SUPPORTING AN EFFECTIVE CYBER INSURANCE MARKET

OECD REPORT FOR THE G7 PRESIDENCY

OECD

This report was prepared by the OECD for the G7 Finance Ministers and Central Bank Governors meeting on 11-13 May 2017.

SUPPORTING AN EFFECTIVE CYBER INSURANCE MARKET

OECD Report for the G7 Presidency

May 2017

The increasing use of and dependence on information technology in economic activities - while creating significant benefits in terms of productivity and efficiency - is also leading to significant risks. Among them are "digital security risks" which, when they materialise, can disrupt the achievement of economic and social objectives by compromising the confidentiality, integrity and availability of information and information systems. It is widely assumed that most companies have been, will be or don't know they have been affected by such "cyber"[1] incidents. Although quantitative measurement is still emerging and raises significant challenges, accounts of the frequency and scope of (reported) cyber incidents regularly find significant growth in both the numbers of incidents and the share of companies they affect. This has led to cyber risk being identified as the risk of highest (or second-highest) concern to doing business in five of the G7 countries in the World Economic Forum's 2017 Global Risk Report.[2]

Insurance coverage for cyber risk provides a means for companies and individuals to transfer a portion of their financial exposure to insurance markets. Insurance markets and companies can potentially contribute to the management of cyber risk by promoting awareness, encouraging measurement, and by providing incentives for risk reduction. For example:

- The process of seeking insurance coverage requires policyholders to understand (and quantify) the risk that they face in order to determine the amount of coverage that they require.

- The underwriting process will usually involve an assessment of risk management and security practices, including recommendations on further preventative measures that could be taken.

- The pricing of risk should provide incentives to reduce the risk to the extent that the investments in risk reduction will lead to reductions in premiums.

However, for insurance to have a significant impact on risk reduction, the market must be offering a material level of coverage to a large share of companies and individuals at risk - which is not currently the case.

---

1 For the purpose of this document, the term "cyber" as in "cyber incident" or "cyber insurance" covers issues related to digital security.

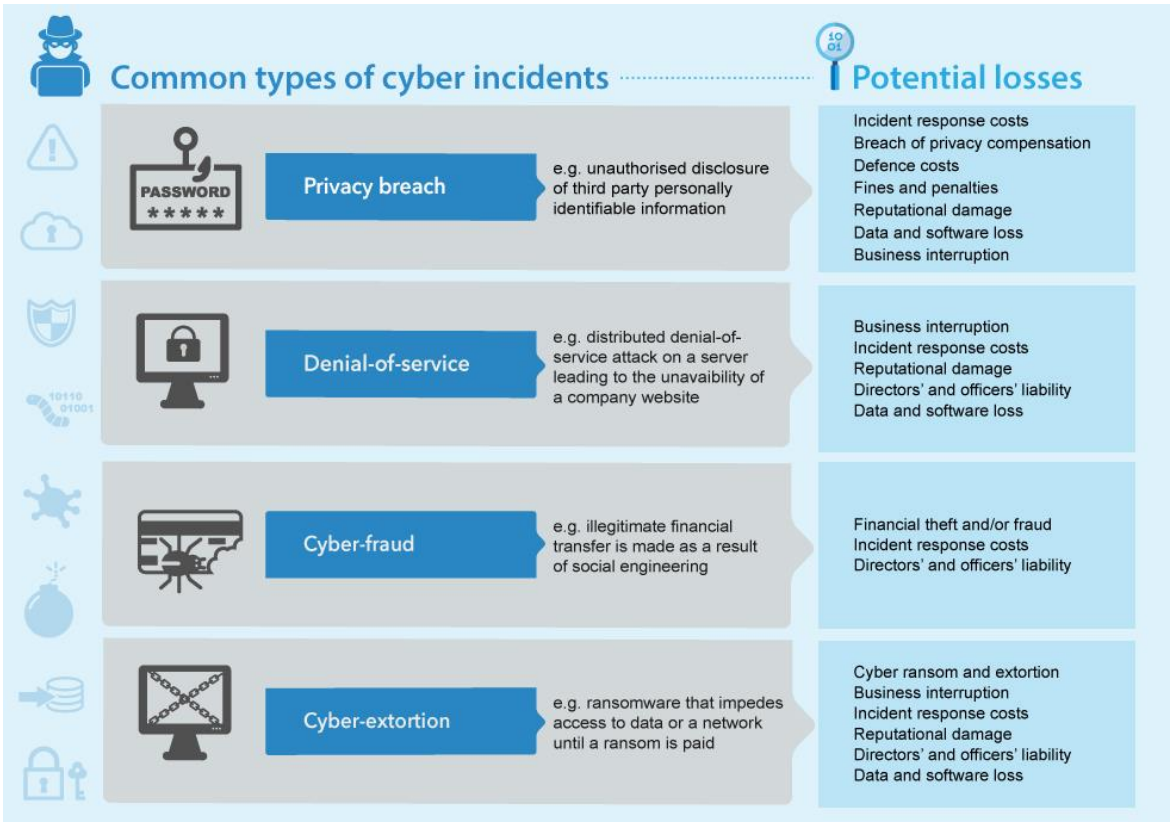
2 For the purposes of its annual Global Risks Report, the World Economic Forum defined two technological risks related to digital security: (i) "large-scale cyberattacks", defined as "large-scale cyberattacks or malware causing large economic damages, geopolitical tensions or widespread loss of trust in the internet"; and (ii) "massive incident of data fraud/theft", defined as "wrongful exploitation of private or official data that takes place on an unprecedented scale."

