julie Fitzgerald, PwC
Reto Haeni, PwC
Dirk Lohmann, Sequaero

The characteristics of cyber risk imply that exposure measurement and modelling approaches that have been developed for other perils cannot easily be transferred to cyber risk. Accumulation risk is a key concern. This report identifies essential challenges of cyber accumulation risk, and looks at how the insurance industry is responding to an environment where a high degree of interconnectivity could lead to potentially unbounded impacts from threats that are constantly changing, can spread widely and rapidly, and recur.

The Geneva Association—International Association for the Study of Insurance Economics
Talstrasse 70, CH-8001 Zurich | Tel: +41 44 200 49 00 | Fax: +41 44 200 49 99
secretariat@genevaassociation.org