Enhancing the Role of Insurance in Cyber Risk Management

OECD

Enhancing the Role of Insurance in Cyber Risk Management

Please cite this publication as:
OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris.
http://dx.doi.org/10.1787/9789264282148-en

ISBN 978-92-64-28213-1 (print)
ISBN 978-92-64-28214-8 (PDF)

Photo credits: Cover © KrulUA/iStock/Thinkstock.com

Corrigenda to OECD publications may be found on line at: *www.oecd.org/about/publishing/corrigenda.htm*.

Foreword

The digital transformation of economic activities is creating significant opportunities for innovation, convenience and efficiency. However, as recent major incidents have highlighted, a growing reliance on digital technologies comes with digital security and privacy protection risks. This presents policy makers with the challenge of finding an appropriate balance between addressing these risks while allowing sufficient space for achieving the economic and societal benefits of digitalisation. The role of the nascent cyber insurance market in enhancing cyber resilience is increasingly being recognised by policy makers.

This report, *Enhancing the Role of Insurance in Cyber Risk Management,* provides a series of policy recommendations aimed at enhancing the contribution of the cyber insurance market to managing this increasingly prevalent risk. The report examines the current state of the market, based on substantive input from the re/insurance companies, brokers and regulators that are directly involved in its development, and the obstacles that are impeding the market from reaching its full potential. It builds on the initial findings in the OECD report on *Supporting an effective cyber insurance market* which was presented to G7 Finance Ministers and Central Bank Governors in May 2017.

The OECD has supported the development of strategies for the financial management of natural and man-made disaster risks for a number of years, including through the *OECD Recommendation on Disaster Risk Financing* which provides a framework for addressing the financial impacts of disasters on individuals, businesses and governments.

This report was prepared by the OECD based on questionnaire responses received from the re/insurance companies and brokers active in this market globally and the ministries of finance and insurance regulators responsible for overseeing that market. It benefited from the support and input of the OECD Insurance and Private Pensions Committee, the OECD High-Level Advisory Board on the Financial Management of Large-Scale Catastrophes and the Working Party for Security and Privacy in the Digital Economy. The report contributes to the OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world (www.oecd.org/going-digital).

Particular efforts have been invested in ensuring that this overview is up-to-date at the time of publication (November 2017) although readers should keep in mind that the nature of cyber incidents and the insurance market response is evolving rapidly.

Table of contents

Tables

Figures

Boxes

Executive summary

Economic and commercial operations have become increasingly reliant on digital technologies which face a constant threat of disruption due to human error or malicious attacks. The potential for serious economic and commercial repercussions, illustrated most recently in the millions of compromised records at Yahoo and Equifax, the disruption of major websites by a denial-of-service attack on Dyn and the hundreds of thousands of computers compromised by the WannaCry and NotPetya ransomware attacks, has meant increasing investment in safeguarding the confidentiality, integrity and availability of information and information systems.

While not a substitute for investing in cyber security and risk management—as having good cyber security and avoiding a disruption is a more preferable outcome—insurance coverage for cyber risk can make an important contribution to the management of cyber risk by promoting awareness about exposure to cyber losses, sharing expertise on risk management, encouraging investment in risk reduction and facilitating the response to cyber incidents. There is some evidence that the insurance market is making this contribution by sharing expertise on risk management, differentiating its pricing based on levels of risk and providing valuable support to both large and small companies in responding to crises.

However, the *potential* contribution of insurance markets to the management of cyber risk is even greater. The stand-alone cyber insurance market remains a fraction of the size of other commercial property and liability insurance markets with penetration (take-up) levels near 30% of companies in almost all countries (and in single digits for small and medium-sized enterprises (SMEs)). For those companies that do purchase cyber insurance, coverage limits are usually much lower than what is available for other perils and provided at a much higher premium level. In addition, some of the most important needs of companies, such as coverage for losses related to reputational damage or intellectual property theft, are rarely covered by cyber insurance products.

Overcoming the major obstacles to the development of the cyber insurance market could lead to greater and wider coverage of cyber risk and have a larger impact on risk management. The lack of historical data on cyber incidents and (in particular) the ever-evolving nature of the risk impede the ability to develop probabilistic pricing and exposure management models. The lack of trusted models reduces the willingness of insurance companies (and reinsurers) to extend significant amounts of coverage and leads them to apply various exclusions and sub-limits to control their exposure. The limited coverage available in the market along with the complexity of the terms and conditions imposed have led policyholders to question the value of cyber insurance coverage in its current form.

This report provides an overview of the financial impact of cyber incidents, the coverage of cyber risk available in the market, challenges to market development and

initiatives aimed at addressing those challenges. It has benefitted from the input of a broad range of stakeholders from across the global re/insurance sector and the digital security and financial sector policy communities, including two OECD committees (Insurance and Private Pensions Committee and the Working Party for Security and Privacy in the Digital Economy) and the High-Level Advisory Board on the financial management of catastrophic risks.

Key findings

- **Insurance can contribute to improving the management of cyber risk and should be considered an essential component of countries' strategies for addressing digital security risks.** The risk management expertise of the insurance sector should be leveraged to help countries address the risks inherent in the ongoing transition to a digital economy. The re/insurance sector's capacity to quantify risk, encourage risk reduction and absorb losses could make an important contribution to improving risk management. In this regard, addressing challenges to the cyber insurance market's development should be considered as a potential objective of digital security risk management strategies and policies.

- **The policy, legal and regulatory framework can have important implications for how much information on cyber incidents is made available and therefore the level of uncertainty when underwriting cyber risk.** The types of notification and disclosure requirements imposed on companies by privacy authorities, securities regulators and/or sectoral regulators are critical factors in determining the availability of data on past cyber incidents. In countries with more limited notification or disclosure requirements, the availability of incident data is generally minimal. Governments should consider the contribution that notification and disclosure requirements could make to improving the availability of data on cyber incidents.

- **The lack of data on cyber incidents is a significant impediment to the management of cyber risk, including the transfer of cyber exposures to insurance markets. Greater public-private collaboration will be required to overcome this obstacle.** There are a number of obstacles to overcome in order to establish incident reporting repositories, including governance and security issues as well as differing approaches to categorisation and definitions. There are significant differences in approach and efforts to identify potential avenues for collaboration between the different initiatives have only recently begun. In order to maximise the availability of data, governments and the insurance sector need to work towards a harmonised framework for categorising cyber incidents and losses.

- **The insurance market, including re/insurance companies, brokers and relevant associations, have an important role to play in providing greater clarity about the coverage available for cyber risk and which policies provide that coverage.** Different approaches to coverage provides choice to policyholders and allows for innovation. However, differences in terminology and diverging approaches to offering coverage exacerbate an already significant amount of misunderstanding among policyholders on how to protect against the financial impacts of cyber risks. The insurance market can greatly reduce the level of uncertainty by working towards a common terminology on risks and

losses - governments should ensure that the insurance market is moving in this direction.

- **There is significant concern about the potential for accumulated losses as a result of an incident with sizeable impacts on a large number of policyholders. Governments should develop strategies for managing the potential financial impacts of a catastrophic cyber event, taking into account the guidance provided in the OECD Recommendation on Disaster Risk Financing Strategies.** This concern is limiting the level of coverage that is being made available and leading to the application of various exclusions to limit insurance company's (and reinsurer's) exposure to accumulation risk. While incidents that have occurred thus far have been well within the capacity of the insurance and corporate sectors to manage, governments may want to examine options for addressing accumulation risk before the occurrence of the cyber equivalent of a September 11th or Hurricane Andrew. The guidance provided in the *OECD Recommendation on Disaster Risk Financing Strategies* could support government efforts in managing their financial exposure to a cyber catastrophe by providing a framework for addressing the financial impacts of catastrophic events.

- **Leveraging its expertise in insurance and digital security risk management, the OECD can contribute to helping governments overcome challenges to the development of the cyber insurance market, including through additional research in the areas identified in this report.**

Chapter 1

Growing cyber risk and the contribution of insurance to cyber risk management

This chapter provides an overview of the context for this study, notably the increasing concerns about the implications of cyber risk, as well as some information on the survey undertaken for the purposes of informing this report. It also describes the potential contribution of insurance to managing cyber risk through: (i) supporting the quantification of cyber exposure; (ii) providing expertise on risk management and prevention; (iii) facilitating access to crisis management services; and (iv) encouraging risk reduction through premium pricing.

The increasing use of digital technologies in economic activities - while creating significant benefits in terms of convenience, 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. Accounts of the frequency and scope of (reported) cyber incidents regularly find significant growth in terms of the numbers of incidents, the share of companies they affect, as well as the impact of these incidents on companies' operations. The growing scope of digital technology in economic activities means that this risk is likely to increase in the near future (see, for example, OECD (2016)). However, the sensitivity around disclosure of cyber incidents and limited history of loss experience, the evolving nature of the threat and potential for accumulated losses as well as the increasing integration of digital technology into operational systems make cyber risk a particularly challenging risk to measure - and manage.