Prepared at the request of the G7 Presidency, this report provides an overview of the market for cyber insurance, including the available coverage and potential gaps as well as the current challenges in terms of data availability, quantification of cyber risks, awareness and misunderstanding about coverage. It is based on a larger report being developed by the OECD on cyber risk insurance.[3] The purpose of this report is to identify potential policy measures to address some of the main challenges to the development of an effective cyber insurance market, thus providing G7 Finance Ministers and Central Bank Governors with inputs for an informed discussion on this issue.[4]

The cyber insurance market

Cyber incidents, such as privacy breaches, denial-of-service attacks, cyber-fraud and cyber-extortion, can lead to a number of different types of losses for affected companies (see Figure 1). There have also been a few examples of physical damage and disruption resulting from cyber-attacks, including damage to a steel mill in Germany in 2014 and a large-scale power disruption in the Ukraine in 2015.

Figure 1. Potential losses from common types of cyber incidents



Note: A list of loss categories and definitions can be found in the annex.

[3] The report benefitted from responses to an OECD questionnaire from OECD governments (ministries of finance and regulators) as well as (re)insurance companies and brokers from around the world. More information on this project is available at: www.oecd.org/finance/insurance/cyber-risk-insurance.htm.

[4] These issues are being also addressed at the OECD from the perspective of the digital economy policy and as part of its work on improving the management of cybersecurity and privacy risk, following the 2016 Cancun Ministerial on the Digital Economy.

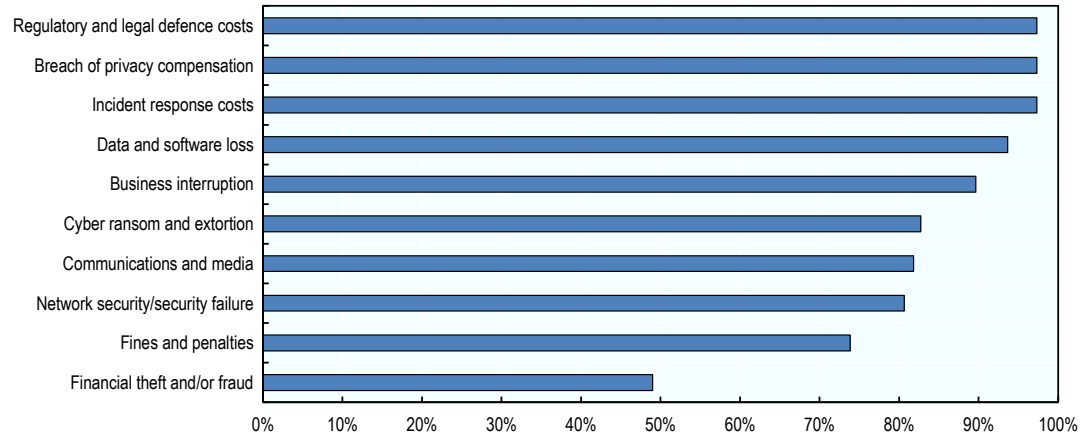
While the market for cyber-insurance is generally perceived as being in its infancy, specific insurance products covering cyber risk have been available for approximately 20 years in some countries. Coverage may be provided as a stand-alone policy, as a specific endorsement on existing policies (e.g., where coverage for specific losses is added to a property policy) or as part of traditional coverages without a specific endorsement (often referred to as silent cyber coverage) (see Box 1). The stand-alone cyber insurance market reached an estimated USD 3.5 billion in written premiums in 2016, of which approximately USD 3 billion was written on behalf of US-based companies and USD 300 million was written on behalf of European companies (for comparison, gross written premiums in G7 countries in 2015 were USD 373 billion and USD 230 billion in the motor vehicle and fire/property insurance lines, respectively (residential and commercial) (OECD, 2016)). Some estimate that the market could more than double by 2020, mostly due to growth in Europe (partly driven by the implementation of the EU General Data Protection Regulation which will create uniform notification and disclosure requirements, impose fines and enhance the ability for victims of data theft to seek compensation).

