Unleashing the Potential of the Cyber Insurance Market

PROGRAMME

22-23 February 2018
Paris, France

OECD

in collaboration with

MARSH & McLENNAN COMPANIES

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.

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, Trustworthy Computing, Microsoft **Hans Allnut,** 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 **Visesh 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,** Assistant Vice-President, Property Claims Service **Julian Enoizi,** 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, brokers and regulators.
Moderator	**Mamiko Yokoi-Arai,** Principal Administrator, Directorate for Financial and Enterprise Affairs, OECD
Panellists	**Philippe Cotelle,** 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
	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
Pannelists	**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

SESSION NOTES

Session 1: Cyber risk, an evolving threat

Cyber risk is an increasing concern for the business community. The 2018 Global Risks Report identified cyber attacks as a top-5 risk to doing business in 23 of the 35 OECD member countries and as the most significant risk in 11 member countries.[1] The annual economic cost of cyber crimes is now estimated to be over USD 1 trillion[2] while the share of companies that have reported being affected by a cyber incident continues to increase. The increasing use of - and dependence on - digital technologies in business operations suggests this trend is unlikely to reverse in the near future.

The uncertainty that results from an ever changing risk environment is as disconcerting as the increasing frequency of cyber incidents. Targets, attack vectors and vulnerabilities are constantly changing. In 2017, a major data breach occurred as a result of unauthorised access through a cloud service provider while some of the most notable cyber-related losses occurred in sectors such as manufacturing and transportation[3] - not in the personal-data rich health and education that have been substantially affected in the past. State-backed actors were accused of diversifying beyond intellectual property theft into ransomware attacks. Attacks on industrial control systems with the potential to cause significant physical damage continued while, in early 2018, the boundaries of exploitable vulnerabilities expanded into central processing units with the identification of the Meltdown and Spectre hardware 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, impact the ultimate cost of responding to data confidentiality breaches. In addition, compensation practices in the context of litigation (i.e. amounts due to injured parties) continue to evolve as the obligations of companies to their employees, customers and shareholders become increasingly stringent - a trend that is unlikely to change in the context of the recent breach of some of the most sensitive customer data at a large US credit reporting organisation.

Key questions for discussion

- What are the most important things that companies can do to protect themselves in an evolving cyber risk environment?
- Are there opportunities for greater information sharing between the public and private sectors on cyber threats?
- How can the legal and regulatory environment evolve to support companies' ability to manage cyber risk?

[1] Turkey, an OECD member country, was not included in the 2018 Global Risks Report risk survey.

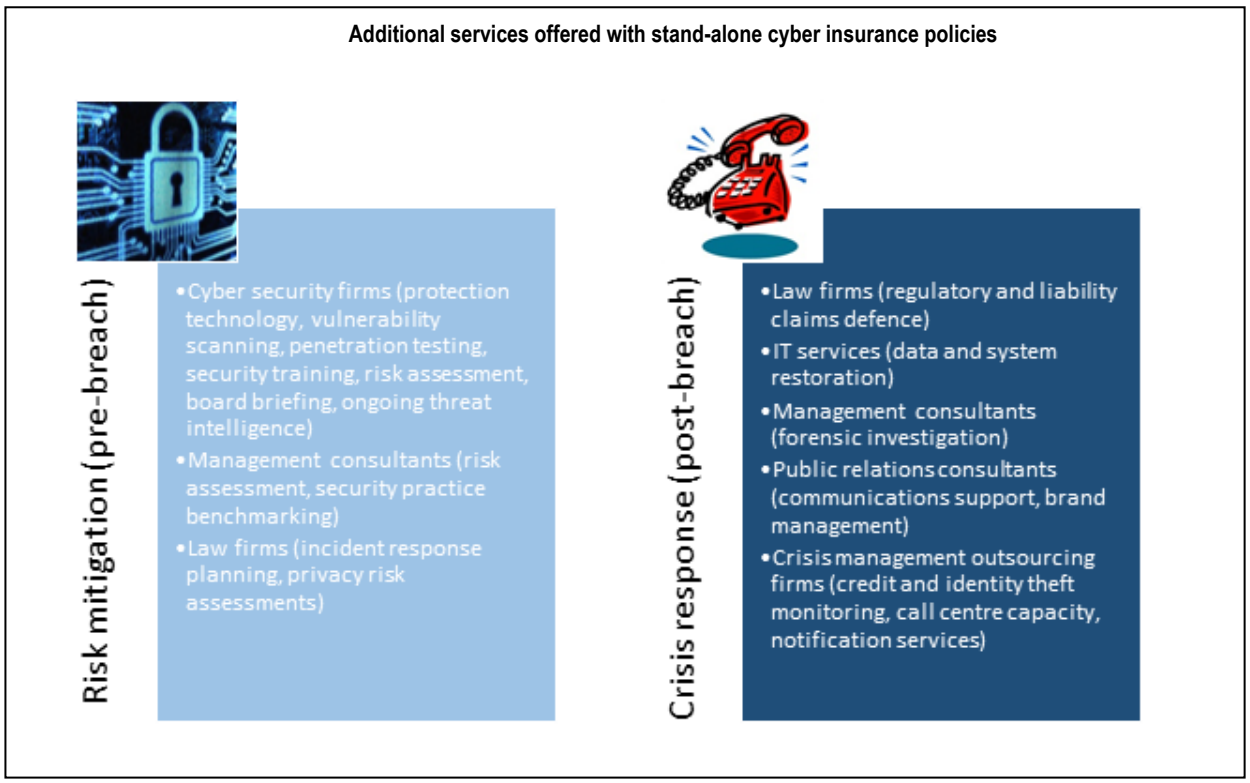
[2] Drzik, J. (2018), "Cyber risk is a growing challenge. So how can we prepare?" W*orld Economic Forum Global Risks Report*, www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready.

