



Unleashing the Potential of the Cyber Insurance Market

CONFERENCE OUTCOMES

22-23 February 2018
Paris, France

About this conference

The growing reliance on digital technologies - while creating significant opportunities for innovation, convenience and efficiency - comes with digital security and privacy protection risks. The potential role of the nascent cyber insurance market in enhancing cyber resilience is increasingly being recognised by policy makers. This conference will provide an opportunity to exchange knowledge and share experience among policy makers, risk managers and insurance market participants on addressing the challenges impeding the development of the cyber insurance market.

About the OECD

The OECD plays a leadership role in supporting the development of strategies for the financial management of natural and man-made disaster risks and has provided guidance and analysis on these issues for the G20 and APEC Finance Ministers. This work is undertaken under the guidance of the High-Level Advisory Board on the Financial Management of Large-scale Catastrophes and the Insurance and Private Pensions Committee. The OECD provides a unique forum for governments to compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

About MMC

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The company's nearly 65,000 colleagues advise clients in over 130 countries. With annual revenue over \$14 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. [Marsh](#) advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. [Guy Carpenter](#) develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. [Mercer](#) delivers advice and technology-driven solutions that help organizations meet the health, wealth and career needs of a changing workforce. [Oliver Wyman](#) serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit mmc.com, follow us on [LinkedIn](#) and Twitter [@mmc_global](#) or subscribe to [BRINK](#).

Photo credits: OECD/Andrew Wheeler

CONFERENCE HIGHLIGHTS

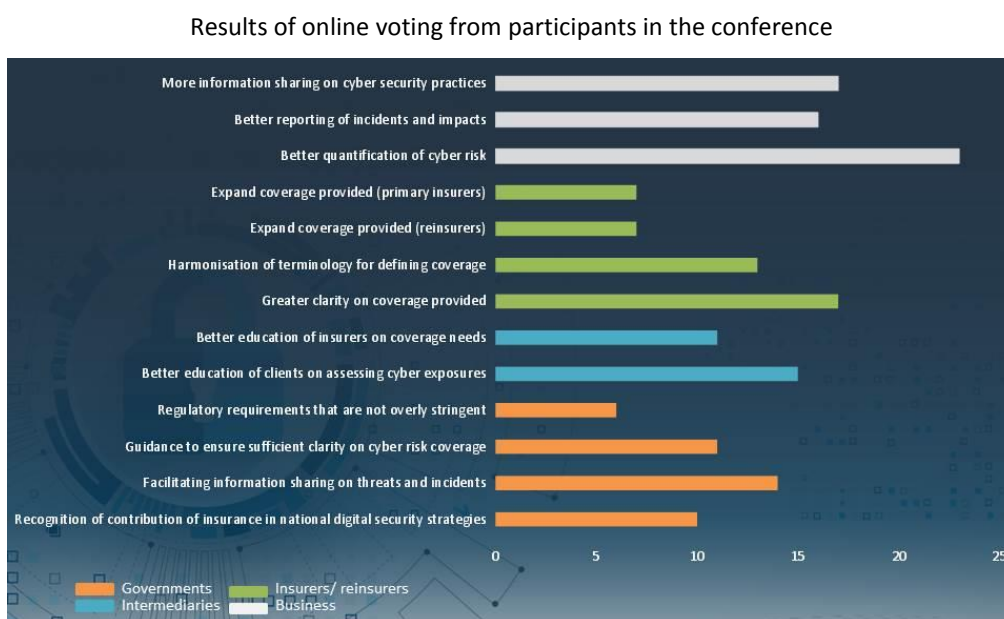
On 22-23 February 2018, the OECD, in collaboration with Marsh & McLennan Companies, brought together approximately 200 government officials and representatives from business and the cyber insurance and reinsurance sector from around the world to identify the challenges to the development of the cyber insurance market and approaches to addressing those challenges.

Key takeaways:

- The growing digitalisation of the economy will continue to create challenges in terms of managing digital security and privacy risks. Action by all stakeholders will be required to ensure that these risks can be managed while allowing sufficient space for achieving the economic and societal benefits of digitalisation.
- There is significant potential for the cyber insurance market to contribute to improving cyber risk management. Substantial progress has been made in understanding, quantifying, modelling and developing insurance coverage for a risk that was barely understood even 20 years ago.
- However, the level of insurance coverage for cyber risk remains well below the levels of coverage for other perils, despite the potential for cyber risk to lead to significant economic losses. As a result, the cyber insurance market is not yet making the contribution that it could to encouraging risk management among policyholders.
- A number of challenges impede the extension of insurance coverage, including low risk awareness, lack of data on cyber incidents, the changing nature of cyber threats and the potential for accumulated losses.
- The needs and expectations of many businesses can diverge from the scope of coverage commonly provided by insurance companies, driving a need for continued education about the scope, purpose and coverage provided by existing cyber insurance products.

Participants were asked to vote during the conference about the relative importance of a set of actions that different stakeholders could take to support the development of a vibrant cyber insurance market (see Figure 1).

Figure 1. What actions would make the most important contribution to developing a vibrant cyber insurance market?



Businesses, intermediaries, (re)insurance companies and governments can all make a contribution to supporting the development of a market for cyber insurance coverage that enhances the resilience of society in the face of increasing digital security risks:

Businesses are ultimately responsible for protecting against cyber incidents that have negative consequences for their employees, customers and shareholders and should allocate sufficient resources into ensuring an appropriate level of cyber resilience.


- To effectively manage cyber risks, businesses should enhance their understanding of the risks that they face and the potential financial consequences. This assessment should be a standard element of an enterprise risk management approach.
- Businesses should contribute to an improved understanding of cyber risks by sharing information on the occurrence and impact of cyber incidents that have affected their operations and potentially by enhancing public disclosure of cyber risks and incidents. A mechanism for sharing (non-public) information needs to be established to ensure that the information shared will remain confidential. For businesses, there must be clear benefits in participating in information sharing arrangements.
- Businesses should augment the level of information on cyber security processes and practices that they share with underwriters who in turn must demonstrate their ability to protect sensitive information and add value as risk management advisors.

Insurance and reinsurance **intermediaries** have a critical role to play in bridging the gap between policyholder needs and insurance company offerings.

- Intermediaries should continue and expand their investments in educating their clients on how to assess their financial exposures and advising insurance companies on how to better aligning their products to client needs.

Insurance companies are responsible for developing (economically-viable) insurance products to address the risk management needs of their policyholders.

- Insurance companies should provide greater clarity on the coverage that they are offering for cyber risk and in which policies that coverage is being offered, including: (i) a clear statement about the coverage for cyber risk in traditional policies; and (ii) harmonised terminology for defining the coverage provided for different incident types and losses as well as greater consistency in terms of the triggers for that coverage, recognising that terminology may need to evolve as the nature of cyber risks changes.
- Insurance companies should aim to continue expanding the scope of coverage provided for cyber risks, including for existing risks not currently covered by insurance policies and for new types of losses that may emerge as a result of an evolving cyber risk environment, while ensuring that the risks involved in any expanded coverage provided are well-understood and will not harm their ability to meet their obligations to policyholders.
- Reinsurance markets (traditional and alternative) should continue to examine ways to expand the scope of coverage that they make available to primary insurers for cyber risks that are well-understood and do not create unmanageable levels of aggregation risk.



Governments' role is to support cyber resilience and the ability of businesses to better manage cyber risk, including through the use of insurance coverage where such coverage contributes to better risk management.

- Governments should recognise the potential contribution of insurance to risk management in national digital security strategies.
- Governments should facilitate information sharing on cyber threats and incidents by sharing the threat information available to them and encouraging greater disclosure and/or information sharing on incidents by affected businesses (including by addressing any legal impediments to information sharing). The needs of the risk management and insurance sectors should be taken into account when defining the information that needs to be submitted for regulatory notifications.
- Governments should monitor the cyber insurance market with the aim of ensuring that there is increasing clarity and declining complexity in the products that are being offered. Where necessary, guidance could be established to encourage greater clarity about coverage being offered (and should recognise the potential benefits of international coordination of regulatory and/or supervisory approaches).
- The regulatory and supervisory requirements imposed on insurance (and reinsurance) companies offering coverage should be proportionate to the level of risk and take into account the need to support a more efficient and resilient cyber insurance market.

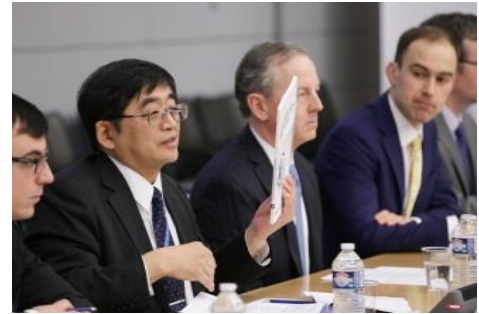
Governments should work with the insurance and reinsurance sectors to assess the potential implications of a cyber catastrophe (before one occurs) and the responsibilities of each in responding to such an event.

Leveraging its expertise in insurance and digital security risk management, the **OECD can contribute to helping overcome challenges to the development of the cyber insurance market**, including through additional research and analysis to support the implementation of these recommendations.