Cyber risk was identified as the risk of highest (or second-highest) concern to doing business in more than one third of OECD countries in the World Economic Forum's 2017 Global Risk Report (and among the five risks of greatest concern in more than half of OECD countries, a higher share than either terrorist attacks or natural disasters).[2] Similarly, the business respondents to the 2017 Allianz Risk Barometer survey ranked cyber incidents (cyber crime, IT failure, data breaches, etc.) third among top global business risks (up from 15th in 2013) and consistently among the top five risks across all regions (Allianz Global Corporate & Specialty, 2017). An estimated USD 9 trillion to USD 21 trillion of economic value creation globally between 2015 and 2022 could depend on the robustness of the cybersecurity environment (Bailey, Del Miglio and

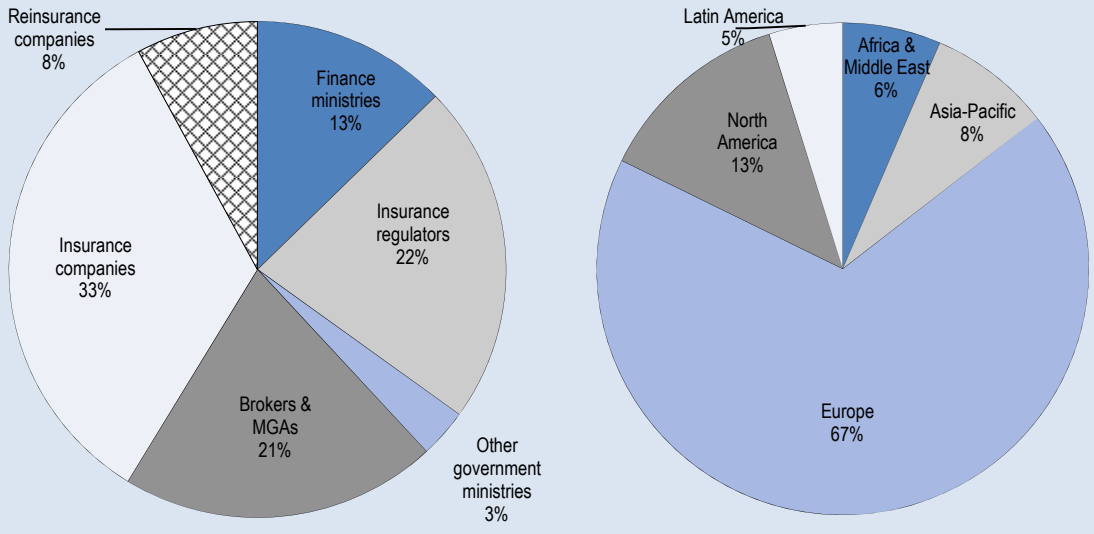
Richter, 2014). As a result, and in the context of the increasing digitalisation of business processes, growing policy attention is being invested in this issue as countries seek ways to build the resilience of both public and private networks against cyber security incidents.

The respondents to an OECD questionnaire on cyber risk insurance[3] generally perceive that their countries and its businesses face a moderate to high-level of risk from cyber incidents (where high risk indicates constant or imminent attack and/or high impact from cyber incidents). None of the respondents indicated that cyber incidents represented "no risk" to their countries. Among the respondents, the perception of the level of cyber risk is highest among insurance brokers and reinsurance companies and lowest among the government officials that responded to the questionnaire (see Figure 1.2).

Box 1.1. OECD questionnaire on cyber risk insurance

In 2016, the OECD circulated a questionnaire through its public and private sector networks seeking information about perceptions of cyber risks, the insurance coverage available for cyber risks, challenges to the extension of cyber insurance coverage and initiatives aimed at addressing those challenges. Responses were received from 58 public and private sector organisations from 32 countries, as described in Figure 1.1.

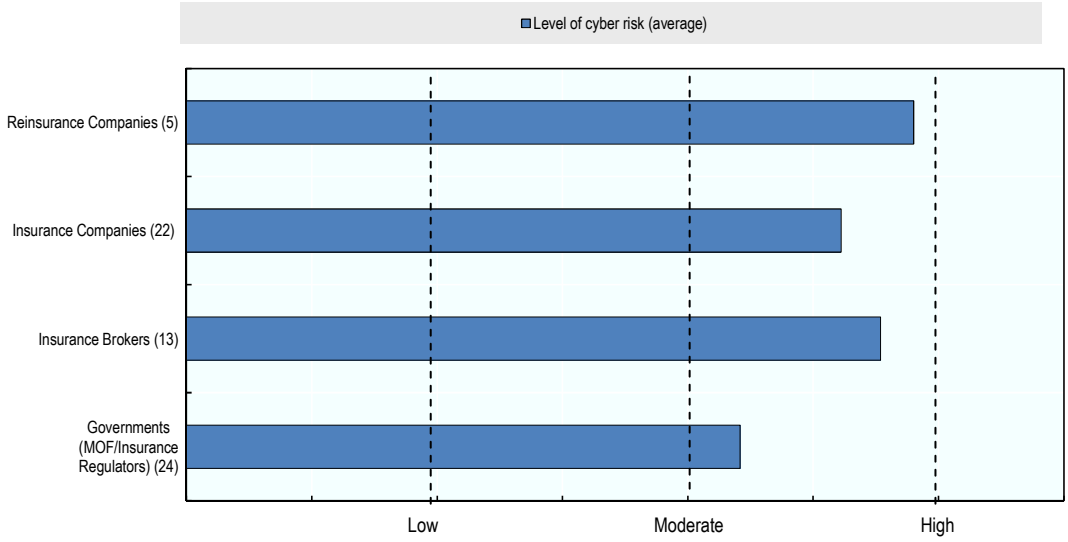
Figure 1.1. **Survey respondents by organisation type and region**



Close to 80% of survey respondents perceived that the frequency of cyber attacks had increased in recent years. This is consistent with the findings of most surveys on the frequency of cyber incidents and the share of companies that have been affected by such incidents. For example, the number of "information security incidents" reported by respondents to *The Global State of Information Security Survey* (a survey of approximately 10 000 companies from around the world) has increased by an average of 60% per year since 2009, although this likely includes both a real increase in incidents as well as improvements in incident detection (see Figure 1.3). A recent survey of business continuity professionals from 700 companies in close to 80 countries identified "cyber attacks" as the fourth most significant cause of business disruption (and "data breach" as the ninth most important source of disruption) (Business Continuity Institute, 2017).

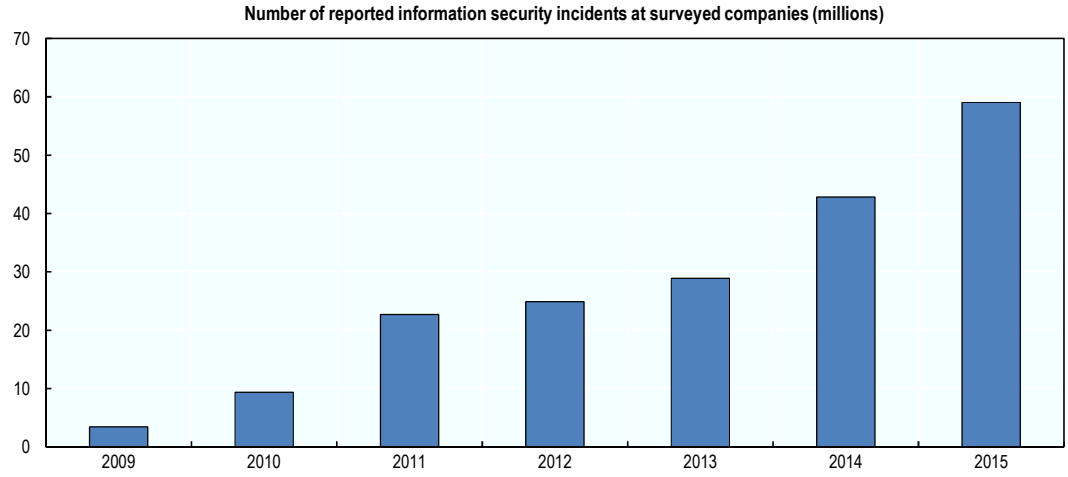
Another recent survey of 3 000 companies in the United States, Germany and the United Kingdom found that 63%, 56% and 45% of those surveyed, respectively, had faced a disruptive[4] attack in the previous 12 months (Hiscox, 2017).

Figure 1.2. **Perceptions of the level of cyber risk**



Source: OECD questionnaire on cyber risk insurance (2016).

Figure 1.3 **Increasing frequency of cyber incidents**



Source: PwC (2014). The data point for the year 2015 was calculated based on the growth rate reported in PwC (2015).

Almost 80% of survey respondents indicated that the severity of cyber attacks facing their countries had increased in recent years. Some of the increase may be due to the growing awareness of cyber incidents that has come with more frequent events and better disclosure. However, the scope and scale of a number of recent incidents, including the denial-of-service attack on Dyn (see Box 2.5), the data confidentiality breaches at Yahoo

and Equifax (see Table 2.2) and the global WannaCry and NotPetya ransomware attack (see Box 2.8), provide some evidence that the severity of cyber incidents could be increasing. This is consistent with predictions reported in McKinsey (2014) that cyber attackers will continue to increase their lead over corporate defences and that the level of sophistication of attacks would increase more quickly than institutions' ability to defend themselves.