[3] The NotPetya ransomware attacks led to an estimated USD 1 billion in losses, including USD 250 million at the European operations of a US shipping company and EUR 250 million suffered by a French construction materials company (FireEye and Marsh & McLennan Companies (2018), *Cyber: The stakes have changed for the C-Suite*; Advisen (2018), Notable European Cyber Losses from 2011-2017).

Session 2: The increasing role of cyber insurance within the risk management process

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

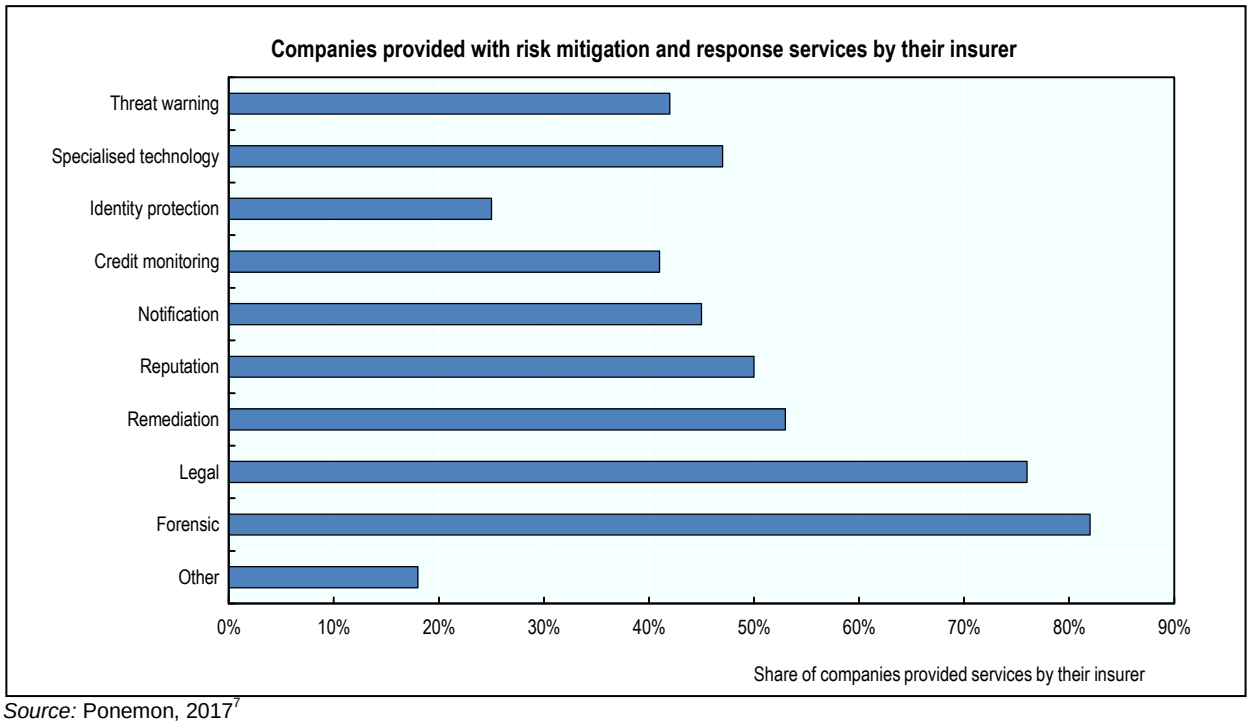


Source: OECD, 2017[4]

There is some evidence that companies see value in these additional services. Many companies use external providers of cyber risk mitigation and response services for assessments of company practices, access to real-time threat information, training for employees and executives, specialised legal services, call centre services, forensic investigations and credit monitoring services.[5] The inclusion of these types of services with insurance policies may

[4] OECD (2018), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
[5] Advisen (2016), *Information Security and Cyber Risk Management: The Sixth Annual Survey on the Current State of and Trends in Information Security and Cyber Risk Management*, Advisen Ltd. (October).

provide access to the services at a reduced cost, lowering the financial impact of cyber incidents and increasing the value of the insurance policy to the policyholder.[6]



Source: Ponemon, 2017[7]

Key questions for discussion

- What elements of the current insurance offering (financial protection, risk management services) has been most useful as part of companies' approaches to managing cyber risk?
- Are there ways in which current cyber insurance offerings should improve (additional types of protection, additional risk management services) in order to increase the attractiveness of insurance for corporate risk managers?

[6] Surveys of US companies have found that additional service offerings (risk mitigation and response together) are important drivers of insurance purchase for both small and large enterprises (see Council of Insurance Agents & Brokers, *Cyber Insurance Market Watch Survey* (October 2016 and May 2017). NetDiligence's *2015 Cyber Claims Study* found that access to these services reduced the cost of responding to cyber incidents by up to 30%.

[7] Ponemon Institute (2017), *2017 Global Cyber Risk Transfer Comparison Report*, Ponemon Institute LLC, Traverse City (Michigan).

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 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.

Drivers of uncertainty in cyber insurance underwriting