FOREWORD

Organisation for Economic Co-operation and Development (OECD)

Managing cyber risk is clearly an important and pressing issue. Cyber attacks and data breach incidents have been a top priority for businesses around the world for years. In the most recent World Economic Forum Global Risks Report, cyber attacks were identified as the risk of greatest concern to doing business in 11 OECD member countries – ranking above extreme weather events, terrorist attacks and other risks that have traditionally kept insurance underwriters awake at night. 2017 was one of the worst years in cybersecurity history, according to a recent report by FireEye and Marsh & McLennan, with ever more significant cyber attacks. There were global ransomware attacks in May affecting health services in the UK, rail services in Germany and other essential services. A second wave of ransomware attacks in June led to significant losses at a global logistics firm and a number of companies in the building materials, pharmaceuticals and other sectors not traditionally targeted by cyber attacks. In September, a data breach incident potentially affecting the most sensitive personal data of 1 out of every 2 American consumers was revealed. 2018 is unlikely to be much better, especially considering the revelation of a vulnerability in the central processing units of almost every desktop and laptop across the world.



Masamichi Kono
Deputy Secretary General, OECD

Insurance can play an important role in helping businesses and consumers manage cyber risks and providing policyholders financial protection against risks that cannot be fully prevented. It can also make important contributions by putting a price on risk - which is critical for making informed decisions on investing in prevention - and in helping companies reduce their risks. The OECD, through its Insurance and Private Pensions Committee and the High-Level Advisory Board on the financial management of catastrophic risks, has been examining the contribution of insurance to managing cyber risks since 2016. Based on responses to a questionnaire received from the insurance sector and from governments, the OECD presented an initial analysis to the G7 Finance Ministers and Central Bank Governors in Italy in May 2017. And in November of last year, we published a much more comprehensive report - *Enhancing the role of insurance in cyber risk management* - providing an overview of the cyber insurance market, challenges to its development, and some of the initiatives that have been put in place around the world to address these challenges.

While there have been insurance products to protect against certain cyber risks for close to 20 years - the cyber insurance market remains underdeveloped. Across OECD countries, cyber insurance accounts for less than 0.5% of gross written premiums in the non-life segment, and no more than 1% of the premiums collected for general liability and property coverage, which are the classes of insurance from which cyber insurance was derived. Insurance limits offered for cyber risks tend to be much lower than those offered for property or liability losses. In developed insurance markets, such as the US, UK and Germany - where commercial property insurance penetration rates approach 100% - cyber insurance coverage is acquired by 60% of all companies at most - and likely closer to 30% outside the US.

There are a number of challenges to the development of the cyber insurance market. Firstly, cyber risk is difficult to quantify, limiting both the demand for cyber insurance coverage and the availability of that coverage. There is also a potential for the accumulation of risk - which is particularly challenging in the case of cyber risk due to few geographical or sectoral boundaries to the propagation of cyber attacks. Systemic risk caused by cyber attacks is very hard to assess. And finally, cyber insurance is a complex product - with significant differences in terminology across different policies, different triggers, different coverages, different exclusions - and sometimes completely different approaches to providing coverage.

Increasing digitalisation will ensure that this risk will remain top-of-the-agenda for the foreseeable future. Policymakers have an important role to play in a number of areas that could contribute to the market's development.

Special address



John Q. Doyle
President & CEO, Marsh

The increasing use of technology has ushered in efficiencies and opportunities that have rapidly transformed business performance, along with many other aspects of our lives. The expanding digital ecosystem comes at a cost, however: increased vulnerability and exposure to cyber threats, which are growing in frequency and severity. Many government and industry leaders invited to this conference acknowledged the challenges in navigating the evolving cyber risk landscape.

Heightened awareness of cyber as a prioritised risk has been coupled with a corresponding increase in cybersecurity investment. But we have yet to see an improvement in cyber resilience – how effectively organizations manage cyber events. A logical conclusion to draw is that what we are doing is not working. **Specifically, the approach to cyber risk management is a developing science that is not keeping pace with the dynamic nature of cyber risk.**

So, how can we rethink our approach?

Business, insurance and government stakeholders each have a role in helping to find a better way.

Businesses need to treat cyber risk as an enterprise-level governance issue with broad stakeholder engagement. Two other ways the private sector can improve cyber risk management are quantifying cyber risk to gauge economic impact, and aiming for holistic cyber risk management solutions that incorporate planning, technology, insurance, and mitigation.

Within the insurance industry, we have a responsibility to better educate clients about the benefits of cyber insurance. We can also improve information sharing with key stakeholders. Marsh welcomes industry initiatives to develop efficient cyber risk governance models, as well as a breach notification template to help insurers access anonymised data collected under the GDPR.

Policymakers can continue to develop national strategies for cybersecurity and promote the development of best practices, which includes the adoption of cyber insurance. The OECD itself is playing an instrumental role in bringing cyber insurance to the forefront of policy discussions.

Results-oriented cyber risk management is important. We believe that cyber insurance can bring positive change in our economic communities, but there is still work to be done to realise its full potential. We look forward to continuing to support the OECD and carrying on the dialogue about this critical issue, as we work toward new solutions to anticipate and meet tomorrow's challenges.

Special address



Inga Beale
CEO, Lloyd's of London

Cyber insurance has huge potential but the cyber insurance market remains frustratingly immature and is not keeping pace with threats and technology. Whereas many businesses have property insurance, only about 20-35% have specific cyber insurance in the United States and Europe. The existing products do not always cover the losses most important for companies, such as the loss of their intellectual property or the reputational impact which creates a bit of understandable scepticism about the value of the product from the company's perspective. The cost of cyber insurance can also appear to be expensive when compared to other classes of insurance. In some cases cyber insurance is up to six times more expensive than property insurance and three times more expensive than liability insurance, according to some sources.

There are a few barriers blocking the development of the cyber insurance market, including the nature of the risk itself which is difficult to detect and evaluate, making it difficult to price from an underwriting perspective. There is very little actuarial data and limited knowledge on how to price in some of the other impacts from cyber incidents. Even where data is available, the potential for aggregation causes insurers to tread carefully. Unlike natural catastrophes, where billions have been spent on modelling, we don't know how to measure accumulation in cyber risk which has no geographic boundaries. The big events that have occurred, like WannaCry or NotPetya, have resulted in only limited insurance losses meaning these events have not contributed much to addressing this data gap. Lloyd's has done a lot of research into these issues, identifying potential scenarios - not to scare people - but because it is the prudent thing to do. Most recently, Lloyd's examined the impacts of a three-day disruption to a cloud service provider and found that it could impact 12.5 million business and cause USD 19 billion in losses - all from a single event. Insured losses were much less - in the range of USD 3-3.5 billion - demonstrating the huge protection gap. The difficulty in assessing aggregation risk makes it difficult for insurers to take it on. These same challenges also limit reinsurer capacity/appetite to assume these risks.

There is also confusion among clients about what coverage products actually provide. Coverage may be provided in stand-alone policies or as endorsements, or may be found in traditional policies that are covering cyber risk silently. This creates a huge amount of uncertainty for the buyers of cyber insurance and challenges in working through the myriad of potential coverages. Should I buy a stand-alone policy? What will it cover?

"Difficulties from the buyers' point of view combined with the lack of knowledge and lack of aggregation capacity explains why we've got a cyber insurance protection gap"

Addressing these challenges requires greater investment in R&D to provide insurance underwriters with the knowledge and expertise needed to understand, price and reserve for cyber risk. Underwriters also have to think more about the certainty of protection provided in their policies and how to provide coverage that companies want. There also need to be more done on the mitigation role of insurance - not just financial compensation - which will require working collaboratively, developing partnerships and leveraging the collective knowledge of all the organisations working on cyber security, including governments, regulators and national security agencies. Particular attention needs to be invested in helping small businesses that don't have access to the resources of big firms for understanding the threats that they face and for measuring their exposure.

"Because we've spent billions on modelling natural catastrophes, we've got lots of capital willing to take that risk on - they feel confident that we've done so much statistical modelling around it."

The onus is not just on insurers to take action. Governments and public bodies such as the OECD can play an important role too, especially around data - providing greater global clarity on definitions of cyber events and identifying trusted third parties to aggregate and anonymise the data necessary for underwriting. The market will only realise this opportunity if it invests for the future and all parties work together to build better cyber resilience.

SESSION 1

Cyber risk, an evolving threat



From left to right: Athanasios Drougkas (ENISA), Emma Green (Department for Digital, Culture, Media & Sport), Jamie Saunders (Independent Strategic Security Consultant), Hans Allnutt (DAC Beachcroft).

"Companies now have to protect themselves against nation-states and professional criminal organisations that are just as good at breaking into an environment and stealing data as the companies are at protecting themselves" - Marshall Heilman, Technical Operations & Reverse Engineering, IR & Red Team Operations, FireEye

technologies have established the potential for significant physical damage, demonstrated most dramatically in attacks on the power grid in the Ukraine. State-backed actors - accused recently of involvement in major 2017 ransomware attacks - are also an increasing concern. Many nation-states have varied roles when it comes to information technology: they try to protect their citizens from cyber attacks and sometimes impose regulatory requirements related to cyber security - but they also exploit the internet by stockpiling vulnerabilities and deploying advanced malware.