Box 1. Possible forms of coverage for losses related to cyber incidents

Stand-alone cyber insurance policies

The stand-alone cyber insurance market has developed in response to the introduction of exclusions of cyber-related losses from property, crime, kidnap and ransom, liability and other traditional insurance policies. There are three main types of exclusions: (i) general exclusions of all losses resulting from a cyber-attack or incident; (ii) an exclusion applied in general liability policies to exclude liability related to data breaches; and (iii) exclusion of losses related to data restoration. The application of these exclusions, along with a requirement that there be property damage in order for business interruption coverage to be triggered, has led to gaps in coverage for these losses as well as other types of losses that are most commonly (or only) incurred as a result of cyber incidents. As a result, most stand-alone cyber insurance policies have been developed to close these gaps and cover some of the main losses that normally result from privacy breaches and, to a lesser extent, denial-of-service attacks, cyber-extortion and cyber-fraud (see Figure 2).

Figure 2. Share of stand-alone cyber policies covering different loss types



Source: The share is calculated as the average of: (i) the share of policies that cover the given type of loss among seven of the largest providers of stand-alone cyber insurance (AIG, Allianz, AXA, Beazley, Chubb, XL Catlin, Zurich); (ii) the share of policies that cover the given type of loss based on a survey of 26 policies (global) undertaken by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016); and (iii) the share of policies that cover the given type of loss based on responses to the OECD's survey questionnaire (including 9 insurance companies and 9 insurance brokers from around the world).

Cyber risk coverage in traditional insurance policies (endorsed and silent)

Where none of the exclusions noted above are applied in traditional policies, some cyber-related losses may be covered by traditional property, liability, crime/fidelity and kidnap and ransom policies (see Figure 3). This coverage may be explicitly understood by the insurer and policyholder, for example through the inclusion of a specific endorsement providing such coverage. However, in other cases, the coverage may only be "discovered" as a result of a claim dispute and/or litigation. There is limited information on the use of the cyber-related endorsements and exclusions in traditional policies (and therefore the extent of coverage for cyber risk in those policies). Anecdotal evidence and responses to an OECD questionnaire suggest that exclusions to property policies (i.e. the general cyber exclusion and the exclusion of data restoration costs) are often used in most markets while the general liability exclusions are more commonly applied in the United States than in European markets (including the United Kingdom).

Figure 3. Potential coverage for cyber risk in traditional policies

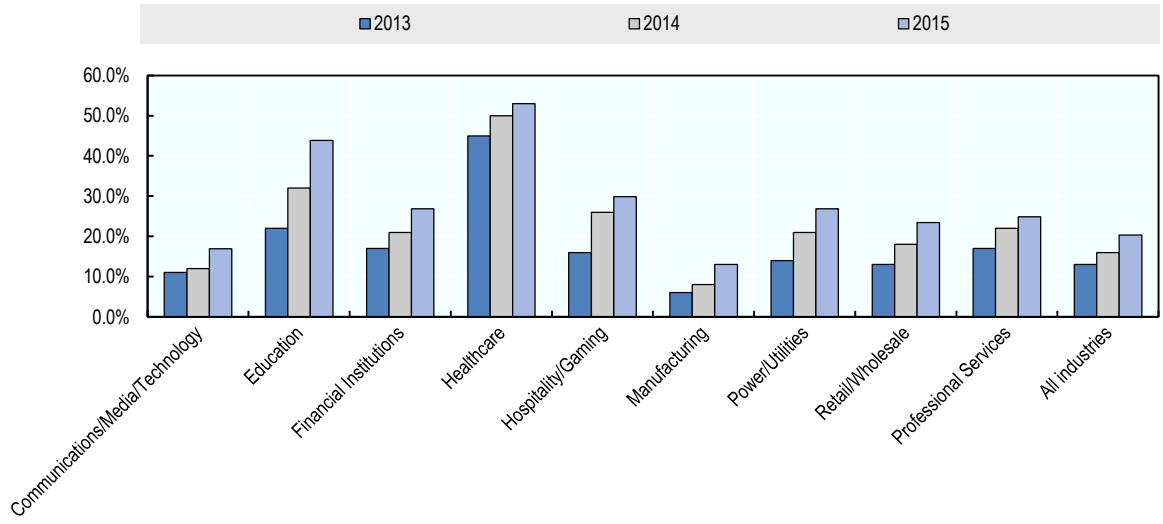
The level of cyber insurance coverage provided through traditional policies is difficult (if not impossible) to estimate as the share of the premium that is collected to cover cyber risk is not reported separately (if disaggregated at all).