While not a substitute for investing in cyber security (and therefore reducing the risk of being affected by an incident), insurance coverage for cyber risk provides a means for companies and individuals to transfer a portion of their financial exposure to insurance markets. Where providing significant levels of insurance coverage, insurance companies can also make an important contribution to the management of cyber risk by promoting risk awareness and encouraging measurement, supporting incident management and providing incentives for risk reduction:

- The process of seeking insurance coverage requires prospective policyholders to identify and quantify the exposures that they face in order to determine the amount of coverage that they require - a process that can also be beneficial for informing decisions on investments in cyber security. The insurance sector, including the insurance brokers that provide advice on coverage decisions, has significant expertise in risk quantification that can be beneficial for the quantification of cyber risk (CRO Forum, 2014; US Department of the Treasury, 2015). The insurance sector's efforts to improve cyber risk quantification are discussed in chapter 5.

- The underwriting process will usually involve the sharing of experience and expertise on the management of cyber risk among the prospective policyholder, broker, insurance company and/or other third party cyber security expert (depending on the scope and complexity of coverage being discussed) (UK Cabinet Office, 2014; Marsh, 2015; Lloyd's, 2016). For small amounts of coverage, this could include relatively standard security protections such as firewalls and anti-virus protections (which may be identified as conditions for coverage). For larger amounts of coverage, the underwriting process could involve more substantial information sharing on technological approaches to protection and security practices or even penetration testing and security audits as a means of identifying potential vulnerabilities. More information on approaches to underwriting cyber insurance coverage is provided in chapter 3.

- Many stand-alone cyber insurance products include access to service providers that can assist policyholders in responding to cyber incidents, including forensic investigators needed to assess the extent of intrusion, legal firms with knowledge of any relevant disclosure or notification requirements and public relations companies able to minimise the reputational impact of cyber incidents. Quick access to these experienced service providers can make an important contribution to reducing the overall level of losses, especially among companies with limited experience in - or capacity for - crisis management and business contingency planning (UK Cabinet Officer, 2014). More information on the additional services that are offered with cyber insurance policies is included in chapter 3.

- The pricing of insurance coverage could provide an incentive to reduce the risk to the extent that risk reduction investments may lead to reduced premiums. Similarly, the expected reduction in premiums resulting from investments in

protection could improve the cost efficiency of security spending and therefore the overall level of investment in cyber security (ENISA, 2012). While there are a number of challenges to pricing insurance coverage (including a number of unrelated factors, such as commercial conditions, that affect insurance pricing), there is some evidence that insurance companies are differentiating premiums based on the level of cyber security (Donlon, 2016) and that companies are investing in cyber security in order to benefit from lower insurance premiums (PwC, 2014). A discussion of cyber insurance pricing is included in chapter 3.

In this context, the OECD's Insurance and Private Pensions Committee held a roundtable on the cyber insurance market at its December 2014 meeting, and, as a result of significant interest in the issue, launched a project on cyber insurance[5]. This report consolidates the findings across the three related components of the project: (i) the cyber insurance market and nature of available coverage; (ii) the role of insurance in supporting cyber resilience; and (iii) regulatory and policy initiatives to support the development of cyber insurance markets.

Notes

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

2. In 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." The inclusion of either of these risks among the top risks was considered to be an inclusion of "cyber risk" among the top risks faced by business.

3. Responses to the questionnaire were received from the governments of Austria, Chile, Colombia, Costa Rica, Estonia, Finland, France, Germany, Hungary, Iceland, Israel, Italy, Japan, Latvia, Luxembourg, Mexico, Poland, Portugal, Russia, Slovak Republic, Sweden, Chinese Taipei, Turkey and the United States. In terms of insurance brokers, managing general agents and their associations, responses were received from the following organisations: A&I Member Services (Australia), Arthur J. Gallagher (Australia), BFL Canada Risk & Insurance, Burns & Wilcox (United States), Collegiate Management Services (United Kingdom), CGSC (United Kingdom), Managing General Agents' Association (United Kingdom), Marsh (Europe), Miller Insurance Services (United Kingdom), Price, Forbes & Partners (United Kingdom), SEIB Insurance Brokers (United Kingdom), The Council of Insurance Agents & Brokers (United States) and Willis Towers Watson (United Kingdom). In terms of insurance companies and their associations, responses were received from the following organisations: AIG (United States), Allianz Global Corporate & Specialty (Germany), Aviva (Canada), AXA (France), AXA (Italy), BTA Baltic Insurance Company (Latvia), CFC Underwriting (United Kingdom), Delta Insurance (New Zealand), ERGO Insurance (Latvia), Global Federation of Insurance Associations, Hollard Specialist Liabilities (South Africa), International Underwriting Association, Lloyd's (United Kingdom), QBE Europe (United Kingdom), SHA (South Africa), Telesure (South Africa), Zurich (Switzerland), an

anonymous insurance company from Belgium and three anonymous insurance companies from Ireland. Responses were received from five reinsurance companies: General Re (United States), JLT Re (United Kingdom), Munich Re (Germany), Partner Re (Switzerland), and Scor (France).

4. While this study does not provide a definition of a disruptive incident, at least 82% of the responding companies reported that it took one hour or longer to recover to business as usual.

5. More information on the project is available at: www.oecd.org/finance/insurance/cyber-risk-insurance.htm

References

Allianz Global Corporate & Specialty (2017), *Allianz Risk Barometer: Top Business Risks 2017*, Allianz Global Corporate & Specialty SE, Munich.

Bailey, T., Del Miglio, A. and W. Richter (2014), "The rising strategic risks of cyberattacks", *McKinsey Quaterly (May)*, McKinsey & Company, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rising-strategic-risks-of-cyberattacks.

Business Continuity Institute (2017), *Horizon Scan Report 2017*, Business Continuity Institute, Caversham (United Kingdom).

CRO Forum (2014), *Cyber resilience: The cyber risk challenge and the role of insurance*, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

Donlon, R. (2016), "Panel looks at the role of insurance in the age of cyber threats", *Property Casualty 360°*, 28 September, www.propertycasualty360.com/2016/09/28/panel-looks-at-the-role-of-insurance-in-the-age-of.

ENISA (2012), *Incentives and barriers of the cyber insurance market in Europe*, European Network and Information Security Agency, Heraklion (Greece).

Hiscox (2017), *The Hiscox Cyber Readiness Report 2017*, Hiscox, London.

Lloyd's (2016), *Lloyd's Cyber-Attack Strategy*, Lloyd's, London.

Marsh (2015), *UK Cyber Security: The role of insurance in managing and mitigating the risk*, Marsh LLC, Marsh.

OECD (2016), "Enabling the Next Production Revolution; The Future of Manufacturing and Services", Interim Report, Meeting of the OECD Council at Ministerial Level, 1-2 June 2016, Paris, www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-andservices-interim-report.pdf.

PwC (2014), *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015*, PwC, www.pwccn.com/home/eng/rcs_info_security_2015.html.

PwC (2015), *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey 2016*, PwC, www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

UK Cabinet Office (2014), *Joint government and industry statement on the cyber insurance market*, 5 November, www.gov.uk/government/publications/cyber-insurance-market-joint-government-and-industry-statement.

US Department of the Treasury (2015), *Remarks by Deputy Secretary Sarah Bloom Raskin at The Center For Strategic And International Studies Strategic Technologies Program (as prepared for delivery)*, 10 September, www.treasury.gov/press-center/press-releases/Pages/jl0158.aspx.

World Economic Forum (2017), *Global Risks Report 2017*, World Economic Forum, http://reports.weforum.org/global-risks-2017/.

Chapter 2

Types of cyber incidents and losses

This chapter provides an overview of the different types of cyber incidents, based on a categorisation approach developed by the CRO Forum, as well as the types of losses that may result from these incidents. Where available, data is presented on the magnitude of losses from past incidents including trends in the magnitude of losses and some of the drivers of cost variations across different countries (such as differences in terms of notification requirements).

There is significant literature on the nature and evolution of cyber risk as well as the magnitude of potential costs - although limited consensus in terms of definitions, categorisation or the reliability of the data that has been made available on the frequency and impact of cyber incidents. For example, there is no prevailing definition of cyber risk or prevailing taxonomy for categorisation of different types of incidents and losses.

Much of the data that is publicly available on cyber incidents and costs is provided by security and consulting firms and is perceived by some as potentially biased due to the commercial incentives that these firms may have to inflate the significance of cyber risk. For example, Romanosky (2016), using data collected mostly by Advisen, questions a number of commonly cited statistics and trends including the typical cost of a third party confidentiality breach, the share of companies that have been impacted by cyber incidents and the rise in the relative share of incidents that are malicious relative to accidental.

Conversely, the lack of reporting of cyber incidents by affected companies (particularly certain types of cyber incidents) have led some to suggest that the publicly available data underestimates the true significance of cyber risk. In the United Kingdom, for example, a recent survey found that only 26% of respondents had reported their most serious breach incident to an external party (of which only 19% of those that reported their most serious breach incident reported it to police and only 8% to customers) (Department for Culture, Media and Sport, 2017). Other estimates suggest that 60% to 89% of incidents are likely to be unreported (Edwards et al., 2014). While it is difficult to know which tendency may be stronger - it is clear that "existing cost estimates are far from perfect" (The Geneva Association, 2016).