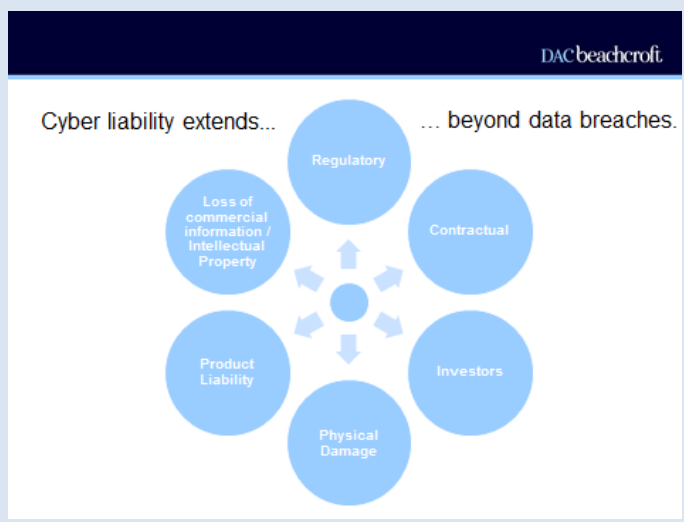
In addition to constantly changing targets, attack vectors and vulnerabilities, the obligations of companies affected by cyber incidents are also evolving. The implementation of new regulatory requirements, such as the EU's General Data Protection Regulation (GDPR), impact the ultimate cost of responding to data confidentiality breaches and ultimately the cost of ensuring that data is secure. In the EU, the GDPR will create fines and a

"The cyber threat has grown significantly, it has become more aggressive and there are concerns about accumulation and systemic risk" - Jamie Saunders, Independent Strategic Security Consultant and Visiting Professor at University College London

The economic cost of cyber crime and the share of companies that have reported being affected by a cyber incident continue to increase. The increasing use of - and dependence on - digital technologies in business operations suggests this trend is unlikely to reverse while the increasing share of value accounted for by intangible assets creates ever increasing value exposed to cyber incidents.

Greater risk awareness as well as the emergence of technical solutions to address the most common (and less-sophisticated) attacks have helped mitigate some of the risk. However, the increasing professionalisation of cyber attacks - evident in recent attacks on the financial services sector that relied on expertise and intelligence on the technologies and processes involved in financial transfers - is a significant concern. Attacks on industrial control systems and other operational

"Personal data and privacy liability is only one aspect....any data held by a company on behalf of a third party has value" - Hans Allnutt, Partner, DAC Beachcroft LLP



"Government's role is to understand how to best use the levers at its disposal to have the greatest impact on the overall level of cyber resilience" - Emma Green, Head of the Cyber Security Incentives and Regulation Team, UK Department for Digital, Culture, Media & Sport

right to compensation for those affected that didn't previously exist in many countries. Compensation practices (and amounts), even in markets with a longer history of privacy compensation, continue to expand with one recent case potentially permitting liability claims beyond an affected company's capacity to pay. In the same case, the judge explicitly referred to the possibility of companies obtaining insurance against such liability. In addition, new forms of liability (such as contractual, supply-chain, shareholders, directors and officers, physical damage and product liability) continue to emerge, particularly as connected devices become increasingly pervasive.

A lack of preparedness among companies remains a concern. In the most recent survey of cyber security breaches in the United Kingdom, close to half of all respondents reported an incident although only a third had a formal policy covering cyber security risks and only 11% had a cyber incident management plan in place. Governments have a role to play in supporting better cyber risk management and improving the baseline level of protection across companies. In the United Kingdom, government efforts have focused on the development of baseline standards ("Cyber Essentials"), particularly focused on SMEs, and creating incentives for better cyber risk management, such as requirements for adherence to the Cyber Essentials in government procurement. A planned re-opening of the December 2016 *Cyber Security Regulation and Incentives Review* will consider additional ways to mandate and/or incentivise better cyber risk management, taking into account the implementation of new EU directives.

"There is a need to focus on rationalising and harmonising the various standards and regulations that are in place" - Erin English, Senior Security Strategist, Microsoft

"Cyber insurance has the potential to make a very important contribution to corporate cyber risk management" - Athanasios Drougkas, Officer in NIS, European Union Agency for Network and Information Security (ENISA)

Some public sector organisations are also examining the role that insurance can play in incentivising better risk management. The European Union Agency for Network and Information Security (ENISA) has found a positive correlation between cyber insurance take-up and the level of preparedness. However, the low penetration of cyber insurance limits its contribution to cyber risk management, leading ENISA to work on addressing some of the challenges to broader

insurance take-up, including a 2017 report on *Commonality of risk assessment language in cyber insurance*. In the United Kingdom, the Department for Digital, Culture, Media & Sport is working with the Information Commissioners Officer on how privacy breach notifications under the GDPR can help address the gap in incident data needed for insurance underwriting.

There was general agreement that insurance offerings needed to evolve in order to provide simpler (and harmonised) coverage for smaller companies and address the challenges of insuring against nation-state attacks where such attacks cannot always be attributed with any significant level of confidence.



From left to right: Jamie Saunders (Independent Strategic Security Consultant), Hans Allnutt (DAC Beachcroft), Erin English (Microsoft), Marshall Heilman (FireEye).

SESSION 2

The increasing role of cyber insurance within the risk management process

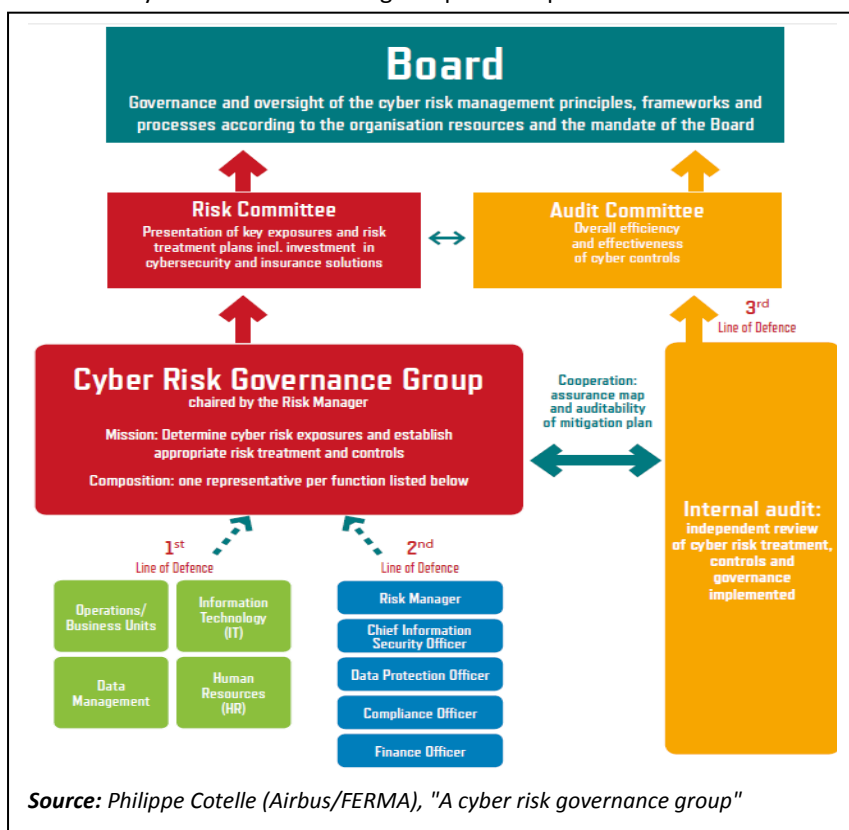
Insurance coverage contributes to mitigating the impacts of risks once they materialise, whether it be by providing funds for rebuilding a damaged building or residence, replacing lost business income resulting from an operational disruption or covering the legal defence and compensation costs related to liability claims against an organisation. But beyond its role in providing financial protection, insurance can also support better management of the risk by putting a price on risk exposure and encouraging and advising on ways to protect against risk. In the case of cyber insurance, the risk management benefits of insurance may be as - if not more - important as the financial protection it provides. The process of securing insurance requires organisations to quantify their exposure to cyber risk, thereby providing a basis for decisions on investment in protection and prevention. Cyber insurance offerings also normally include a broad range of pre- and post-breach services that can contribute to reducing the risk *ex ante*



From left to right: Nilay Ozden (Marsh), Ruth Davis (BT Security), Philippe Cotelle (Airbus.)

and more efficiently managing the impacts of cyber incidents *ex post*.

For companies, insurance should be considered as only one component of a broader risk management strategy involving an analysis of cyber risks to business operations (i.e. as an enterprise-wide risk), consideration of the optimal level of investment in mitigating that risk and identifying the residual that can potentially be transferred to insurance markets. The importance of this process has persuaded FERMA to develop specific guidance on the governance arrangements that companies should put in place to implement this process with the involvement of technical, operational, and financial expertise - providing management with the insight necessary to make strategic decisions on where to allocate scarce cyber security resources.



ultimately quantifying - cyber risks to business operations is not simple. An evolving regulatory environment creates new exposures, while the increased reliance on digital technologies (mobile environments, connected devices, big data, cloud computing) generates new vulnerabilities. To make this exercise manageable, companies need to have a firm



From left to right: Augusto Perez Arbizu (Telefonica), Raf Sanchez (Beazley), Nilay Ozden (Marsh).

understanding of the assets that are critical for keeping their business running and the realistic scenarios that can have an impact on those assets.

Managing residual risk through the purchase of insurance requires an understanding of existing coverage relative to the potential full range of cyber incidents (including operational technologies as well as data assets), potential resulting gaps and an assessment of how best to address those gaps. Traditional insurance lines such as property and general liability, depending on how they are worded, could include coverage for damages and losses without regard for the type of triggering event, meaning that some cyber incident consequences could be covered. In some cases, changes to wordings in existing policies may provide a solution to identified gaps in coverage - for other impacts/events (e.g. business interruption without physical

damage, data breach-related fines and penalties) a specific cyber coverage could be needed to address the gaps.