Signs of market immaturity

While the market has been growing rapidly in recent years, there are a number of signs that the market has yet to mature:

- *Relatively low take-up:* In most mature insurance markets, take up of commercial property and liability insurance coverage will be very high (potentially approaching 100% of all businesses). However, in the case of cyber risk, the share of businesses that have purchased coverage is much lower - 20% to 35% of all US companies have specific (stand-alone or endorsed) cyber insurance coverage whereas in Europe and the United Kingdom, an estimated 20% to 25% of mid-to-large companies (which have a broker) have purchased specific cyber insurance. Given that cyber risks are not consistently excluded from traditional policies, the purchase of specific cyber insurance coverage by all companies should not be necessary. However, the differences in take-up rates across different sectors (see Figure 4) and between large and small companies suggest that a lack of awareness may partly explain the low levels of penetration.[5]

Figure 4. Estimated stand-alone cyber-insurance take-up rates by sector (Marsh clients)



Source: Marsh (2015c) reports take-up rates in 2013 and 2014 among its clients (mostly US clients). Marsh (2016) only reports growth in take-up among its clients so the estimated take-up rate in 2015 is derived based on the reported growth rates.

[5] A number of studies have suggested that limited awareness of cyber risk - and particularly, awareness of the potential cost of cyber incidents - among companies is an important impediment to broader take-up of cyber insurance coverage. Close to 80% of the respondents to the OECD questionnaire indicated that the level of awareness of cyber security risk among potential policyholders was an important or moderately important driver of the level of cyber security risk. In the PwC 2016 Annual Survey of Corporate Directors, board engagement on cyber security differed widely depending on firm size. For example, 68% of directors at mega-sized companies indicated that their board is very engaged in overseeing/understanding the risks of cyber-attacks, compared to 32% of directors at smaller companies.

- *Broad differences in coverage available from different insurers*: The types of losses covered by stand-alone cyber insurance policies can vary significantly across providers as can the level of coverage for cyber risk that remains in traditional insurance policies after exclusions. In the case of stand-alone policies, important differences exist across policies in terms of the coverage of different types of liability (breach of privacy compensation, communications and media and network security/security failure), whether fines and penalties and ransom payments are covered,[6] as well as the extent to which losses involving some form of human error are covered.[7]

- *Policies may not be covering some important losses*: Some types of cyber incidents can result in significant losses that are not usually included within the scope of stand-alone or traditional insurance coverage. A large privacy breach, for example, can have significant impacts on a company's reputation and future business (see Box 2) although very few policies[8] provide any compensation for these types of losses (which is not usually available for other perils either). The loss of value of intellectual property (due to its theft through cyber-espionage, for example) is also rarely covered in either stand-alone cyber policies or traditional insurance policies.[9] In both cases, the key impediment to coverage is the difficulty in quantifying the value of the future business that has been lost due to reputational damage or the reduced ability to exploit the commercial value of intellectual property.[10]

- *The amount of coverage available may be limited*: There is some evidence that the amount of coverage available, particularly for larger companies in high-risk sectors, is insufficient relative to the coverage demanded.[11] In addition, sub-limits and deductibles, such as the 8-12 hour deductible period often imposed before business interruption coverage is triggered, also serve to limit the level of coverage available.

---

6 Some jurisdictions do not permit insurance coverage for regulatory penalties and fines or have legal systems where the legality of insurance payments for penalties and fines has been challenged. In addition, some insurers do not provide coverage for fines and penalties or ransom payments based on their own internal business practices.

7 For example, the theft of funds through social engineering may be excluded from policies where coverage for financial losses is limited to unintentional acts (a transfer of funds, even where initiated under false pretences, could still be deemed to involve an intentional act by an employee).

8 Less than half of the 26 policies examined by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) provided coverage for reputational damage while none of the policies of the seven large providers of stand-alone cyber insurance included such coverage.

9 Less than a quarter of the 26 policies examined by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) provided coverage for intellectual while none of the policies of the seven large providers of stand-alone cyber insurance included such coverage.