A description of the main categories of incidents and losses, based on definitions and a taxonomy developed by the insurance sector, is included in Box 2.1. This is followed by a description of the types of incidents that could be included under each category and some illustrative examples and data, where available (which are also summarised in

Figure 2.6 at the end of this chapter). The purpose of this overview is to provide context for the subsequent sections of the report and support a better understanding of the range of potential incidents and how these incidents can translate into costs that can be transferred to insurance markets. It should not be interpreted as providing a comprehensive taxonomy of cyber incidents or a measure of the impacts of cyber incidents (which are beyond the scope of this report).

Box 2.1. Definitions and categorisation of cyber incidents and losses

Definition of cyber risk

Neither a standard definition of cyber risk nor a common definition used broadly within the insurance sector currently exist. A couple of definitions have been put forward by associations of insurance companies:

- A group of insurance company Chief Risk Officers (CRO Forum, 2014) has defined cyber risk as encompassing: "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks".
- The Geneva Association (2016), an international insurance think tank whose members include large insurance and reinsurance companies, has suggested a similar definition: "any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services."

Both of these definitions broadly define cyber risk to include risks related to the use of information and communications technologies, which could include both risks related to human error as well as intentional/malicious attacks, whether generated by internal or external parties (nation states, terrorists, industrial competitors, organised crime, hacktivists or lone hackers/criminals). The Geneva Association (2016) definition usefully narrows the scope of cyber risk to incidents that lead to a ***compromise of data or service***, which captures the types of incidents that are normally considered as within the potential scope of cyber insurance coverage.

Types of cyber incidents

There are a number of different possible approaches to categorising the different types of incidents. For the purposes of this study, the categorisation developed by the CRO Forum (2016) is used which includes four broad categories: (i) data confidentiality [breach]; (ii) system malfunction/issue; (ii) data integrity/availability; and (iv) malicious activity. These categories are described[1] in the sections below, including examples of real-life (where existing) or hypothetical scenarios as well as any available data on the frequency or impacts of incidents for each category. It should be noted that the CRO Forum (2016) taxonomy is evolving based on an evaluation of an ongoing incident reporting exercise (see Chapter 5) and an effort to incorporate metrics commonly used for threat and security incident reporting ("VERIS" and "STIX").

Types of cyber losses

Cyber incidents can potentially lead to a number of different types of losses, including damages to tangible and intangible assets, losses related to business disruption and theft, as well as various forms of liability to customers, suppliers, employees and shareholders (amongst others). The CRO Forum (2016) has developed a set of "incident type groups" that provides a useful categorisation of the different types of losses that could be incurred as a result of cyber incidents. The categories of losses put forward by the CRO Forum are described in Table 2.1.

Table 2.1. **CRO Forum Incident Types**

CRO Forum (2016) "Incident Type Group" (loss types)	CRO Forum (2016) "Coverage Scope"
Business interruption Interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage.
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.
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.

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.
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).
Intellectual property theft	Loss of value of an intellectual property asset, resulting in pure financial loss.
Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defence costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences 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.
Breach of privacy [compensation]	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs.
Network security/security failure [liability]	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.
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.
Regulatory & legal defence costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company or 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 defence costs: coverage for own defence costs incurred to the observed company or related third parties facing legal action in courts following a cyber attack.
Fine 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.
Communication and media [liability]	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.
Legal protection - Lawyer fees	Costs of legal action brought by or against the policyholder including lawyer fees and costs in case of trial (e.g. identity theft, lawyer costs to prove the misuse of victim's identity).
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.
Products [liability]	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 (Technology errors and omissions) and excluding Professional Services errors and omissions).
Directors and officers (D&O) [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.
Technology errors and omissions (E&O) [liability]	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber event.
Professional services errors and omissions (E&O)/Professional indemnity [liability]	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber event, excluding technical services and products (Technology errors and omissions).
Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber event.
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.
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. sensitive data leakage leading to suicide).

Note: The classification described in this report involves an interpretation of the CRO Forum categorisation which may not reflect what was intended by those that designed the classification.

Source: CRO Forum (2016)

Data confidentiality

Incidents involving the compromise of confidential data (also commonly referred to as "data breaches") are among the most common forms of cyber incidents. The CRO Forum (2016) classification sub-divides data confidentiality incidents into two types: (i) incidents involving own confidential data (e.g. financial data, trade secrets, intellectual property); and (ii) incidents involving third party confidential data (e.g. customers' personal information). Usefully, the classification of an incident in this category is based on the detection by a company of the confidential data "outside of its data perimeter" rather than the specific incident that led to the unauthorised release of data. This means that the scope of this category includes the many different underlying causes of the release of confidential data, ranging from improper disposal of company records to unauthorised access to a company's internal networks (often referred to as a "network security breach").

The release of confidential data through employee error (e.g. through the loss or improper disposal of a portable device containing confidential data) has historically been the most common form of data confidentiality incidents (and still accounted for 25% of all "data breaches" in 2016 according to some sources (Ponemon Institute, 2017)).

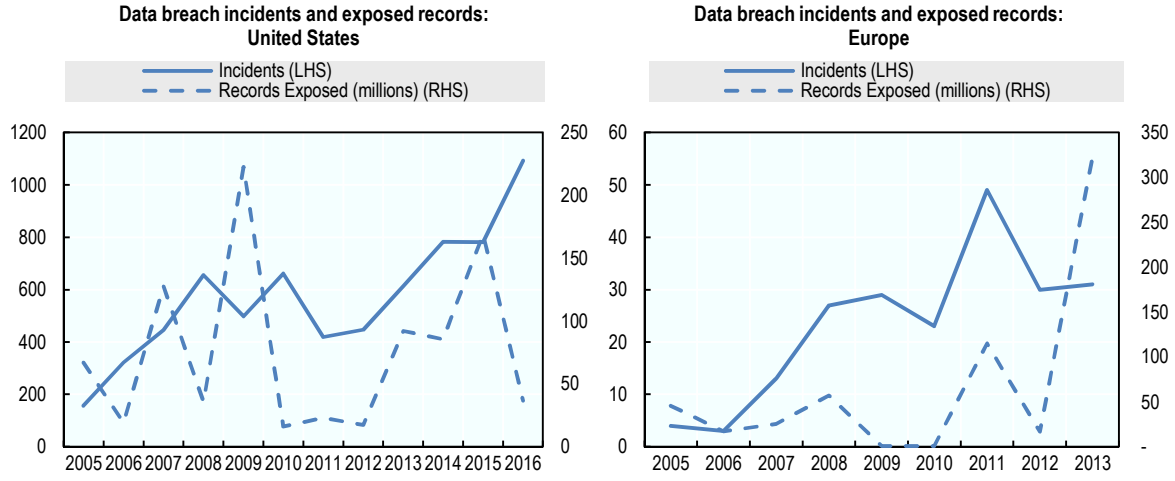
However, incidents caused by malicious attacks have accounted for an increasing share of data confidentiality incidents, particularly as encryption of portable devices has become more common (reducing the risk of confidential data releases from lost portable devices and therefore the share of all incidents involving employee error) (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). Malicious attacks aimed at compromising data confidentiality would normally be motivated by financial gain (e.g. the sale of personally-identifiable information or the sale and/or exploitation of trade secrets) but could also be driven by political or social motivations, such as the desire to harm a company (e.g. the data confidentiality breaches at Ashley Madison and Sony Pictures) or political party (e.g. the data confidentiality breaches that affected the United States' Democratic National Committee and Emmanuel Macron's presidential campaign in France).

Third-party data confidentiality breaches

Most publicly reported breaches of data confidentiality have involved the loss or theft of third party data, and particularly personally-identifiable information (Gemalto NV, 2016). A data confidentiality incident involving third-party personal data is more likely to be reported than other types of data confidentiality incidents due to the notification requirements imposed in many jurisdictions related to the release of personal information (see Box 2.2). However, the availability of data (particularly comparable data) on data confidentiality incidents remains limited (even in countries with notification requirements) - resulting in uncertainty even in terms of whether the number of such incidents is increasing or remaining stable. Some reports have found a general upward trend in the number of reported incidents and the records exposed (see Figure 2.1) although there are other reports of a decline in such incidents in recent years (particularly serious incidents) - potentially attributable to the implementation of effective prevention measures and/or the declining black market value for some types of personally-identifiable information[1] (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). One recent analysis found a measurable decline in the frequency of smaller (less than 100 000 records) data confidentiality breaches and a small decline in the frequency of larger incidents (for 2016 only) (Risk Management Solutions, Inc. and

Cambridge Centre for Risk Studies, 2016). However, for respondents to the OECD questionnaire, the existence of a black market for this type of information remains one of the most important factors driving the overall level of cyber risk.

Figure 2.1. **Third party data confidentiality breach incidents and exposed records**



Source: Data for the United States is from Identity Theft Resource Center (2016), accessed from Statista on 20 February 2017 (www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/). The Identity Theft Resource Center defines a "data breach" as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure, either electronically or in paper format." The data for Europe is from Howard and Gulyas (2014) who define a "data breach" incident as an "incident involving the loss or exposure of digital personal records".