An understanding of the likely resources needed to respond to - and recover from - a cyber incident is also critical in making decisions on insurance purchase. This starts with a plan for how the company will respond to a cyber incident and an understanding of what components of the business must be protected should an incident occur. Upon detection of the WannaCry ransomware in its network, for example, Telefonica took immediate steps to limit the spread of the malware and ensure that the incident did not have an impact on its telecommunications networks or the services provided to customers. Insurance companies often offer crisis management support as part of the coverage they provide for cyber risks. Insurance clients are increasingly asking questions about insurers' ability to provide those services in the context of an event impacting multiple clients. The challenge for insurance companies offering these services is to ensure that

"Many traditional insurance policies already cover cyber exposure if you separate the trigger for coverage (i.e. the event) from the consequence" - Augusto Perez Arbizu, Director of Corporate Risk and Insurance, Telefonica

"Insurance is a very useful tool....but it can't be seen as a substitute for managing cyber risk - you can't transfer accountability at the end of the day" - Ruth Davis, Head of Cyber Security Strategy, BT Security

"Insurers are like the fire brigade...that does not mean an organisation should stop investing in fire extinguishers, practicing fire drills or having fire wardens" - Raf Sanchez, International Breach Response Service Manager, Beazley

they have the capacity to achieve the expected service levels - in an environment where what seemed like unrealistic doomsday scenarios continue to become reality.

However, even the most thorough assessment of coverage gaps and service level needs will not make insurance more than part of the solution. Companies need to be pro-active in keeping on top of emerging threats, building their resilience and detecting cyber incidents, through intelligence sharing, exercises and monitoring the "darkweb" for signs of customer data. Companies - no matter their size or sector - need to realise that it's not a matter of "if" they'll be impacted by a cyber incident but "when". Nation-states and sophisticated criminal organisations have significant resources

to invest and only need a single gap in security - whether technical or human - to be successful in their aims - and they are often innovating at a faster pace than those providing protection. Companies also have to realise that their accountability extends to their decisions on third party providers of information technology services, such as cloud service providers, who may have their own vulnerabilities that companies are unlikely to understand.

Insurers also need to consider how they will meet the needs of their clients in an increasingly digitalised environment. Intangible assets (reputation, trust, intellectual property) are an increasing component of company's value - for start-up's, it may be the only component - although it's not clear that financial protection for these assets can be provided through the existing structure of property and casualty insurance products. Ultimately, there is a need for greater partnership between insurance companies and businesses - with the aim of better managing risk and adapting products to meet the needs of digitalised world.

"Maybe there is an opportunity for the insurance sector to go through its own digital revolution." - Philippe Cotelle, Head of Airbus Defence and Space Insurance Risk Management and Board Member for the Federation of European Risk Management Associations (FERMA)

SESSION 3

Addressing the gaps in incident data and advances in modelling capacity

Underwriting insurance for cyber risks requires a solid understanding of both the likelihood of a cyber incident that would trigger coverage as well as the

"Data is the basis for all actuarial exercises and the basis for all our modelling" - Anna Maria D'Hulster, Secretary General, The Geneva Association

expected financial impacts of such incidents. For other perils, such as flood or earthquake, years of historical data on occurrence and impact, scientific research into understanding the underlying drivers, trusted information on physical characteristics, engineering studies on structural vulnerabilities and past insurance claims data all provide a basis for estimating the expected losses for a given insured asset. In the case of cyber, a number of factors increase the level of uncertainty in underwriting insurance coverage.



From left to right: Nick Kitching (Swiss Re), Scott Stransky (AIR Worldwide), Tom Harvey (RMS).

The CRO Forum has engaged in a multi-year effort to begin to address the lack of data for understanding digital risks and cyber exposure. In 2014, the work focused on identifying the gap and began with an effort to develop a taxonomy, published in 2016, that could integrate the terminology used by information technology, information security, risk management and underwriting experts to improve the ability to communicate about these digital risks across specialisms. In 2017, the taxonomy was tested through a pilot exercise to determine if the categorisation could be used to capture data on incidents in a way that could provide analytical value for companies while also sharing this data anonymously. The 10-month exercise captured data on more than 700 incidents determined as having 'medium' to 'high' severity impacts by the companies contributing to the exercise. The latest publication from this project, released in February 2018, highlights valuable lessons on how to improve the taxonomy and increase the value of anonymised incident reporting for risk management and underwriting.

"The CRO Forum's work aims to bring together many different perspectives/industries - including policyholders, insurers and modellers - towards a common language so that all can start to understand each other and their cyber risks" - Nick Kitching, Chief Risk Officer, Swiss Re Europe

Modelling of Cyber Insurance Coverages Offered Today

Source: Scott Stransky (AIR Worldwide)

"Hurricanes don't learn whereas cyber attackers do - but that can be an advantage as it is much easier to fix a computer vulnerability or provide cyber security training to people than it is to replace a weakness in a building" - Scott Stransky, Assistant Vice President and Principal Scientist (Research and Modeling), AIR Worldwide

boundaries; and (iii) a significant driver of risk is human nature, both among attackers and defenders, which is not always simple to observe.

"Petabytes of data are being created about cyber risk every day - but there is lots of noise - what is critical is identifying the right data to solve the given problem" - Pascal Millaire, CEO, CyberCube

Modelling firms are making significant use of technology to understand the potential vulnerabilities of companies to cyber risk, including the significant infrastructure that exists to capture data on information security and network activity (such as attempts to exploit vulnerabilities through phishing emails or efforts to gain network access). A key focus is on understanding the technologies that companies rely on in their operations (i.e. providers of cloud services, payment services, internet services, domain name system services, technology vendors, etc.) and the potential weaknesses of those service providers. They are also making use of intelligence to understand the motivations and capability of potential attackers and to gain insight on what types of companies may be targeted based on the value of the data that they hold or due to any controversial activities that might make them a target of politically-motivated attackers.

All of the modelling firms identified people, processes and practices as a critical element in understanding the level of risk for a given company, using information on cyber security staffing levels, employee training, security policies in place (and compliance with those policies) as well as the extent to which companies are effectively using the security technologies at their disposal.

"Less than a third of incidents result from actual direct hacking - most of it is people and process" - Visesh Gorani, Director of Risk and Actuarial, Cyence Risk Analytics, Guidewire Software

"What insurers are nervous about is the potential for systemic cyber catastrophes to cause large-scale losses across their business" - Tom Harvey, Senior Product Manager, RMS Cyber and Digital Risks

Ultimately, models can generate predictors of the likelihood of a given company being affected by a cyber security incident based on its nature and activities, security technology and processes and its material technology dependencies. This can help insurers build a portfolio of insureds that minimises their exposure and quantify the impact of different predictors of

vulnerability - which can also be useful for insurers when providing risk management advice to their clients.

A particular focus has been placed on aggregation risk, including the development of potential deterministic aggregation scenarios and assessments of the likelihood of an aggregation event. For example, Lloyd's and AIR Worldwide collaborated on a report to assess the impacts of a three-day cloud disruption in the United States - a realistic disruption based on past experience - which found a loss potential of USD 15 billion across 12.5 million companies - with half of the loss concentrated among large companies. This work is particularly important for understanding silent cyber coverage where policy limits are higher. The use of modelling for underwriting and pricing is only beginning to emerge and only for incident types where more data (including claims experience) is available, such as privacy breaches.

"The cyber security and insurance industry used to be competitors only two or three years ago - companies either invested in their invested security or bought insurance - that mentality has changed " - Bernard Poncin, Global Head of Financial Lines, Allianz Global Corporate & Specialty SE

There may be opportunities for the cyber security and insurance industries to collaborate more closely on understanding the drivers of cyber risk. There is also a need to make greater use of expertise from other areas within insurance companies (e.g. property, professional lines) where there is significant experience in modelling impacts such as business interruption.

Ultimately, better and more harmonised data on incidents - including on the security practices of those affected and the financial impacts - will support advances in modelling and provide insurers and other capital providers with the level of confidence needed to provide more coverage for cyber risks. The efforts of the CRO Forum - as well as the agreement on a set of Cyber Core Data Requirements among Lloyd's, AIR Worldwide and RMS - are significant steps in developing a common language.



From left to right: Visesh Gorani (Cyence), Pascal Millaire (CyberCube), Bernard Poncin (Allianz), Anna Maria D'Hulster (The Geneva Association).

SESSION 4

Enhancing the contribution of reinsurance and capital markets



From left to right: Tom Johansmeyer (PCS), Julian Enoizi (Pool Re), Philippe Gouin (Guy Carpenter), Maya Bundt (Swiss Re), Didier Parsoire (SCOR).

As in other insurance lines, reinsurance and capital markets can make an important contribution to the availability of underwriting capacity in the primary market. Some reports have suggested that there is limited reinsurance appetite for cyber risks and that the capacity that is available is being provided cautiously - while others suggest that there is significant capacity (and appetite) in the reinsurance market for cyber risk evident in the growing range of coverage structures available, including both proportional and non-proportional.