Limited historical data	• Cyber risk has only emerged as a peril in recent years (limited time-series data on incident frequency/impact) • A potentially low share of cyber incidents are discovered • Few incentives to voluntarily disclose incidents (and related impacts) that are discovered
Changing nature of risk and impact	• Attacks are driven by human behaviour rather than natural/physical forces • Attack methods evolve/improve and respond to improvements in defences • Increasing exposures as reliance on digital technologies increases • Changing legal and regulatory environment (including liability/compensation practices) leads to changes in financial implications (complicated by differences across jurisdictions)
Limited understanding of - and access to - security information	• The effectiveness of different security practices is impacted by evolutions in attack methods • Sensitivity of information on corporate defences creates a reluctance to share information between insured and insurer

The modelling of cyber risk for the purposes of underwriting (and pricing) insurance coverage, transferring risks to reinsurance and capital markets and calculating capital requirements is just emerging. Most currently available models are scenario-based rather than probabilistic and focused on extreme incidents for the purpose of managing accumulation risk. Some probabilistic models have been developed for higher-frequency incident types such as third party (personal) data confidentiality breaches given the greater availability of data. A number of modeling firms are also developing new approaches focused on the security practices of companies rather than the nature of the peril and attackers.

Key questions for discussion

- To what extent can policy and regulation support disclosure of - and access to data on - cyber incidents? Are there legal or regulatory impediments to data sharing that need to be addressed?
- Is it feasible to expect modelling to play a similar role for cyber risk as other natural or man-made catastrophe risks?
- Is an eventual convergence in incident data collection and modelling approach desirable? If so, how can it be achieved?

Session 4: Enhancing the contribution of reinsurance capital markets

Accumulation risk is a common challenge to insurance providers whose business is based on their ability to pool a set of uncorrelated risks and benefit from risk diversification. In the case of cyber risk, dependence on the same information technology infrastructure, software and services across countries and sectors limits the ability to build a diversified portfolio and leaves insurance companies exposed to accumulation risk related to vulnerabilities in commonly-used software, hardware and/or operating systems and disruptions to cloud service, domain name system and other service providers.