Third party data confidentiality incidents involving the loss or theft of personally-identifiable information are most common in sectors that collect such information, such as health care, financial services, educational institutions, retail and the public sector (Identity Theft Resource Center, 2016; Howard and Gulyas, 2014) although there has been a significant recent decline in the frequency of incidents in the financial services sector, potentially as a result of increasing investment in security and data protection (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). A particular target are companies that process debit and credit card payments through point-of-sale (POS) terminals that collect and transmit details on payment cards and PIN codes. Healthcare providers were also becoming an increasingly significant target due to an increase in the black market value of health care records relative to other types of records. However, there has been a recent shift in the types of incidents affecting health care organisations away from data confidentiality breaches towards cyber extortion (such as the recent WannaCry ransomware attack in May 2017 which widely affected the United Kingdom's National Health System - see Box 2.8) .

Box 2.2. **Notification and disclosure requirements and related fines and penalties**

Data confidentiality breaches involving unauthorised access to personally-identifiable information may be subject to notification and/or disclosure requirements (either to a regulator or to those affected) and fines and penalties in several countries:

- In the **United States**, there are prompt notification requirements established at the state-level in all but three states as well as federal privacy requirements that require notification (to regulators and affected individuals) if health or financial information is stolen (*Health Insurance Portability and Accountability Act* and *Graham-Leach-Bliley Act*, respectively). The requirements in 36 states as well as the federal requirements related to health information allow for the respective authorities to impose penalties on organisations for the release of that information. In addition, regulatory actions can be brought by a number of federal and state agencies, including the Federal Trade Commission and state Attorney Generals (Allianz Global Corporate & Specialty, 2015). The US Securities and Exchange Commission (SEC) requires disclosure by public companies of cyber incidents, where an incident is "reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition" and where an incident is likely to "materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions" (SEC, 2011). Data breach incidents could be included within the scope of this disclosure requirement although a number of significant breaches have not been disclosed by public companies (Tsukayama, 2016).
- In the **European Union**, notification requirements are currently less prevalent although there are potential notification requirements in some sectors. The *Payment Services Directive 2*, for example, allows for the possibility of public ("payment service user") notification in cases where "an incident has or may have an impact on the financial interests of its payment service users". There are also notification requirements related to incidents that are operationally disruptive to critical services (see the section below on system malfunction). This will change as a result of the General Data Protection Regulation (GDPR) (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data*) which will come into effect in May 2018 and will include more generalised notification requirements. The GDPR will require prompt notification to the supervisor in cases where there is a risk to the "rights and freedoms of data subjects" (and to affected individuals if there is a high-risk) and will impose administrative fines in the case of breaches that are deemed intentional or involving negligence (Steptoe and Johnson LLP, 2016).
- In **Australia**, **Canada** and **Japan** fines may be imposed although only in the context of non-cooperation with an investigation or non-compliance with a specific order (BakerHostetler, 2015) (although, in Australia, changes to privacy legislation will lead to broad notification requirements and the potential for penalties of up to AUD 1.8 million for "serious or repeated interferences with the privacy of an individual" to be imposed by federal courts (Lui, 2017)). In Japan, financial sector businesses are required to notify the supervisory authority of data breaches while companies in other sectors may be required to notify supervisory authorities, depending on the nature of the data breach, the type of data involved and the number of data subjects affected, along with other relevant factors. In **Singapore**, the *Personal Data Protection Act* introduced requirements for the protection of personal data that is collected and fines of up to SGD 1 million can be imposed (Allianz Global Corporate & Specialty, 2015). An amendment to the **Republic of Korea**'s *Personal Information Protection Act* allows for fines of up to KRW 100 million (and a prison sentence of up to ten years) (PwC, 2016). **Mexico** also imposes monetary penalties related to violations of the *Ley Federal de Protección de Datos Personales en Posesión de Particulares* (Federal Law on the Protection of Personal Data held by Private Parties).

Data confidentiality breaches involving third party (personal) data can lead to different types of losses, including (in particular) data and software losses, incident response costs, breach of privacy compensation, reputational damage, regulatory and legal defence costs, fines and penalties, legal protection - lawyer fees and directors and officers (D&O) liability. In its *2017 Cost of Data Breach Study* (based on estimates from the 419 companies that participated in its annual survey), the Ponemon Institute (2017) estimates that the average total cost (excluding breach of privacy compensation) of a data breach incident (defined as a breach which puts an individual's name and either a health or financial record at risk; i.e. a third party data confidentiality breach) to a company was USD 3.62 million (down from USD 4.0 million in 2016). This is generally consistent with the findings of a 2015 annual survey of companies in the United Kingdom which estimated that the cost of addressing the worst breaches impacting large companies ranged fromGBP 1.5 million toGBP 3.14 million (Department for Business, Innovation and Skills, 2015) and with estimates by Verizon of an average cost range of between USD 5 million and USD 15.6 million for large privacy breaches (100 million records or more) (Verizon, 2015). The average cost of data breaches varies significantly across countries, ranging from USD 1.52 million to USD 1.68 million in India and Brazil to USD 4.31 million in Canada and USD 7.35 million in the United States (as cost is significantly affected by notification requirements, penalties and compensation practices, as described below) (Ponemon Institute, 2017).

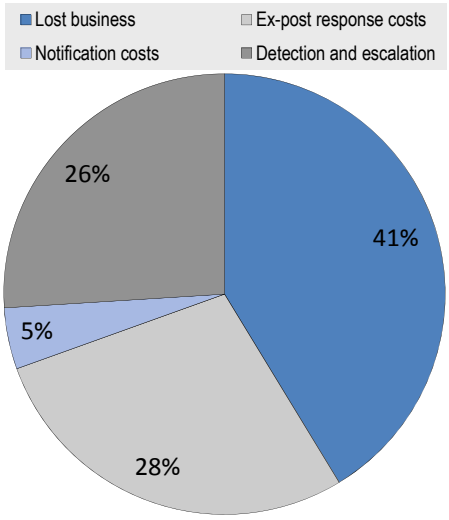
The limited available data on cyber insurance claims identifies an average cost (i.e. sum of claims paid and self-insured retention) of USD 650 000 to USD 675 000, although with higher average costs in certain sectors such as retail, health care and financial services and among large companies (USD 4.8 million to USD 5.9 million for companies with USD 10 billion to USD 100 billion in revenues) (NetDiligence, 2015; NetDiligence, 2016).

An important driver of the differences in cost across countries and sectors is differences in the legal frameworks related to privacy protection. As an illustration of this, data breach claims incidents account for close to 90% of all insurance claims in the United States (NetDiligence, 2015; NetDiligence, 2016) where notification requirements are widespread but were found to account for less than 25% in Europe (AIG, 2016). The major components of the costs of a third party data confidentiality breach across jurisdictions are:

- *Fines and penalties:* As noted in Box 2.2, a number of jurisdictions may impose fines and penalties as a result of a data confidentiality breach involving personally-identifiable information. The magnitude of these fines varies by jurisdiction and sector. In the United States, organisations affected by a data confidentiality breach involving health records have been fined as much as USD 5.5 million (Department of Health and Human Services, 2017). In Europe, the scope of potential fines and penalties currently varies across member states. For example, in the United Kingdom, the Information Commissioner's Office can issue fines for up toGBP 500 000 (Information Commissioner’s Office, 2015). The GDPR, effective in May 2018, will allow for fines of up to EUR 20 million or 4% of worldwide annual turnover (whichever is greater) and will apply to all entities that process personal data of EU citizens.
- *Incident response costs:* In some jurisdictions (notably, the United States), individuals affected by a data confidentiality breach must be notified that their personal information has been compromised, particularly when there is a risk that

the release of that information could cause harm. Notifying individuals can be costly (on average, 5% of total costs - see Figure 2.2), especially in the case of breaches that affect large numbers of individuals. In addition, affected organisations are likely to incur public relations and communications costs once the data confidentiality breach is made public. An analysis of the breakdown of costs related to data confidentiality breach claims in the United States found that 75% (USD 375 000, on average) of costs incurred were related to "crisis services" including forensic investigations, notification costs, public relations (as well as credit/identity theft monitoring which is classified in this study as breach of privacy compensation) (NetDiligence, 2016). A report by a legal firm that supports US companies in responding to third party data confidentiality breaches found that a forensic investigation was undertaken in approximately one third of incidents at an average cost of USD 102 806 (BakerHostetler, 2016).

Figure 2.2. **Breakdown of data confidentiality breach costs by type (2015)**



Source: Ponemon Institute (2015). Losses resulting from a data confidentiality breach are classified in the study as: (i) "Ex-post response costs" which includes some components of breach of privacy compensation costs (credit-watch services) and incident response costs (public relations and communications costs and remediation costs) as well as regulatory and legal defence costs and fines and penalties; (ii) "notification costs" which include incident response costs related to informing customers that their information has been compromised; (iii) "lost business" which includes both the disruption to business that directly results from responding to the event (i.e. business interruption) as well as the loss in revenue resulting from reputational damage after the event; and (iv) "detection and escalation" which includes the IT investigations and forensic analysis component of incident response costs. Large breaches (involving more than 101 000 compromised records) are excluded from the scope of the study.