"The development of reinsurance market capacity for cyber risk could be impeded by the significant potential for accumulation risk and the problems in assessing 'silent' exposure" - Philippe Gouin, Senior Broker, Guy Carpenter

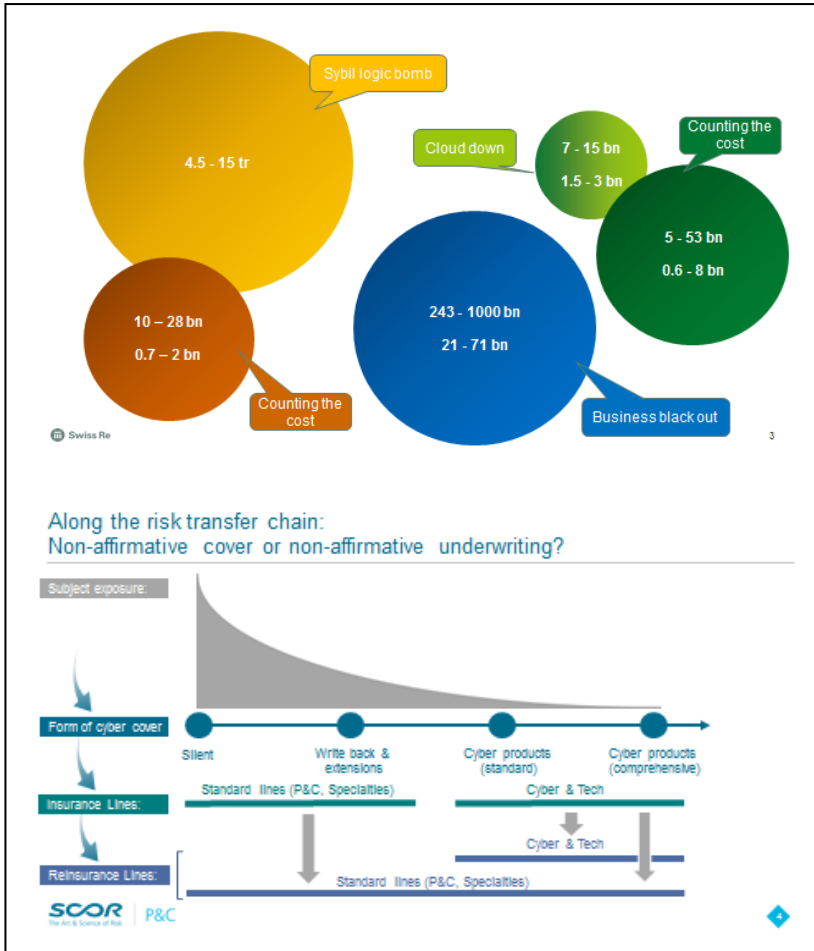
The potential for accumulation and aggregation is a key concern for reinsurance companies. While the business model of reinsurers depends on building a portfolio of risks from across

"Cyber risk is not very visible...it is pretty much everywhere... and it accumulates in ways that we are not totally aware of" - Maya Bundt, Head Cyber & Digital Strategy, Swiss Re

regions and sectors (which provides diversification benefits), the drivers of cyber accumulation and the potential scope of catastrophic losses are not well understood leading to reluctance among many reinsurers to provide significant capacity. Reinsurers are also concerned about their potential exposure to "silent" or non-affirmative cyber risk assumed through the traditional policies of primary insurers, which involve much more substantial insured values than affirmative stand-alone cyber insurance. Many traditional policies use wordings that were developed with no regard for the potential for losses triggered by intangible perils. Many primary insurers have responded by inserting exclusions for cyber as a cause of losses or for losses related to intangible assets such as data although these exclusions are applied inconsistently and not well tested - leading to uncertainties about how a policy will respond to cyber events.

"Affirmative coverage for cyber risk, including stand-alone products and extensions provided to existing property, kidnap & ransom, general liability and other policies are the tip of the iceberg" - Didier Parsoire, Chief Underwriting Officer, Cyber Solutions, Scor Global P&C

Increasing digitalisation and regulatory developments, such as the General Data Protection Regulation (GDPR) and Network and Information Security Directive (NIS) in Europe, are likely to lead to more losses that materialise through traditional policies, such as shareholder claims in directors and officers liability policies, physical damages in property policies and bodily injury resulting from physical damage in general liability policies. Where cyber is being affirmatively endorsed in traditional policies, there is some concern about whether the exposure is fully understood. Unlike practices in other lines of business, there is limited standardisation in terms of the information collected by primary insurers and provided to reinsurers when transferring their cyber exposure to reinsurers. Lack of information and inconsistencies in information provided is particularly problematic for non-proportional treaties which may be part of the reason why proportional reinsurance cover remains more widely available.



Significant efforts have been invested by insurers, reinsurers and modelling companies in better understanding cyber accumulation risks in both stand-alone and traditional policies. A number of recent studies have examined the potential insured and economic losses from various types of aggregation events, including software flaws, cloud disruptions and a power supply disruption - usually involving an assessment of potential insured losses in both stand-alone cyber insurance and traditional lines of business. In some cases, these studies have found economic losses in magnitudes similar to annual losses during a severe natural catastrophe year - although with much lower levels of insured losses. As noted in the previous session, modelling is advancing towards probabilistic assessments, particularly for incidents like privacy breaches where there is a more comprehensive set of loss and claims data.

Reinsurers are also managing this risk by being selective about risks that they assume and placing limits on businesses with too much inherent uncertainty.

Some are also placing hard exclusions on losses that could become truly systemic from an aggregation perspective, such as outages of external networks (e.g. cloud service and other technology service providers) - although the effectiveness of this approach can be hindered for large tower policies involving a syndicate of (re)insurers using

"Potential systemic risks - such as outage of external networks - require insurers and reinsurers to take a common stand to exclude" - Daljitt Barn, Head of Cyber Innovation, Munich Re

different wordings and exclusions. Reinsurers are also making use of expertise from other lines of business, such as property, to better understand their potential exposure through traditional policies.

"The cyber insurance line has performed well, there is lots of capacity and soft pricing - this is unlikely to change unless there is a major loss event or action by regulators or rating agencies" - Catherine Rudow, Senior Vice President (North America P&C) and Senior Underwriter (Casualty), Partner Re

Losses Tell the Growth Story

- The market is growing in a specific way
 - Vertical growth appears to be slowing
 - Horizontal growth is increasing rapidly
- Result:
 - More programs at US\$100-500 mn
 - Some upward movement in limit for underinsureds
 - Increased cyber adoption by uninsureds
 - But, we'll have to wait for US\$1 bn to become widely available
- Meanwhile, economic losses would still exceed the largest coverage limits in place
 - 8 of 9 PCS Global Cyber loss events exceeded coverage limits
 - Southwest Airlines is the one exception
 - Equifax and Merck likely 2X the US\$600 mn thought to be the market's largest cyber program

How 2017 Could Have Looked

Insured	Insured Loss	Economic Loss
Equifax	US\$125 mn	> US\$1 bn
Merck	US\$275 mn	> US\$1.5 bn
FedEx	US\$0	> US\$300 mn
Maersk	US\$0	US\$300 mn
Nuance Comms	US\$30 mn	UNK
Others	US\$0	US\$600 mn

- With full penetration: industry loss > US\$3.5 bn
- With towers at \$3-500 mn: industry loss > US\$2 bn
- At current levels: industry loss = US\$430 mn

With data from PCS Global Cyber, Capicum Re and PCS Internal research

Source: Tom Johansmeyer (PCS)

There have also been some real-life examples of accumulation events, including the 2015 and 2016 power outages in the Ukraine, the attack on Dyn and the WannaCry and NotPetya ransomware attacks, providing some experience with such events although few insured losses. In fact, a

2017 Partner Re survey of cyber underwriters found that, for most, the Dyn and WannaCry incidents had no significant impact on pricing or capacity in the market. A soft reinsurance market, combined with good loss ratios in the cyber line

of business to date, has meant that plenty of reinsurance capacity is available for now, particularly in the US and on a proportional basis - which has also meant limited scope for reinsurers to diverge from market practices.

"Removing the cyber-terrorism risk from the market - a risk which they had little appetite in covering - should allow for more capacity to take-on remaining parts of cyber risk" - Julian Enoizi, Chief Executive Officer, Pool Re

The difficulty in attributing cyber attacks to a given actor creates a "silent" exposure to war and terrorism losses that are normally excluded from property and liability policies. A number of national terrorism insurance pools are beginning to address this exposure

by adding some coverage for cyber terrorism. In the United Kingdom, Pool Re undertook extensive research on the potential for cyber terrorist attacks and market consultations on the market's appetite and capacity for covering cyber terrorism incidents, culminating in the extension of its reinsurance coverage for property damage that results from cyber terrorism. The coverage provided by Pool Re has been designed to maximise market involvement, by requiring risk retention by primary insurers and retroceding Pool Re exposure back to the market (which involved some challenges as not all retrocedants were willing to take on cyber terrorism exposure). The coverage is also designed to encourage risk reduction by providing premium discounts for companies that implement cyber security standards. The approach creates an *ex ante* solution to a potential future exposure with the hope of avoiding future panic and market disruption should a significant cyber terrorism incident materialise.

Capital markets have made an important contribution to increasing reinsurance market capacity in other lines of business, notably property catastrophe. Thus far, there has been limited demand for - and limited supply of - capital market capacity for cyber insurance risk - although market growth is expected to lead to more demand for retrocession coverage. Capital market instruments such as Industry Loss Warranties could provide a risk transfer approach that minimises the need for sharing confidential information among reinsurance competitors as well as the need for the development of a common language on cyber incidents and loss types. There is some cautious interest among Insurance-Linked Security fund managers in expanding into covering cyber risk.

"Growing insured exposure will create demand for retrocession capacity...ILWs may provide an answer that doesn't require sharing of proprietary information or common language on cyber incidents and losses" - Tom Johansmeyer, Co-Head, PCS



From left to right: Philippe Gouin (Guy Carpenter), Daljitt Barn (Munich Re), Catherine Rudow (Partner Re), Tom Johansmeyer (PCS), Julian Enoizi (Pool Re).

There were divergent views on whether a government backstop is needed to cover cyber catastrophe exposure with some suggesting that a catastrophic backstop could be helpful in placing a limit on private market exposure and therefore allowing insurers to confidently

expand their appetite for cyber risk. It was noted that governments already have a role in managing catastrophic incidents for other perils (e.g. natural disasters) and an impact through their foreign policies on whether companies are targeted by nation-state actors. However, it was also recognised that the low level of current losses would make it difficult to make a convincing *ex ante* case for government involvement.