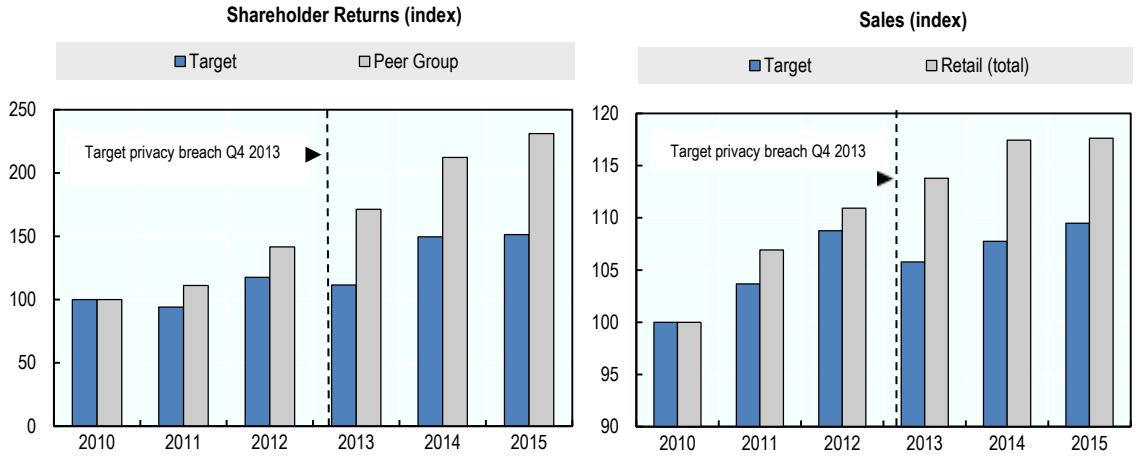
10 As an example, the pirating of an unreleased motion picture might lead to reduced cinema attendance, although it is extremely difficult (if not impossible) to isolate the specific value of lost business due to the unauthorised release.

11 See, for example: Betterley (2015); Council of Insurance Agents & Brokers (2016a); Sclafane (2015); PwC (2015b).

Box 2. The implications of lost business: Target breach

In the fourth quarter of 2013, Target, a major US retailer, discovered a significant privacy breach that led to the theft of approximately 40 million payment card records (along with 70 million other information records such as addresses and phone numbers) (Phillips, 2014). As of 30 January 2016, the company has reported USD 291 million in incurred expenses as a direct result of the privacy breach, including settlements with four major payment card networks, affected customers and financial institutions (as issuers of the payment cards). A number of lawsuits remain pending, including those launched by Canadian customers and shareholders as well as investigations by State Attorneys General and the Federal Trade Commission which could result in fines or penalties (Target Corporation, 2016). While the direct expenses incurred were significant, there is some evidence that the larger impact has been in terms of lost business and reputation. While competitors' shareholder returns and sales continued to rise during the period, Target's sales and shareholder returns declined immediately after the breach, widening the gap between Target and its peers (see Figure 5).