- *Reputational damage*: Where data confidentiality breaches are made public, affected organisations may face a loss of profits due to a loss of confidence in the company among its customers (see Box 2.3). The Ponemon Institute (2015) found that, on average, the most significant costs for organisations affected by data confidentiality breaches are due to lost business (abnormal customer turnover, increased customer acquisition costs, reputation losses). However, there is some evidence that the reputational impacts of a data confidentiality breach may be declining (or may be lower than expected). An analysis by PCS (an insurance claims data provider) of 12 major US data confidentiality breaches found that companies did not always face a share price decline after the disclosure of an

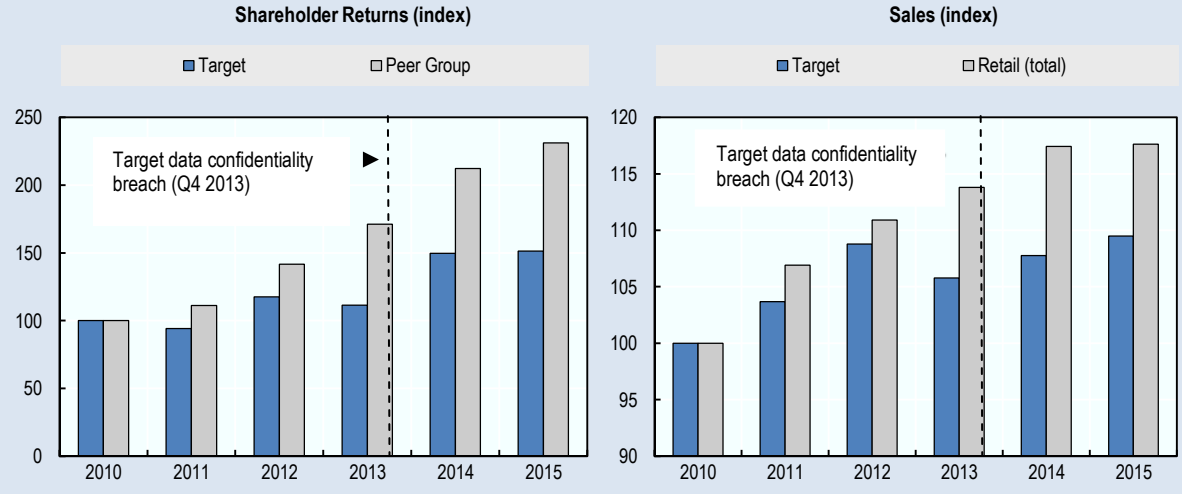
incident and that the impact on share prices have declined over time (Artemis, 2017). A 2014 study on consumer responses to companies affected by data confidentiality breaches found that 44% of respondents would end or reduce their business relationship with a company affected by a data confidentiality breach (where informed by media coverage) although 71% of those actually affected by an incident maintained their business relationship with the affected company, mainly because of a lack of alternatives or the perception that most companies are affected by such incidents (Ponemon Institute, 2014).

Box 2.3. The implications of lost business: Target data confidentiality breach

In the fourth quarter of 2013, Target, a major US retailer, discovered a significant data confidentiality 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 2017, the company had reported USD 292 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). In May 2017, the company reached a USD 18.5 million settlement with numerous US State Attorneys General that had launched investigations into the breach (Hurtado, 2017).

While the direct expenses incurred were significant, the company also faced an initial decline in sales and shareholder returns in the aftermath of its data breach disclosure. Subsequent growth in sales and shareholder returns also lagged behind the performance of its peers, suggesting that the company may have faced longer-term reputational damage as a result of the incident (see Figure 2.3).

Figure 2.3. **The business impact of a major data confidentiality breach**



Source: Target Corporation (2014 and 2016); US Census Bureau (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).

- *Breach of privacy compensation:* Individuals (and organisations) whose information has been affected by a data confidentiality breach may seek compensation from the organisation that was breached, usually based on a contractual obligation of the company to protect that data (either explicit or implicit) (Alder, 2015). Some privacy and data protection legislation may also explicitly establish (or reaffirm and/or define) private rights of action to seek

compensation (e.g. European Union member states through the GDPR, some Canadian provinces). With the implementation of the GDPR, companies operating in Europe will be liable for breaches of confidential data for which they have responsibility, even if the source of the breach was a third party. There is a strong expectation among consumers that companies will provide some compensation if the personal data that they have collected is compromised. A 2014 study found that between 58% and 67% of respondents in the United States expected some combination of monetary or in-kind compensation, identity theft insurance or credit monitoring services from a company affected by an incident (Ponemon, 2014) and many companies will provide this type of compensation or services.[2]

The most common forms of compensation provided by companies to those affected by data confidentiality breaches are credit monitoring services and identity theft protection.[3] In many cases, those affected by a data confidentiality breach will also seek monetary compensation although this would normally require a demonstration that they have been harmed as a result of the breach (e.g. that their identity has been stolen and their credit or reputation has been negatively affected as a result).[4] In practice, breached companies and/or their insurers have reached settlements with affected consumers in order to avoid a costly legal process with an uncertain outcome, particularly in jurisdictions where collective redress actions are permitted.

In the United States and Canada, individuals affected by a release of their personal information may cooperate through a class action lawsuit to seek compensation (although class action lawsuits have been less successful in Canada due to more stringent requirements and because the right of action only arises after a full investigation by the Privacy Commissioner (BakerHostetler, 2015)). According to an analysis of third party data confidentiality breaches by a legal firm providing response services in the United States, litigation resulted from only 6% of all incidents involving the company's response services (BakerHostetler, 2016) while available claims data found that legal settlements accounted for approximately 10% of costs incurred (with legal defence accounting for a further 3%) (NetDiligence, 2016). Where class actions have been pursued, the average settlements ranged from USD 0 to USD 13.63 per person with a tendency towards higher amounts for breaches involving personal health information, lower numbers of claimants and fewer non-cash benefits (such as identity theft monitoring) (Phillips et. al, 2017). However, there have been a number of cases where settlements (or amounts sought) have been outside that range, including:

- the theft of 45 million payment card records from TJ Maxx (a US retailer) in 2007 led to reported settlements with customers of USD 11 million (equivalent to approximately USD 30 per claimant with evidence of documented losses) (Insurance Information Institute, 2014);
- a 2013 lawsuit related to the theft of medical records sought damages of USD 1 000 and 10 000 per person under health privacy legislation in California (Aschkenasy, 2013); and
- in a recently settled class action suit related to the breach of data at Anthem, an alternative settlement of USD 50 per person was agreed to for individuals who did not want to enrol in the services offered as part of the settlement (MacLean, 2017).

Consumer class actions are less common (and more restricted) in the United Kingdom and continental Europe. In continental Europe, consumer class actions (collective redress) are possible although affected consumers can only be represented by a qualifying non-profit consumer association (rather than a fee-earning law firm as in the United States and Canada). In addition, in some European members states (e.g. France and Germany), collective redress actions related to data protection will only allow injunctive relief (i.e. corrective action), not compensation for damages (Swiss Re, 2017). The GDPR will leave it to member states to determine whether to maintain these restrictions or allow for compensation for damage awards. In the United Kingdom, collective redress actions are not restricted to consumer associations and it is possible to seek compensation for damages suffered (i.e. not just injunctive relief). A 2015 Court of Appeal ruling allows individuals to bring claims for distress without having to demonstrate that a financial loss has occurred (De Freltas, 2016). A June 2016 settlement awardedGBP 2 500 toGBP 12 500 per person to asylum seekers whose personal information was released (Swiss Re, 2017).

In the particular case of data confidentiality breaches involving payment card details, specific (contractual) penalties may be imposed by the operators of payment card networks on the basis of contractual obligations where non-compliance with the requirements of the Payment Card Industry Data Security Standard[5] was a causal factor (Goodman, 2016). Fines for non-compliance with the standard range from USD 5 000 to USD 50 000 (BakerHosteler, 2016). In addition, an acquirer (retailer) that suffers a breach involving payment card information may face assessments (or legal action) by the entities that issued the payment cards (or the payment card networks acting on their behalf) to cover the costs of re-issuing cards and covering any losses due to fraudulent use of the affected payment cards. These costs can be substantial with one study finding costs that range from USD 7 to USD 65 per set of card information (with an average of USD 30) (BakerHosteler, 2016). For example, the theft of 1.5 million payment card records from Global Payments Inc. in 2012 led to USD 35.9 million in fraud losses, fines and other charges (i.e. fines and assessments) expected to be imposed by the payment card networks (Information Security Media Group, 2013). The massive breach of payment card information (up to 100 million cards) at Heartland Payment Systems in 2007 led to over USD 100 million in assessments/settlements with the payment card networks (see Table 4.1). Target's assessment/settlement with Visa (on behalf of issuing financial institutions) was reported to be up to USD 67 million (Insurance Information Institute, 2014). According to a study of insurance claims paid in the United States, Payment Card Industry (PCI) fines and assessments were incurred in 5% of insured incidents and involved average insurance payouts of just under USD 500 000 and up to USD 3 million (NetDiligence, 2016).