SESSION 5

Providing greater clarity on coverage - "policyholder" perspective

The variation and complexity of cyber insurance policies is often cited as an impediment to the greater take-up of cyber insurance. When seeking insurance coverage for cyber risks, companies usually face wide disparities in the types of coverage being offered, including whether the coverage is offered as an

"The lack of comparability across policies is also a sign of the richness of the insurance market's offers...it's both good for buyers as well as a challenge" - Nic De Maesschalck, Director, European Federation of Insurance Intermediaries (BIPAR)

endorsement to a traditional property or liability coverage or a stand-alone policy as well as the types of risk mitigation and crisis management services that are included. This makes it extremely difficult for companies to compare the

different offers and advise senior management on the insurance coverage to acquire. While also an indicator of innovation in the market, this variation creates specific challenges for SMEs who often have a limited understanding of their risk in the first place, let alone the coverage that they might need.

The limits and exclusions imposed by insurers may also limit the perceived value of cyber insurance for potential buyers leading some to suggest that the scope of coverage is driven more by what insurance companies are willing to offer than what companies are seeking to acquire. Some types of potentially significant losses common to cyber incidents (such as intellectual property theft, reputational losses, external service provider disruptions) are not normally covered. The practice of offering coverage on a claims-made basis increases the complexity and may also limit the benefits of coverage from the policyholder perspective. Some of these risks, such as intellectual property theft are not new and challenging to insure under any line of business. Some companies might also question whether they will actually be willing to make claims in

"The vast majority of stand-alone cyber insurance policies are triggered on a claims-made basis which places time limits for reporting claims to the insurer - which is good from a solvency perspective but a potential limitation for policyholders" - Ekrem Sarper, Lead Manager (Bilateral Affairs), National Association of Insurance Commissioners



From left to right: Graeme Newman (CFC Underwriting), Mamiko Yokoi-Arai (OECD), Joel Wood (CIAB), Nic De Maesschalck (BIPAR), Philippe Cotelle (Airbus).

"As insurers and reinsurers tread carefully - with modest limits and tight restrictions - clients wonder what the value of cyber insurance is for them" - Joel Wood, Senior Vice President, Government Affairs, US Council of Insurance Agents and Brokers

cases where they are not required to disclose the incident and could face (uncovered) reputational impacts if the incident becomes public knowledge as a result of notifying the intermediaries, insurers and reinsurers (or panels of insurers and reinsurers) and the third party technical experts that are usually involved in settling claims. However, it was acknowledged that this challenge may be dissipating as a result of the greater acceptance that companies will be affected by cyber incidents and the increasing recognition of the benefits of pro-active communications that demonstrate resilience in the event of an incident.

For buyers of cyber insurance, the process of applying for cyber insurance coverage usually involves the sharing of highly-sensitive information on security practices, vulnerabilities and processes for managing those vulnerabilities. Of

particular concern is the need to share information on risks that the company is unable to effectively mitigate - usually the risks for which they are seeking insurance coverage - which is information not usually disclosed to more than a handful of the company's own employees. Insurers need to demonstrate that they can manage sensitive information and also consider what information is truly needed. There are also concerns that some cyber insurers may be setting security standards that are impossible to achieve, particularly for SMEs.

"Companies need some guarantees from insurers about their ability to manage confidential, highly-sensitive information" - Philippe Cotelle, Head of Airbus Defence and Space Insurance Risk Management and Board Member, Federation of European Risk Management Associations (FERMA)

While it is still a relatively new market with limited levels of business, regulators are beginning to examine cyber insurance underwriting practices. In the United States, the National Association of Insurance Commissioners (NAIC) has focused on collecting the necessary data on premiums and claims to allow for a better understanding of the market and its evolution. The NAIC designed a data supplement in 2015 and has collected data for 2015 and 2016 which provides some capacity to examine underwriting quality (although limited by the small portfolios of many insurers). Among the findings of the data collection exercise is that a number of insurers have had difficulty assigning premiums to cyber risk in package policies leading to a recommendation that this be rectified in future submissions.

In the United Kingdom, the Bank of England's Prudential Regulation Authority (PRA) undertook market consultations with insurance buyers, (re)insurance providers, modellers and other regulators in 2015 as part of a thematic review of cyber insurance underwriting, leading to a formal consultation in February 2017. The consultations found that the market was having difficulty in comprehensively assessing its exposure to non-affirmative cyber risk, making it difficult

"Market reception of the supervisory statement was good...and we hope it can act as a catalyst for providing greater clarity in the market" - Alex Ntelekos, Senior Manager, Insurance Supervision, Prudential Regulation Authority, Bank of England

for insurance company boards to take ownership of a company's overall strategy for underwriting cyber risk - partly a reflection of a lack of expertise in the insurance sector for understanding cyber risk. In July 2017, the PRA released a supervisory statement setting out its expectations for the management of non-affirmative cyber coverage, including that insurers be explicit about the coverage for cyber risks that they offer.

There was general agreement that insurers need to provide greater clarity on the coverage that they are providing for cyber risk - not to the extent of developing a commoditised product but working towards common definitions of terms. Brokers and agents have an important role to play in building understanding of the insurance products available, particularly among SMEs who could benefit from a more tangible presentation of the risks and potential coverage options. While there are some persuasive arguments in support of expanding stand-alone over endorsed coverage (easier to understand exposure, manage limits and encourage risk mitigation), the most critical need is in providing greater clarity. Some buyers, especially SMEs, are also likely to prefer endorsed coverage in all-risk policies over

acquiring multiple policies. While regulation can be helpful in encouraging greater clarity, significant losses in traditional policies not intended to cover cyber risks (e.g. ransomware losses in kidnap and ransom coverage) are likely to drive the market towards providing more clarity.

There is also a need to better manage buyer expectations about the coverage that cyber insurance is meant to provide, particularly as technology becomes increasingly pervasive in company's operations. Cyber insurance has not been designed to address every potential risk and loss related to the use of technology. Part of the challenge will be in appropriately integrating cyber risk coverage into other lines of business in recognition of the potential for cyber risks to create losses.



From left to right: Ekrem Sarper (NAIC), Alex Ntelekos (Bank of England), Graeme Newman (CFC Underwriting) Mamiko Yokoi-Arai (OECD).

Greater consistency across legislative and regulatory frameworks applicable to data breach notifications and rights to compensation, cyber risk management and disclosure requirements as well as supervisory expectations for cyber insurance underwriting could also contribute to improving harmonisation across the insurance products being offered. In establishing supervisory expectations for cyber insurance underwriting, supervisors should focus on ensuring proper management of cyber risk assumed through the coverage provided and carefully consider the potential impact on policyholders and the availability of coverage. The PRA, for example, is calibrating its expectations to try and ensure that insurance companies don't respond by simply establishing more limits or exclusions in the cyber insurance coverage that they provide.

"If you are a property insurer, or an aviation insurer or a product liability underwriter, you have to realise you face the risk of a cyber attack" - Graeme Newman, Chief Innovation Officer, CFC Underwriting

SESSION 6

Providing greater clarity on coverage - insurer perspective

For insurance companies, increasing digitalisation and the recognition of data as an asset of value for business (rather than a by-product of doing business) has led to a need to develop new products and coverage to meet their client needs. The market has responded by developing a broad set of new coverage for intangible assets and incidents that were barely understood even 20 years ago.

"It is important to recognise what has been achieved by the industry in creating a market that provides coverage globally for intangible incidents and assets - in a relatively short period of time" - Scott Sayce, Global Chief Underwriting Officer (Cyber), AXA Global P&C

However, as with any emerging product, there are misunderstandings about the purpose of cyber insurance and gaps between the coverage desired by companies and what insurance companies are willing to provide. The sector recognises that greater clarity is required in defining the coverage available for cyber risks and where to find it (particularly for SMEs) - and that there will be a continuing need to innovate to meet client needs.

The first element of providing greater clarity relates to clarity about whether cyber risks are covered or not in a given policy. There are differing views on the best approach to providing coverage for cyber risk. For insurance companies, the inclusion of cyber risk in various lines of business makes it more difficult to manage, particularly when the processes for properly assessing and monitoring cyber risk are not in place within underwriting teams for traditional lines. However, the pervasiveness of technology across business operations and the increasing potential for cyber risks to create losses normally covered in traditional lines (e.g. property damage or bodily injury) will likely lead to an increasing recognition of cyber as peril rather than a product. Market practices will also have an impact. For example, in the US market, major carriers have affirmatively placed coverage for business interruption without material damage in property policies which has led other carriers to do the same either when participating with those carriers in providing coverage as part of a panel of insurers, due to the dominance of those large carriers' wording in property policy forms - or simply in response to client and broker expectations. The same applies to liability lines, particularly in Europe, where underwriters are affirmatively including coverage for cyber risks.

"Standardisation efforts may help SMEs – although in order to avoid stifling innovation, which could ultimately harm rather than help SMEs - it should occur organically within industry and be consistent with ongoing market developments" - Stephen Simchak, Vice President and Chief International Counsel, American Insurance Association and Chair, GFIA Cyber Risks Working Group



From left to right: Stephen Simchak (AIA), Jean Bayon de la Tour (Marsh), Leigh Wolfrom (OECD), Tracie Grella (AIG).