Figure 5. The business impact of a major privacy breach: Target

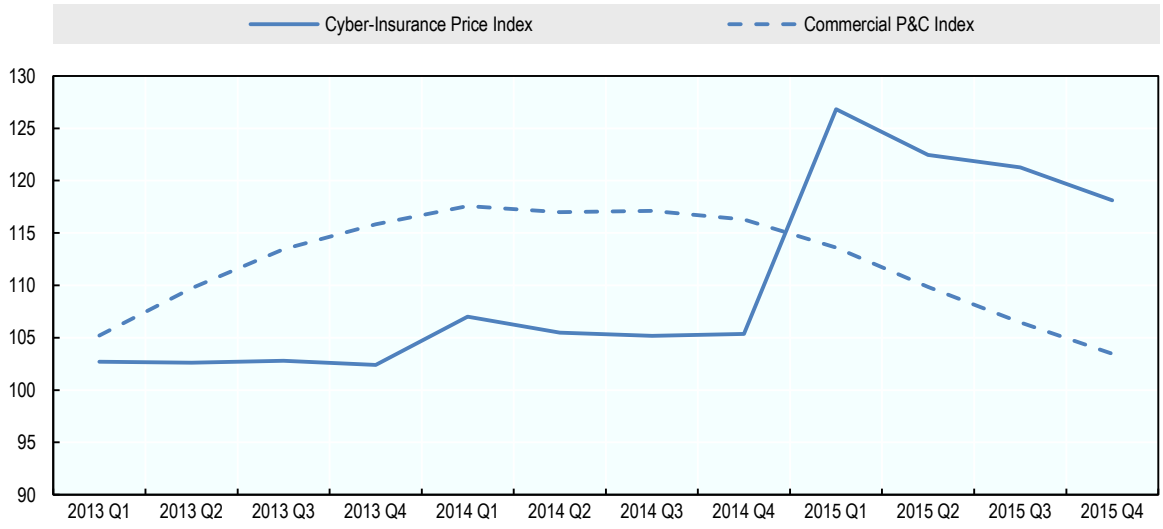


Source: Target Corporation (2014 and 2016); US Census Bureau, *Retail Excluding Motor Vehicle and Parts Dealers*, www.census.gov/retail/marts/www/adv4400a.txt (accessed 22 November 2016). The peer group included in the figure on shareholder returns was defined in Target Corporation (2016) which also included the data on shareholder returns. Both shareholder returns and sales have been converted into indices (2010 base year).

- *The premiums charged for cyber insurance coverage is high and variable*: The premiums for cyber insurance per million in coverage has been estimated to be three times more expensive (for the same amount of coverage) than general liability coverage and six times more expensive than property coverage. In addition, premiums have been increasing (in general) even as the cost of other types of commercial insurance coverage has been declining in recent months (see Figure 6). There are also anecdotal reports of significant variation in prices being quoted by different insurance companies for the same underlying risk.[12]

[12] For example, a company in Germany reportedly received quotes for EUR 5 million in coverage that ranged between EUR 20 000 and EUR 120 000. A pharmaceutical company in the United States was quoted premiums that varied by 300% for a defined set of coverage (Sclafane, 2015).

Figure 6. Cyber and commercial property insurance price indices (United States)



Source: The cyber-insurance price index was derived from the growth rates in average primary price per million for cyber liability insurance reported by Marsh (2014a, 2015c, 2016) (2012=100), although growth rates are presented by Marsh relative to the same quarter in the previous year. For the years considered, most pricing data was for Marsh clients in the United States. The commercial property and casualty index was derived from the average quarterly change in pricing across all US companies as reported by the Council of Insurance Agents and Brokers (2013, 2014, 2015b, 2016b) (2012 Q4=100).

Cyber insurance market challenges

There are a number of factors that may be impeding the availability and affordability of cyber insurance coverage, including factors that lead to a higher cost for cyber insurance coverage (such as uncertainty about the level of exposure to cyber risk and the potential for correlated exposures) as well as factors that may be reducing companies' willingness-to-pay for that coverage (such as lack of risk awareness and misunderstandings about available coverage):

- *Uncertainty about exposure*: Cyber risk is a relatively new peril meaning there is limited historical data on which to base the pricing of insurance premiums. The general unwillingness of the victims of cyber incidents to share information on these events and their impacts (out of concern for potential reputational impacts) further limits access to historical data. Furthermore, the fast-evolving nature of cyber risk - where the perpetrators of cyber-attacks can be expected to continue to improve their methods of attack and find new ways to evade cyber defences - constrains the usefulness of the limited historical data that does exist. The legal and regulatory environment is also quickly evolving, impacting the scope and magnitude of the costs likely to be incurred as a result of a cyber-incident.

- *Risk of correlated exposure*: There is significant potential for cyber-related losses to be correlated across insureds (i.e. where a number of insured companies are affected by the same (or same type of) incident). A number of potential scenarios could lead to correlated losses, including: (i) a vulnerability in a commonly-used software that, if exploited, would allow for an opportunity for widespread sabotage or for a widespread data breach (for example, what could have occurred as a result of the "Heartbleed" vulnerability disclosed in

2014[13]); (ii) attack methods that are easily scalable and widely applicable; or (iii) attacks on common information technology infrastructure, such as a cloud service provider, the domain name system that underpins the functioning of the internet (such as the 21 October 2016 denial-of-service attack against a domain names system service provider that disrupted access to a number of internet sites in the United States), critical infrastructure provider (power supply, payment system, satellites or air traffic control systems) or an important participant in a supply chain.

- *Limited awareness of potential exposures to cyber losses*: While most companies will be aware of the possibility that their networks might be breached or that their web servers could face a denial-of-service attack, a much lower proportion have assessed the potential financial impact of a cyber-incident[14] - which would normally be the basis for any decision to purchase insurance.