The magnitude of losses from a data confidentiality breach also varies significantly by sector. Highly-regulated sectors (including sectors faced with specific notification requirements) incur higher costs per stolen record than less regulated sectors and the public sector (although this could also be due to better reporting of breaches in highly-regulated sectors). In 2016, the total reported cost per stolen record averaged USD 380 in the health sector, USD 245 in the financial sector and USD 200 in the education sector compared to USD 71 for records stolen from the public sector (Ponemon Institute, 2017). However, this figure varies substantially based on the country as well as the total size of

the data confidentiality breach. Breaches above 101 000 records are excluded from the Ponemon Institute estimates and would generally involve a lower cost per stolen record given that some costs are fixed (as low as USD 5 per record in some cases (Sclafane, 2015)). For example, the cost per stolen record of a breach involving more than 50 000 records is significantly less[6] than the cost per stolen record of a breach involving less than 10 000 records (Ponemon Institute, 2017). Some examples of the reported costs of selected data confidentiality breaches are provided in Table 2.2.

Table 2.2. **Costs of data confidentiality breaches: selected examples**

Incident	Description	Reported costs
Equifax	On 7 September 2017, Equifax, one of the largest credit reporting bureaus in the United States, reported that the names, addresses, social security numbers, birth dates and some driver license numbers of 143 million individuals in the United States (along with some personal information for residents of Canada and the United Kingdom) had been breached. In addition, credit card numbers for approximately 200 000 individuals were also accessed.	• In the five trading days following the disclosure, the company lost USD 3.5 billion in market value (Reuters, 2017) and the stock price remained 30% down at the end of September (Petterson, 2017). • The company is expected to face multiple state and federal investigations into the breach (Basak and Surane, 2017). In addition, at least 100 lawsuits had been filed including consumer class actions, a securities class action and also multiple lawsuits by municipal authorities (Reuters, 2017; Petterson, 2017). In many cases, the company was accused of violating its responsibility under the *Fair Credit Reporting Act* to keep the information it collects private. The company has agreed to provide credit monitoring services to all US consumers for a period of one year (the company is a provider of such services). The potential cost of settling the consumer lawsuits is estimated at USD 200 million (Petterson, 2017). The data confidentiality breach has also led to new regulatory proposals related to the protection of information by credit reporting bureaus (Insurance Journal, 2017a; Insurance Journal, 2017b). • Several senior executives (including the Chief Executive Officer) have resigned or taken early retirement and some reports suggest that a clawback of executive compensation is being considered (Advisen, 2017c; McCrank, Voltz and Mukherjee, 2017) • The company reportedly has USD 100 million to USD 150 million in stand-alone cyber insurance coverage (Basak and Surane, 2017).
Yahoo	In 2016, Yahoo disclosed two separate breaches involving approximately 1 billion and 500 million users in 2013 and 2014, respectively (with some accounts affected by both incidents). The incidents involved a breach of confidentiality of names, email addresses, telephone numbers, dates of birth as well as encrypted or partial information on passwords and security questions and answers. In October 2017, Yahoo reportedly increased its estimate of the number of users affected to 3 billion (all of its users at the time of the breach) (Harrison, 2017).	• A decline in the acquisition price of the company of USD 350 million relative to an offer made prior to the disclosure of the breaches (The Associated Press, 2017). • As of March 2017, the company had reportedly incurred USD 16 million in direct costs in response to the breaches (Goel, 2017) • Investigations with potential penalties have been launched by the Securities and Exchange Commission and the Federal Trade Commission (The Associated Press, 2017). • The company faces 43 consumer class action lawsuits as a result of the breaches (Goel, 2017). • A shareholder lawsuit was filed in January 2017 seeking compensation for the loss in share value (and loss in acquisition value) resulting from the data confidentiality breach (Lacroix, 2017). • The company's CEO did not receive a USD 2 million cash bonus or a share bonus with a USD 12 million approximate value (Goel, 2017).
TalkTalk	In October 2015, TalkTalk, a UK telecommunications company, disclosed that the personal information of more than 156 000 customers (names, addresses, dates of birth and contact information) had been breached. Among the affected customers, more than 15 000 also had their bank account information accessed.	• In its 2016 Annual Report, the company reported exceptional costs ofGBP 42 million attributable to the data breach, including direct incident response costs and customer management costs including additional call centre agents, communication and marketing costs, restoration with enhanced security features and increased retention costs including the cost of providing free upgrades. The company reported that the cost of credits to retain customers was approximatelyGBP 3 million (TalkTalk Group, 2016). • The company's pre-tax profits fell toGBP 14 million in the year ending

Incident	Description	Reported costs
		March 2016 relative toGBP 32 million in the previous period (Rodionova, 2016). Total revenue growth fell to 0.2% in the second half of fiscal year 2015 from 4.7% in the first half of the fiscal year, partly as a result of the data breach (TalkTalk Group, 2016). The company attributed a loss of 95 000 broadband customers to the data breach incident (TalkTalk Group, 2016) and may have lost 250 000 customers overall (IDT911, 2016). • Executive directors annual bonuses were reduced from 6.4% to 4.0% of base pay as a result of the data breach incident (TalkTalk Group, 2016) • The company was finedGBP 400 000 by the UK Information Commissioner's Office for failing to take appropriate measures to protect personal data (Rodionova, 2016). • There were reports that customer information was used in subsequent phishing attacks that led to the disclosure of banking details and the transfer of funds from their bank accounts. At least one law firm was examining whether there was cause for seeking compensation from the company on behalf of affected customers (Leigh Day, 2016).
Ashley Madison	In July 2015, a hacker group made a public claim that it had accessed confidential data on clients of Ashley Madison, a Canadian online dating website targeting people in relationships with others, and threatening to release the data unless the website was shut down. In August and September 2015, the hackers published names, usernames, encrypted passwords, addresses and phone numbers of 32 million Ashley Madison clients.	• The company was fined USD 17 million jointly by 13 US states and the US Federal Trade Commission (although paid USD 1.65 million due to an inability to pay the higher amount) (Larson, 2016). • The company reportedly lost a quarter of its revenue as customers ended their memberships (Rosenthal, 2016). • The company also reportedly faced a CAD 578 million lawsuit from its customers (Lord, 2016). It settled a US class action lawsuit involving approximately 37 million affected users for USD 11.2 million in July 2017 which provides users with up to USD 3 500 depending on documented losses (Stempel, 2017)
Anthem	In February 2015, Anthem (health insurance provider) disclosed that an unauthorised access had allowed hackers to obtain various types of personal information, including names, birthdays, health care identification/social security numbers, street addresses, email addresses, phone numbers and employment information, including income data. According to the company, there was no evidence that financial or health-related information was obtained. The incident reportedly affected 78.8 million "members" (i.e. insureds) and employees (Herman, 2016).	• The company reportedly spent USD 12 million initially on forensic investigation and remediation costs, including an assessment of needed cybersecurity enhancements. The company invested a further USD 130 million in 2015 and 2016 to improve its level of protection against cyber attacks (Advisen, 2017b). • The company indicated that they are providing credit monitoring and identity protection services to those affected (reportedly for two years) and that they have incurred expenses related to forensic investigation and remediation. • In its most recent Annual Report (Anthem Inc., 2017), the company indicated that there were ongoing investigations by various state and federal regulators that could lead to fines.. In June 2017, the company reportedly agreed to a USD 115 million settlement to resolve consumer claims from the breach (MacLean, 2017). • The company reportedly had USD 100 million in insurance coverage although reports suggest that this amount was unlikely to cover more than the cost of notification and credit monitoring (Osborne, 2015).
JP Morgan Chase	In September 2014, JP Morgan Chase (US bank) disclosed that the confidential information of 83 million clients (76 million individuals/households and 7 million small businesses) had been accessed, including names, addresses, phone numbers and email addresses (not usernames, passwords or financial information).	• The company indicated that it has increased its investment in cyber security defences from USD 250 million per year in 2014 to an expected USD 600 million per year in 2016 (JP Morgan Chase & Co., 2016). • Investigations by government agencies were reported although there is no indication that fines or penalties were imposed. • According to one report, credit monitoring services were not offered to affected customers (as only contact information had been breached and the company reported no increase in fraudulent activities) (Kerner, 2014b).
eBay	In May 2014, eBay (a US online retailer) disclosed a breach involving all of its 145 million users. The company's network was accessed by an unauthorised party using employee credential(s) and led to a breach of the confidentiality of username and encrypted passwords as well as	• The company reported reduced activity among its users and reduced its revenue projections for 2014 by USD 200 million after the disclosure of the breach (i.e. from USD 18.0 to USD 18.5 billion range after Q1 to USD 18.0 to USD 18.3 billion range after Q2) (Drinkwater, 2014).