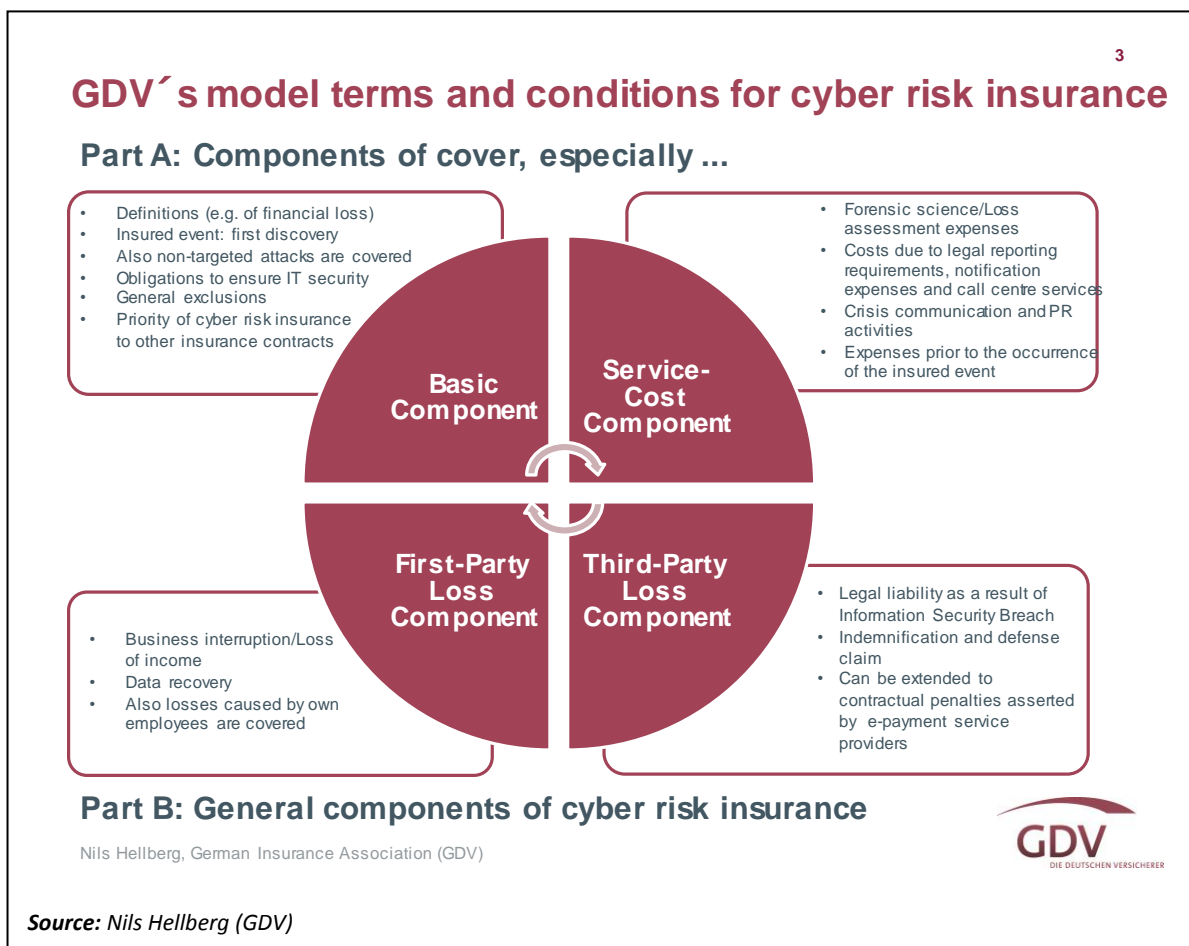
"While it would be easier for insurers to manage cyber exposure if it was all in a single policy, the market needs to prepare for cyber as a peril, especially in the era of the Internet of Things" - Tracie Grella, Global Head of Cyber Risk Insurance, AIG

The other aspect of providing greater clarity on coverage relates to the use of common terminologies, which will naturally differ in a developing insurance line. Full standardisation - particularly if mandated by government - might have unintended consequences in terms of reducing market appetite to provide coverage as well as consumer choice - different companies, operating in different sectors with different capacities to invest in risk mitigation will have different coverage needs. The market is moving towards

increasing standardisation, particularly for some types of costs such as forensic investigation costs, notification costs, regulatory fines and penalties and legal and regulatory defence costs. Industry organisations are also working on common terminologies and definitions for voluntary use. This effort will be most effective if it takes into account the lexicon used by risk managers and information security professionals in their work.

In Germany, the insurance association has developed both a model set of terms and conditions and a non-binding risk assessment tool to support insurers in extending coverage to SMEs (currently, a relatively limited market in Germany despite the significant risks that SMEs face). The models were developed in close consultation with potential buyers, intermediaries, insurance companies and reinsurers with the aim of developing a policy that responds to the needs of clients while also being acceptable to both underwriters and the reinsurance market. The model policy is meant for use in providing stand-alone coverage for first and third party losses and service costs (forensics, public relations, notification, etc.) as a result of an impairment of the availability integrity or confidentiality of electronic data, whether targeted or not and perpetrated by either an external or internal actor (subject to standard terrorism and war exclusions). The coverage is meant to supersede non-affirmative coverage potentially provided in traditional policies. It also includes a set of definitions of key terms and establishes obligations for policyholders related to cyber security risk management.

"Model wordings were developed in consultation with customers, brokers and insurers taking into account the desired coverage as expressed by policyholders" - Nils Hellberg, Head of Department, German Insurance Association (GDV)



Insurers are working to extend coverage to include other types of losses not normally covered in existing policies. Some are providing coverage for reputation losses and examining the possibility of responding to losses related to situations where companies voluntarily take-down information technology systems in order to prevent an incident. Some types of coverage will remain challenging to offer, however, including coverage for the value of lost or stolen trade secrets (which are difficult to value no matter the cause of loss) as well as coverage for disruptions to outsourced service providers and contingent business interruption which entail significant aggregation risks given common dependencies on major suppliers. Coverage related to connected devices is also likely to emerge - although this will be challenging

without greater attention from producers of connected devices on security (which may require the imposition of standards by government). Extending coverage in these areas will require better data and modelling to support underwriting and also the development of a common approach with reinsurers to ensure risk can be shared across insurance and reinsurance markets.

Providing coverage that meets the needs of SMEs presents a particular challenge. The capacity of SMEs to invest in cyber risk management - and to keep up with developments in attack tactics and the identification of new vulnerabilities - is much more limited than larger companies. Their more limited ability to mitigate against cyber risks can also lead to higher premiums for a given level of coverage. The increasing offer of services with cyber insurance policies, particularly advice and services for protecting against cyber risks, might be one means of overcoming these challenges. The development of cyber security guidance and standards tailored for SMEs, as well as the continued development of certification and ratings processes common in other areas, could also play a role in helping SMEs become more resilient and in providing insurers increased confidence in the level of resilience achieved.

Continued collaboration will be critical in overcoming the challenges to the market's development, including collaboration among insurers as well between insurers and clients, intermediaries, reinsurers, the cyber security industry and governments. The global nature of cyber risks also creates potential benefits for collaboration across countries. However, there are limits to collaboration, particularly in areas such as incident data sharing given the challenges of anonymising data on high-profile incidents and the obligations that insurers have to companies to only use their claims data for their own underwriting purposes.

"The insurance market is increasingly moving to a service provider model - providing companies with help in mitigating their risks, not just paying claims" - Jean Bayon de la Tour, Cyber Development Leader (Continental Europe), Marsh



From left to right: Jean Bayon de la Tour (Marsh), Leigh Wolfrom (OECD), Tracie Grella (AIG), Scott Sayce (AXA), Nils Hellberg (GDV).

PROGRAMME

22 February 2018 (Room CC9)

08:45-09:15 **Opening Session**

Speakers

Masamichi Kono, Deputy Secretary-General, OECD
John Doyle, President and CEO, Marsh

09:15-10:45 **Session 1: Cyber risk, an evolving threat**

Topics

The nature of cyber risk and the players involved are continuously evolving. The security environment is constantly changing as new attack vectors and defence mechanisms are developed - while the number of connected targets increases exponentially. The legal and regulatory environment in which companies operate and the accountabilities they have to their clients, suppliers and shareholders are only beginning to be defined with limited harmonisation across national borders. Meanwhile, the role of different actors in cyber-attacks and their motivations change regularly in an environment where the boundaries between non-state and state actions is increasingly blurred. This session will examine the implications of constant change on the development and expansion of the cyber insurance market as well as the potential role of public-private partnerships in addressing these challenges.

Moderator

Jamie Saunders, Independent Strategic Security Consultant and Visiting Professor at University College London

Panellists

Marshall Heilman, Technical Operations & Reverse Engineering, IR & Red Team Operations, FireEye
Erin English, Senior Security Strategist, Microsoft
Hans Allnutt, Partner, DAC Beechcroft LLP
Emma Green, Head of the Cyber Security Incentives and Regulation Team, UK Department for Digital, Culture, Media & Sport
Athanasios Drougkas, Officer in NIS, European Union Agency for Network and Information Security (ENISA)

10:45-11:15

Coffee break

11:15-12:30 **Session 2: The increasing role of cyber insurance within the risk management process**

Topics The purchase of cyber insurance is an important component of corporate risk management, not only in terms of providing financial protection, but also in providing expertise in risk assessment, risk reduction and crisis management. Estimating the potential financial impact of a cyber loss scenario can support the overall design of the cyber risk strategy and priorities. For many buyers of cyber insurance, particularly SMEs, the risk management services are as - if not more - important than risk transfer as a driver of purchase decisions. This session will examine the contribution of insurance to corporate risk management.