- *Misunderstanding in the coverage available*: As noted, coverage for cyber-related losses may be provided through stand-alone cyber insurance policies, endorsements to stand-alone policies or traditional policies, or in any number of traditional policies covering property, crime, kidnap and ransom or various types of liability. Even among stand-alone cyber insurance policies, significant variation exists in terms of the types of losses covered, sub-limits and deductibles applied, as well as the time basis for claim eligibility. The complexity involved in ensuring appropriate coverage for cyber risk, along with the mismatch between the coverage available and some of the types of losses commonly incurred (e.g. reputational harm and intellectual property theft) has resulted in some concern about whether cyber insurance will actually pay out in the event of an incident.[15]

Impediments to cyber insurance and potential policy priorities to support the development of the market

The potential for cyber insurance coverage to contribute to risk reduction and the management of cyber losses will only be achieved if the market is able to meet the most important needs of commercial and individual policyholders. Governments can potentially play a role in supporting the development of the market and maximising the contribution it makes to managing this fast-evolving risk by examining ways to address the main impediments to market development, particularly across the following priorities:

- *Understanding impediments and gaps of the market*: As losses from cyber incidents increase, the benefits of and interest in having insurance coverage for this risk is increasing. However,

---

13 The "Heartbleed" vulnerability was publicly disclosed in April 2014 as a serious vulnerability in the commonly-used OpenSSL cryptographic software library which, if exploited, would allow for the stealing of information that is normally protected by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs) (heartbleed.com, 2014).

14 For example, a survey of global companies by BAE Systems (2014) found that only 48% had assessed the potential financial impact of a cyber-attack. This is supported by a survey by Advisen (2014) which found that, for 73% of insurance broker respondents, insureds lack of understanding about the potential financial impact of cyber security incidents was the biggest impediment to purchase.

15 For example, surveys by KPMG of information technology professionals in the United Kingdom found that close to 50% did not believe that their cyber insurance policies would pay out in the event of a cyber-attack (Reeve, 2015; Z/Yen, 2015

in order for coverage to become widely available and responsive to demand, there are a number of impediments and gaps in the market. International organisations should be encouraged to work further in this direction, including in particular the OECD which is expected to publish a policy report that could propose policy recommendations that address the impediments to market development and the availability of cyber insurance. This report, which will be provided to G7 countries, will contribute to their discussion on possible actions that can be taken going forward.

- *Improving the data available for quantifying exposures*: More comprehensive data on the frequency and impact of cyber incidents (and the related claims payments) would provide more confidence in the underwriting of insurance coverage for cyber risk - and therefore should support availability and affordability. The development of a more comprehensive data set on cyber incidents would likely require: (i) a common classification of cyber incidents and types of losses; (ii) a trusted party (e.g. government agency) to collect and report the data; and (iii) incentives (or requirements) for reporting by companies affected by cyber incidents and insurance companies that have paid related claims. There are a number of initiatives in the insurance sector and in individual countries aimed at meeting some of these requirements.[16] The OECD has also started to explore these issues as part of its work on improving the evidence base on cybersecurity and privacy policy-making following the 2016 Cancun Ministerial on the Digital Economy.

- *Improving public policies to manage cyber risk*: Most governments have adopted national cybersecurity or digital security strategies. However, while these strategies aim at improving awareness about cyber risk, they do not always address cybersecurity as an economic and social risk management issue. As called for by the 2015 OECD Council Recommendation on Digital Security Risk Management for Economic and Social Prosperity, national strategies could include incentives for businesses to measure and manage their exposure to cyber risk. In particular, corporate governance practices can provide an avenue to foster the integration of cyber risk into the broader enterprise risk management framework (instead of addressing it only as a technical matter). National strategies could also consider the benefit of further co-operation and co-ordination between government bodies in charge of cyber security, which could include insurance regulators. Finally, governments can play a role in ensuring that clarity is provided on the extent of coverage for cyber risk included in stand-alone and traditional policies by encouraging the insurance and policyholder communities to develop a common understanding about the appropriate place for cyber coverage and/or establishing requirements for insurers to provide greater transparency on the coverage provided (and losses that are excluded).[17] This would be particularly important for SMEs and individuals.

---

16 For example, work on classification of cyber incidents is being undertaken by the CRO Forum (insurance company chief risk officers and through the CyRiM (Cyber Risk Management) project in Singapore. The possibility of establishing a central data repository for information on cyber incidents is being examined by insurance companies and government agencies in the United Kingdom and the United States. Voluntary (and some mandatory) cyber incident reporting initiatives have been established in a number of countries.

17 For example, the UK Prudential Regulation Authority recently published a consultation paper recommending that insurers explicitly indicate (and charge premiums for) coverage provided for cyber security incidents in traditional policies. In France, an exercise led by IRT System X has resulted in the development of a matrix showing the areas of coverage of cyber risk provided by stand-alone cyber and various traditional policies in the French market.