Recent events with potential for accumulation risk

Wannacry (common software vulnerability)

In May 2017, a massive global attack using a ransomware worm known as "WannaCry" reportedly infected more than 300 000 computers in 150 countries around the world, including at the UK National Health Service, the Russian Ministry of Interior, the DeutscheBahn railway and global companies such Nissan, Renault, and FedEx. The ransomware took advantage of a known vulnerability in the Microsoft Windows operating system (for which a patch had been released in March).

NotPetya (common software vulnerability)

In June 2017, a second ransomware attack, known variously as "Petya", "NotPetya" and "GoldenEye" affected companies in North America, Asia. Latin America, Australia and particularly Europe, including large companies such as Maersk and FedEx's TNT subsidiary. Similar to "WannaCry", the ransomware accessed companies through a "backdoor" vulnerability (through an accounting software commonly-used in the Ukraine).

Meltdown and Spectre (common hardware vulnerability)

Meltdown and Spectre are vulnerabilities to the most common processors disclosed in January 2018. The vulnerabilities could allow access to sensitive information contained in a computer's memory by exploiting the speculative execution capacity designed to improve the performance of central processing units. It is not known whether this vulnerability has been exploited.

Source: OECD, 2017;[4] Codenomicon, 2014 (Heartbleed image);[8] Cyber Defence Intelligence Consulting, 2016 (Mirai botnet image);[9] Graz University of Technology/Natascha Eibl, 2018 (Meltdown/Spectre image).[10]

While thus far limited in impact, a catastrophic event involving losses to many policyholders, such as the simultaneous exploitation of a common software vulnerability, could be beyond the market's capacity and lead to numerous exits from the market (similar to what occurred after Hurricane Andrew in 1992 or the September 11 terrorist attacks in the United States).

Reinsurance companies face many of the same challenges to providing coverage for cyber risks as primary insurers - lack of historical experience, changing risk landscape - and particularly the potential for accumulation risk. Reinsurers

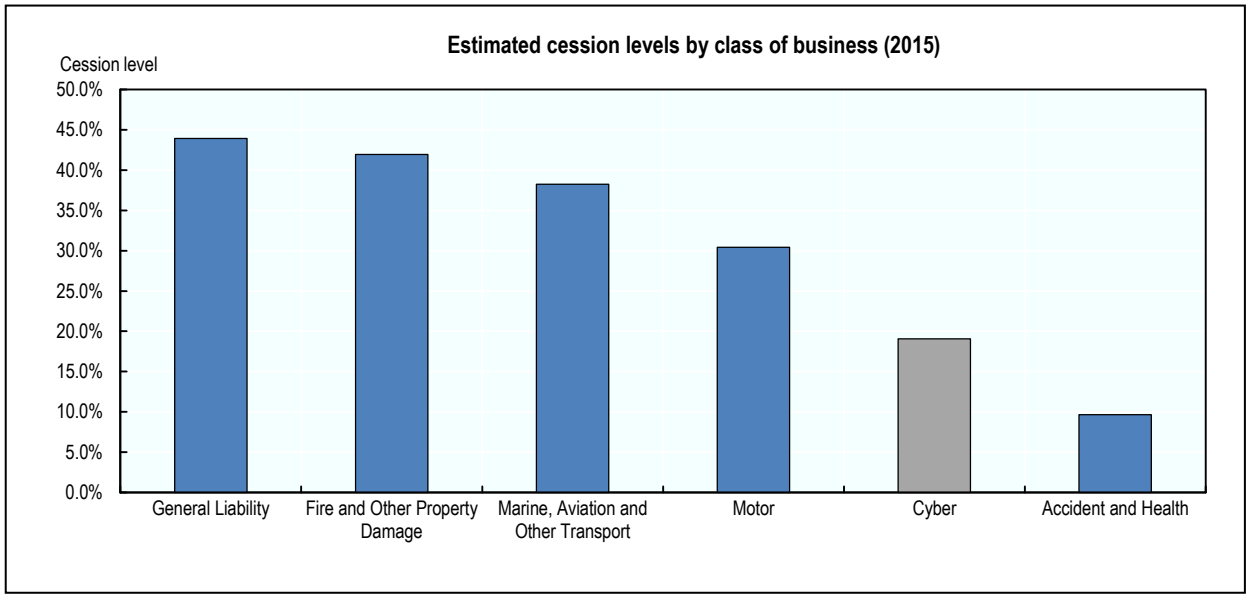
[8] The Heartbleed name and logo were established by Codenomicon, 2014 (http://heartbleed.com/heartbleed.svg).