Moderator **Nilay Ozden**, Head of FINPRO and Credit Specialties (Continental Europe), Marsh

Panellists **Augusto Perez Arbizu**, Director of Corporate Risk and Insurance, Telefonica

Ruth Davis, Head of Cyber Security Strategy, BT Security

Philippe Cotelle, Head of Airbus Defence and Space Insurance Risk Management and Board Member, Federation of European Risk Management Associations (FERMA)

Raf Sanchez, International Breach Response Service Manager, Beazley

12:30-13:00 **Keynote speech - Inga Beale, CEO, Lloyd's of London**

13:00-14:30 *Lunch break (hosted by Beazley) - George Marshall Room, Chateau de la Muette, OECD*

14:30-16:15 **Session 3: Addressing the gaps in incident data and advances in modelling capacity**

Topics Historical data plays a critical role in understanding risk exposure and underwriting insurance coverage, even for perils like cyber risk where the frequency and severity is constantly evolving. Limited reporting of cyber incidents (except where disclosure is mandatory) has meant that information on past incidents is limited, complicating the ability of buyers and sellers of insurance coverage to quantify potential exposure to cyber risk. Risk modelling is increasingly used for the quantification of risk across a range of insurance lines and a number of risk modelling companies have been developing models to support the underwriting of cyber insurance coverage, despite the lack of historical incident data as well as the ever-changing nature of cyber risk and motivations for cyber-attacks. This session will explore efforts to improve the availability of data and modelling capacity for underwriting cyber risk.

Moderator **Anna Maria D'Hulster**, Secretary General, The Geneva Association

Panellists **Nick Kitching**, Chief Risk Officer, Swiss Re Europe S.A.

Scott Stransky, Assistant Vice President and Principal Scientist (Research and Modeling), AIR Worldwide

Tom Harvey, Senior Product Manager, RMS Cyber and Digital Risks

Vishesh Gosrani, Director of Risk and Actuarial, Cyence Risk Analytics, Guidewire Software

Pascal Millaire, CEO, CyberCube

Bernard Poncin, Global Head of Financial Lines, Allianz Global Corporate & Specialty SE

16:15-16:30 *Coffee break*

16:30-18:15

Session 4: Enhancing the contribution of reinsurance and capital markets

Topics

As in other insurance lines, reinsurance and capital markets can make an important contribution to the availability of underwriting capacity in the primary market. In the case of cyber risk, the development of reinsurance and capital markets capacity has been impeded by the significant potential for accumulation risk as well as uncertainty about the level of exposure present in the coverage that is being provided by primary insurers. This session will explore the impediments to greater reinsurance and capital market involvement in covering cyber risk and potential ways to overcome those challenges. It will also examine the role of government in providing coverage for terrorist cyber-attacks and explore whether there is need for government involvement in state-sponsored cyber-attacks.

Moderator

Philippe Gouin, Senior Broker, Guy Carpenter

Panellists

Maya Bundt, Head Cyber & Digital Strategy, Swiss Re

Didier Parsoire, Chief Underwriting Officer, Cyber Solutions, Scor Global P&C

Catherine Rudow, Senior Vice President (North America P&C) and Senior Underwriter (Casualty), Partner Re

Daljitt Barn, Head of Cyber Innovation, Munich Re

Tom Johansmeyer, Co-Head, PCS

Julian Enozi, Chief Executive Officer, Pool Re (United Kingdom)

18:30-20:00

Cocktail reception – George Marshall Room, Chateau de la Muette, OECD

23 February 2018 (Room CC9)

08:45-10:30

Session 5: Providing greater clarity on coverage - "policyholder" perspective

Topics

The complexity of current coverage offerings for cyber risk is often cited as an impediment to the market's further development as potential buyers voice concerns about whether the insurance coverage will actually cover their needs in the event of a cyber incident. Cyber insurance products usually provide coverage for losses that might have otherwise been covered by a range of first party property and third party liability policies. The practice of some companies to include cyber risk under traditional policies while others exclude these risks and offer stand-alone coverage exacerbates the level of confusion. This is further complicated by the differences in how different policies treat state-sponsored and terrorism-related attacks. This session will provide a range of perspectives on these issues from the point of view of policyholders, intermediaries and regulators.

Moderator

Mamiko Yokoi-Arai, Principal Administrator, Directorate for Financial and Enterprise Affairs, OECD

Panellists

Philippe Cotellet, Head of Airbus Defence and Space Insurance Risk Management and Board Member, Federation of European Risk Management Associations (FERMA)

Nic De Maesschalck, Director, European Federation of Insurance Intermediaries (BIPAR)

Joel Wood, Senior Vice President, Government Affairs, US Council of Insurance Agents and Brokers

Ekrem Sarper, Lead Manager (Bilateral Affairs), National Association of Insurance

Commissioners

Alex Ntelekos, Senior Manager, Insurance Supervision, Prudential Regulation Authority, Bank of England

Graeme Newman, Chief Innovation Officer, CFC Underwriting

10:30-11:00

Coffee break

11:00-12:45

Session 6: Providing greater clarity on coverage - insurer perspective

Topics

The complexity of current coverage offerings for cyber risk is often cited as an impediment to the market's further development as potential buyers voice concerns about whether the insurance coverage will actually cover their needs in the event of a cyber incident. Cyber insurance products usually provide coverage for losses that might have otherwise been covered by a range of first party property and third party liability policies. The practice of some companies to include cyber risk under traditional policies while others exclude these risks and offer stand-alone coverage exacerbates the level of confusion. This is further complicated by the differences in how different policies treat state-sponsored and terrorism-related attacks. This session will provide a range of perspectives on these issues from the point of view of insurance companies.

Moderator

Leigh Wolfrom, Policy Analyst, Directorate for Financial and Enterprise Affairs, OECD

Panellists

Tracie Grella, Global Head of Cyber Risk Insurance, AIG

Scott Sayce, Global Chief Underwriting Officer (Cyber), AXA Global P&C

Nils Hellberg, Head of Department, German Insurance Association (GDV)

Stephen Simchak, Vice President and Chief International Counsel, American Insurance Association and Chair, GFIA Cyber Risks Working Group

Jean Bayon de la Tour, Cyber Development Leader (Continental Europe), Marsh

12:45-13:15

Supporting the development of an effective cyber insurance market - the way forward

Chair

Pierre Poret, Deputy Director, Directorate for Financial and Enterprise Affairs, OECD

FURTHER READING

AIR Worldwide (2016), [Cyber Exposure Data Standard and Preparer's Guide](#), AIR Worldwide.

Allnut, H. and R. Webster (2017), [Personal Data: the new oil and its toxic legacy under the General Data Protection Regulation](#), DAC Beachcroft.

Beazley (2018), [2018 Breach Briefing](#), Beazley.

Cambridge Centre for Risk Studies (2016), [Cyber Insurance Exposure Data Schema V1.0](#), Cambridge Centre for Risk Studies.

Council of Insurance Agents & Brokers (2017), [Cyber Insurance Market Watch Survey: Executive Summary](#), Council of Insurance Agents & Brokers.

Le Club des juristes (2018), [Report: Insuring Cyber Risk](#), Cyber Risk Commission Report, Paris.

CRO Forum (2018), [Supporting on-going capture and sharing of digital event data](#), CRO Forum.

Department for Culture, Media and Sport (2018), [Cyber Security Regulation and Incentives Review](#), Department for Culture, Media and Sport, London.

Department for Digital, Culture, Media and Sport (2018), [Cyber Security Breaches Survey 2018](#), Department for Digital, Culture, Media and Sport, London.

Department of Homeland Security (2015), [Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository](#), Department of Homeland Security, Washington.

Drzik, J. (2018), "[Cyber risk is a growing challenge. So how can we prepare?](#)" *World Economic Forum Global Risks Report*.

ENISA (2016), [Cyber Insurance: Recent Advances, Good Practices and Challenges](#), European Network and Information Security Agency, Heraklion (Greece).

ENISA (2017), [Commonality of risk assessment language in cyber insurance](#), European Network and Information Security Agency, Heraklion (Greece).

FERMA and ECIIA (2017), [At the junction of corporate risk governance and cybersecurity](#), Federation of European Risk Management Associations and European Confederation of Institutes of Internal Auditing.

FireEye and Marsh & McLennan Companies (2018), [Cyber: The stakes have changed for the C-Suite](#); FireEye and Marsh & McLennan Companies.

GFIA (2018), [GFIA Observations on Cybersecurity](#), Global Federation of Insurance Associations.

IRT SystemX (2016), [Mastery of Cyber Risk Throughout the Chain of its Value and Transfer to Insurance: Results of the Research Seminar \(November 2015-July 2016\)](#), IRT System X, Palaiseau (France).

Lloyd's (2015), [Business Blackout: The insurance implications of a cyber attack on the US power grid](#), Lloyd's, London.

Lloyd's (2016), [Cyber Core Data Requirements](#), Lloyd's, London.

Lloyd's (2018), [Cloud Down: Impacts on the US economy](#), Lloyd's and AIR Worldwide, London.

Lloyd's and Cyence (2017), [Counting the cost: Cyber exposure decoded](#), Lloyd's, London.

Marsh and Microsoft (2018), [By the numbers: Global cyber risk perception survey](#), Marsh and Microsoft.

National Association of Insurance Commissioners (2017), [2017 Report on the Cybersecurity Insurance Coverage Supplement](#), NAIC, Kansas City.

OECD (2015), [Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document](#), OECD, Paris.

OECD (2017), [Enhancing the role of insurance in cyber risk management](#), OECD, Paris.

PartnerRe (2017), [2017 Survey of Cyber Insurance Market Trends](#), PartnerRe.

Prudential Regulation Authority (2017), [Cyber insurance underwriting risk: Supervisory Statement 4/17](#), Bank of England, London.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), [Managing Cyber Insurance Accumulation Risk](#), Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

Ruffle, S.J. et al. (2014), [Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe](#), Centre for Risk Studies, University of Cambridge.

The Geneva Association (2016), [Ten Key Questions on Cyber Risk and Cyber Risk Insurance](#), The Geneva Association, Zurich.



[www.oecd.org/finance/insurance/
2018-oecd-conference-cyber-insurance-market.htm](http://www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm)



in collaboration with