ANNEX: LOSS CATEGORIES AND DEFINITIONS (AS DEFINED BY 2016 CHIEF RISK OFFICERS FORUM)

Incident Type Group	Coverage Scope
Assistance coverage - psychological support	Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent.
Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensible data leakage leading to suicide).
Breach of privacy [compensation]	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs.
Business interruption Interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage.
Communication and media	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web-page defacement as well as Patent/Copyright infringement and Trade Secret Misappropriation.
Contingent business interruption (CBI) for non-physical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage.
Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g. access to data is locked until ransom is paid).
Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted.
D&O [Directors' and officers' liability]	Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event.
Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event.
Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g. shares). It covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrong-doing by the observed company.

Incident Type Group	Coverage Scope
Fines and penalties	Compensation for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed.
Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defense costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defenses costs; (ii) public relations and communications costs; (iii) remediation costs (e.g. costs to delete or cost to activate a "flooding: of the harmful contents published against an insured); (iv) notification costs.
Intellectual property theft	Loss of value of an Intellectual Property asset, resulting in pure financial loss.
Legal protection - Lawyer fees	Costs of legal action brought by or against the policyholder including lawyer fees costs in case of trial. Example: identity theft, lawyer costs to prove the misuse of victim's identity.
Network security/Security failure	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incident response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach a third party.
Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company.
Products	Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (Tech E&O) and excluding Professional Services E&O.
Professional services E&O, Professional indemnity	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (Tech E&O).
Regulatory & legal defense costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company ir related third-parties when responding to governmental or regulatory inquiries related to a cyber-attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties). B: Legal defense costs: coverage for own defense costs incurred to the observed company or related third parties facing legal action in courts following a cyber-attack.
Reputational damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company.
Tech E&O	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event.

REFERENCES

Advisen (2014), *Cyber Liability Insurance Market Trends: Survey*, Advisen Ltd. (October).

BAE Systems (2014), *Business and the Cyber Threat: The Rise of Digital Criminality*, BAE Systems plc, Surrey, United Kingdom.

Betterley, R. (2015), "Cyber/Privacy Insurance Market Survey 2015", *The Betterley Report,* (June).

Council of Insurance Agents & Brokers (2016a), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (April).

Council of Insurance Agents & Brokers (2016b), Q2 Commercial P/C rates continued decline, according to CIAB Market Survey", *News Release*, 4 August, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2015), Pricing continued gradual decline in Q2, while interest in Cyber Liability grew", *News Release*, 29 July, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2014), Commercial P/C Pricing continued slide in Second Quarter of 2014, according to CIAB Survey", *News Release*, 31 July, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2013), Commercial P/C Pricing increases slowed in Second Quarter, according to CIAB Survey", *News Release*, 23 July, Council of Insurance Agents & Brokers.

CRO Forum (2016), *CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk*, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf.

Marsh (2016), *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*, Marsh LLC, March.

Marsh (2015), *Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise*, Marsh LLC, March.

Marsh (2014), *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh LLC, April.

OECD (2016), "Insurance business written in the reporting country: Premiums written by classes of non-life insurance", *OECD.Stat*, OECD Publishing, Paris, http://dotstat.oecd.org//Index.aspx?QueryId=25401.

Phillips, M. (2014), "Target's traffic still hasn't recovered from the giant data breach", *Quartz*, 21 May, http://qz.com/212003/targets-traffic-still-hasnt-recovered-from-the-giant-data-breach/, accessed 18 October 2016.

Prudential Regulation Authority (2016), *Cyber insurance underwriting risk: Consultation Paper CP39/16 (November)*, Bank of England, London, www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf.

PwC (2015), *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*, PwC.

PwC (2016), "The swinging pendulum: Board governance in the age of shareholder empowerment", *PwC's 2016 Annual Corporate Directors Survey*, PwC.

Reeve, T. (2015), "Cyber insurance not trusted by business, KPMG claims", SC Magazine UK, 1 May, www.scmagazineuk.com/cyber-insurance-not-trusted-by-business-kpmg-claims/article/412535/.

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, http://cambridgeriskframework.com/getdocument/39.

Sclafane, S. (2015), "Cyber Risk Insurers Lag in Buying Cyber Cover", *Carrier Management*, 16 July, www.carriermanagement.com/news/2015/07/16/142577.htm.

Target Corporation (2016), *2015 Annual Report*, Target Corporation, Minneapolis.

Target Corporation (2014), *2013 Annual Report*, Target Corporation, Minneapolis.

World Economic Forum (2017), *Global Risks Report 2017: 12th Edition*, World Economic Forum, Geneva, www.weforum.org/reports/the-global-risks-report-2017.

Z/Yen Group (2015), *Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance*, Long Finance.