[9] The image for the Mirai botnet is from: Cyber Defence Intelligence Consulting, "BestBuy Hackers Are Offering Mirai Botnet To Fellow Hackers As a Paid DDoS", *Cyber Defence Intelligence Consulting*, https://www.cyberintelligence.in/BestBuy-Hackers-Offering-Mirai-Botnet-As-a-paid-DDoS-Service/

[10] The logos for meltdown and spectre were established by Graz University of Technology (2018), Meltdownattack (website), https://meltdownattack.com/.

may also face significant amounts of implicit (silent) exposure to cyber risk through their traditional lines as exclusions are not commonly applied in casualty (liability) reinsurance programmes and the cyber exclusions that are sometimes applied by reinsurers on property reinsurance coverage are generally untested.

Some reports have suggested that there is limited reinsurance appetite for cyber risks and that the capacity that is available is being provided cautiously through the use of sub-limits and event limits. 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 limited data available suggests that the use of reinsurance for cyber risk coverage is low relative to other lines of business.



Source: OECD Insurance Statistics;[11] OECD, 2017[4]

Key questions for discussion

- How will increasing digitalisation impact the level of accumulation risk?
- What is needed to enhance the contribution of reinsurance and capital markets to absorbing cyber exposure?
- Is there a need for a government backstop for covering cyber risk (or some portion of cyber risk)?

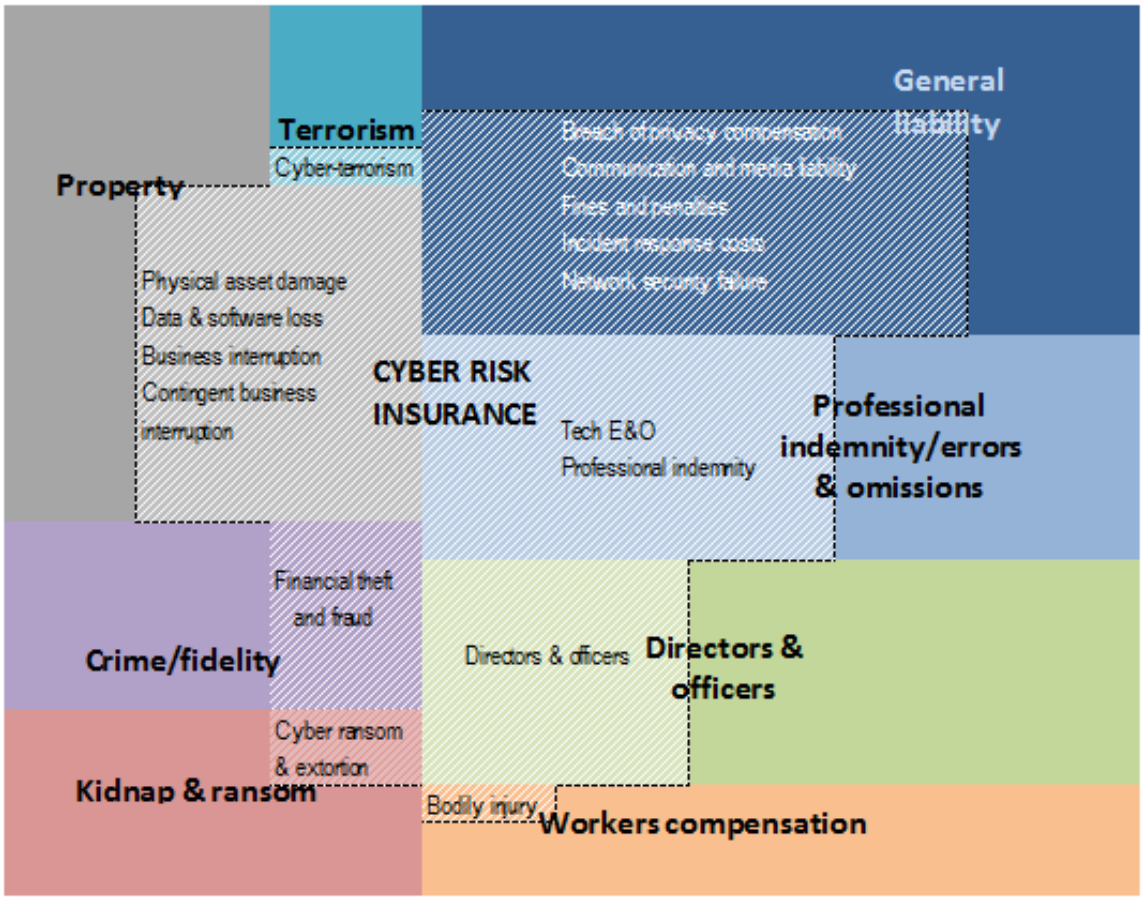
[11] OECD (2016), "Dataset: Premiums written by classes of non-life insurance", *Insurance Statistics database*, OECD.

Sessions 5/6: Providing greater clarity on coverage

The variation and complexity of cyber insurance policies - and the resulting misunderstandings related to the coverage provided - is often cited as an impediment to the greater take-up of cyber insurance:

- *Traditional vs. stand-alone coverage:* Coverage for cyber risk may be found in either dedicated cyber insurance policies (i.e. stand-alone cyber insurance policies) or various types of traditional policies. Stand-alone products have developed by carving-out specific cyber-related exposures (e.g. business interruption without material damage, data breach liability, social engineering fraud, cyber-extortion) from traditional property, general liability, crime and kidnap and ransom policies. Some traditional policies include cyber-related coverage, either by not applying exclusions or by specifically endorsing coverage for cyber-related exposures. There is limited sign of an emerging consensus on the best approach, either among underwriters or brokers that are providing advice on insurance for cyber risk.

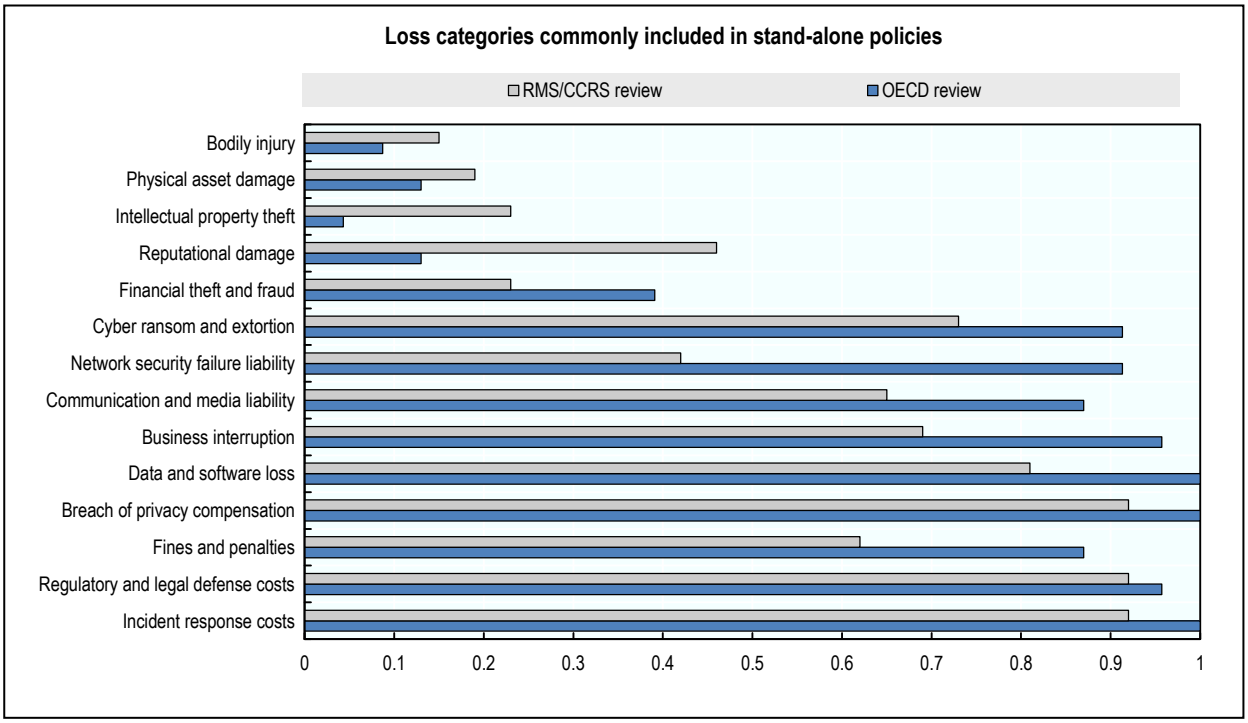
The potential for overlapping coverage in stand-alone and traditional policies



Source: OECD, 2017[4]

- *Complex and variable terms and conditions:* Coverage for cyber risks is complex and rapidly-changing with significant variation across policies - leading to challenges in understanding the specific conditions and coverage limitations in different cyber insurance policies. Important differences exist in terms of the triggers for payment, the possibility for retroactive coverage and the coverage provided for human error, voluntary notification and for incidents involving outsourced systems.

In addition to the variation and complexity of cyber insurance policies, there is some evidence that existing policies are not responding to all of the needs of prospective policyholders. This may be the result of limited coverage of losses related to reputational damages (i.e. loss of profits due to customer churn) and own intellectual property theft which are often cited as material cyber risks although rarely covered in cyber (or other) insurance policies.



Source: OECD, 2017[4]

Key questions for discussion

- What particular element of existing market offerings causes the most confusion for cyber insurance buyers?
- Is there an emerging consensus in the markets towards either providing coverage for cyber risks in stand-alone or traditional policies? What are the advantages and disadvantages of each approach?
- Is there a need for [enforced] standardisation of policies or will this inhibit innovation? What is the likelihood that an appropriate level of harmonisation will be achieved as the market develops?

Closing Session: Supporting the development of an effective cyber insurance market

There is significant potential for the cyber insurance market to contribute to improving cyber risk management. However, to achieve that potential, a number of challenges to the market's development need to be addressed:

- The lack of data on cyber incidents and the changing nature of cyber threats are significant impediments to the management of cyber risk, including the transfer of cyber exposures to insurance markets.
- The potential for accumulated losses with sizeable impacts on a large number of policyholders is an important concern for insurance and reinsurance companies that limits their willingness to extend significant levels of coverage.
- There is a misalignment between the expectations of businesses in terms of their financial protection needs and the scope of coverage provided by insurance companies, partly attributable to the complexity of cyber risk and available policies.

Businesses, brokers, (re)insurance companies and governments all have a role to play in supporting the development of a vibrant cyber insurance market that contributes to cyber risk management. **Modellers and actuaries** can make an important contribution to reducing uncertainty about cyber risk and expanding the scope of cyber insurance coverage.

Businesses are ultimately responsible for protecting against cyber incidents that have negative consequences for their employees, customers and shareholders.

- To effectively manage cyber risks, businesses should enhance their understanding of the risks that they face and the potential financial consequences.
- 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, potentially through enhanced public disclosure of cyber risks and incidents.
- 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 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 where 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.
- Insurance companies should expand the scope of coverage provided for cyber risks, including for existing risks not normally covered by insurance policies and for new types of losses that may emerge as a result of an evolving cyber risk environment.
- Reinsurance markets (traditional and alternative) should expand the scope of coverage that they make available to primary insurers for cyber risks. The case for any government intervention in providing a backstop for catastrophic cyber losses needs to be made by the reinsurance sector.

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

- Brokers should invest more in educating their clients on how to assess their financial exposures and insurance companies on better aligning their products to client needs.

Governments' role is to support 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 strategies for addressing digital security risks.
- 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).
- Governments should ensure that the cyber insurance market is increasing clarity and reducing complexity in the products that they offer. Where necessary, supervisory guidance could be established to encourage greater clarity about coverage being offered (with consideration of the potential benefits of international coordination).
- Governments should not impose overly stringent regulatory or supervisory requirements on insurance (or reinsurance) companies offering coverage.

The growing reliance on digital technologies 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.

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.

www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm

in collaboration with