Incident	Description	Reported costs
	complementary non-financial information (addresses, dates of birth).	• In its Q2 investor relations calls, the company reported a 1.9% decline in operating margin that was attributed to expenses related to the breach incident (and subsequent investments in network security improvements) (Kerner, 2014a). • As of 31 January 2017, eBay had received information requests from various regulatory and other government agencies although no payments of fines or penalties had been disclosed. A putative class action lawsuit had been filed against the company in July 2014 although was dismissed (with leave to amend) (eBay Inc., 2017).
Korea Credit Bureau	In January 2014, it was reported that a contractor working for the Korean Credit Bureau, a private organisation that manages credit information for financial institutions, had stolen 105.8 million personal information records from three issuing banks involving the confidential personal information of 20 million individuals. The stolen information, which included credit card numbers and validation dates, credit ratings, resident registration numbers, and contact details (but not passwords or personal identification numbers) was sold to marketing firms.	• A class action lawsuit was reportedly filed on behalf of 130 cardholders seeking KRW 110 million in compensation per victim (Lee, 2014). • Within the first two weeks after the disclosure of the breach, 2.28 million requests for cancellation and 3.84 requests for reissuance of the affected credit cards were made (Kim and Cha, 2014) • The Financial Supervisory Commission fined the three issuing banks whose cardholders were affected (KB Kookmin Bank, Lotte Card and NH Nonghyup Card) KRW 6 million each and banned them from issuing new credit cards for three months (Vaas, 2014).
Sony Play Station Network	In May 2011, Sony disclosed that some personally identifiable information from each of its 77 million Play Station Network (video game) user accounts had been breached, including usernames, passwords, email addresses, home addresses and some credit card information in encrypted form.	• The company provided USD 1 million in identity theft insurance protection for each user. In late May 2011, the company estimated that it would incur USD 171 million in costs for the identity theft programme and various promotional offers provided to customers in response to the breach (Hachman, 2011). • In 2012, a judge dismissed one of the US class action lawsuits filed on behalf of those affected (Kerr, 2012). Other lawsuits were filed in the United States and Canada (seeking CAD 1 billion in the Canadian lawsuit (Rose, 2011)). As of May 2015, the company reported that US class action suits had been settled (amounts were not disclosed) although a non-US lawsuit remained pending (Sony Corporation, 2015). • The UK Information Commissioner's Office fined the companyGBP 250 000 for security failures related to the incident (Halliday, 2013).
Heartland Payment Systems	In 2009, Heartland Payment Systems (US payments processor) disclosed that confidential payment card (debit and credit) information had been breached for up to 100 million cards issued by more than 650 financial services companies. The information that was accessed reportedly did not include unencrypted personal identification numbers or cardholder social security numbers or contact details (McGlasson, 2009)	• The company provided a detailed breakdown of many of the expenses that it incurred as a result of the data confidentiality breach in its 2010 Annual Report. The company incurred approximately USD 31.4 million in legal fees, investigative costs, remediation and crisis management services. The rest of the company's expenses (USD 114.7 million) were incurred for the settlement of claims/assessments, including USD 3.5 million to settle with American Express, USD 59.3 million with Visa and related parties, USD 34.8 million with MasterCard and USD 5.0 million with Discover (likely related to the cost of re-issuing cards and any fraudulent transactions resulting from the breach) (Heartland Payment Systems, 2011). USD 31.2 million was recovered through insurance. • The 2010 Annual Report also identified a number of ongoing class action lawsuits on behalf of cardholders and financial institutions. The company also faced a number of regulatory investigations and enquiries from a number of agencies in the United States and Canada. • The company's share price reportedly declined by 77.6% in the six weeks after the disclosure of the breach and remained 50% down almost six months after the breach relative to the price before the breach was announced (King, 2009). • Approximately 5 000 of the company's 250 000 merchant clients reportedly left in the weeks after the data confidentiality breach was disclosed (SecureWorks, 2012).

A data confidentiality breach of third party data could involve third party corporate (rather than personal) data, the release of which could be deemed defamatory, involve a copyright infringement or disclose third party trade secrets. In such cases, the company affected by the data confidentiality breach may be liable for compensating the third party whose information was disclosed. The CRO loss classification defines such losses as communications and media [liability].

First-party (own) data confidentiality breaches

There is more limited information on data confidentiality breaches involving unauthorised access to own data (e.g. trade secrets or financial data) as there are no (or limited) notification or disclosure requirements related to these types of incidents (with the exception of US Securities and Exchange Commission disclosure requirements which may apply in some instances). There are some estimates of the prevalence and impact of intellectual property theft. For example, in the United Kingdom, a survey of firms in 2015/2016 found that 1% of those surveyed had been affected by intellectual property theft in the previous 12 months (Department for Culture, Media & Sport, 2016) while an older report suggested that intellectual property thefts may account for one-third of the total estimated economic cost of cyber crime (Detica and Cabinet Office, 2011). In Europe more generally, a report by a cyber security firm found that, in 2016, 19% of all data that was exfiltrated as a result of malicious cyber incidents involved trade secrets (FireEye, 2017). An annual study on US insurance claims payments included one payment in 2016 for loss of trade secrets for an amount of USD 4.9 million and three payments in 2014 for amounts ranging from USD 150 000 to USD 900 000 (including self-insured retention) (NetDiligence, 2016).

These types of breaches are most commonly targeted at the public sector, manufacturing industries and professional services sector (Verizon, 2016). In December 2016, for example, ThyssenKrupp, a German industrial engineering conglomerate, disclosed that it had been the victim of a significant cyber attack that led to the theft of confidential business information from its steel production and manufacturing plant design divisions (Auchard and Käckenhoff, 2016). The value of the stolen trade secrets was not disclosed. A more recent target for intellectual property theft has been the media industry which has faced a number of ransom demands in recent months to prevent the early release of films and/or television episodes (Smith, 2017).

System malfunction/issue

The CRO Forum classification includes five sub-categories of system malfunction/issue: (i) own system malfunction; (ii) own system affected by malware; (iii) network communication malfunction; (iv) inadvertent disruption of third-party system; and (v) disruption of external digital infrastructure.

Own system malfunction/own system affected by malware/network communication malfunction

The CRO Forum classification identifies three categories of system malfunction/issue involving a company's own systems or software:[7] (i) own system malfunction (i.e. where a company's own systems create system errors, freeze completely or are otherwise rendered inoperable); (ii) own system affected by malware (i.e. where an intrusion of a company's systems is suspected due to the detection of malware or the abnormal behaviour of systems and software);[8] and (iii) network communication malfunction (i.e.

where a company's systems cannot communicate via the internet or other digital network). Two practical examples of own system malfunctions are a malfunction in a core business system (either due to human error or a malicious attack) and a denial-of-service attack. These types of own system malfunctions and the kinds of losses that may be generated are described below.

Companies depend on digital systems and software for a wide-range of corporate functions, from internal communications to payroll and financial reporting to control systems for the operation of machinery and equipment. A malfunction of any of these systems or software can lead to important consequences for business operations. For example:

- Business interruption/interruption of operations: An internal disruption to the provision of digital services, particularly a core digital service, could lead to an interruption of operations, extra expense and/or lost profits;
- Data and software loss: A malfunction of a system or software would likely lead to costs for restoring or replacing data and/or software;
- Product liability or professional services errors and omission (E&O) liability/professional indemnity: Depending on the nature of the companies' business, a system or software malfunction leading to a defect in the company's product or a failure to provide adequate professional services could lead to a liability claim or class action by its customers;
- Physical asset damage: If the system that malfunctions is involved in controlling the functioning of machinery or equipment (i.e. operational technology), damage to physical assets is possible (see Box 2.4). Damages to system hardware (whether or not as part of an operational technology failure) would also normally be considered physical asset damage.
- Technology errors and omissions (E&O) liability: If the system or software that malfunctions was acquired from a third party technical services provider, the provider may face a liability claim related to the malfunction.

There is very little information on the frequency or impact of systems malfunctions as notification and disclosure requirements are much more limited than in the case of third party data confidentiality breaches. In the European Union, under the *Network and Information Security Directive*, operators of "essential systems" must notify the competent authority or computer security incident response teams of "incidents having a significant impact on the continuity of the essential services they provide" with a possibility for public disclosure in certain circumstances (European Union, 2016). In addition, under the *Payment Services Directive*, payment services providers must notify the competent authority in the event of any major operational or security incident and payment system users (i.e. the public) where the incident "may have an impact on the financial interests of its payment service users" (European Union, 2015). In the United States, major operational incidents could be covered within the scope of the US Securities and Exchange Commission disclosure requirements.

A denial-of-service (DoS) (or distributed denial-of-service, DDoS if a network of computers is involved) attack could be considered as a form of system malfunction, specifically a network communications malfunction under the CRO classification. A DoS attack is aimed at bombarding a web server with traffic in order to disrupt its

functionality. There are various sources of data on the volume of DoS and DDoS attacks. According to one estimate, half of all major US corporations experienced a DoS attack in 2015 and one-in-eight of those attacks led to a disruption of website services (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). A survey of UK firms in 2016/2017 found that 8% of those surveyed had been affected by a DoS attack in the previous 12 months (relative to 15% in 2015/2016) (Department for Culture, Media & Sport, 2016; Department for Culture, Media & Sport, 2017).

Box 2.4. **Physical asset damage due to cyber attacks on operational technologies**

There is significant concern about the potential losses that could result from a cyber attack targeted at control systems, particularly control systems used in the operation of critical infrastructure such as electricity networks, water supply, or communication infrastructure. There is also some evidence of increased frequency of attacks on some critical infrastructure sectors, such as the energy sector. For example, the US Industrial Control System Cyber Emergency Response Team registered 303 reported incidents affecting industrial control systems in 2015 relative to 138 in 2012 (NCCIC/ICS-CERT, n.d.). A recent report found that, in 2016, 18% of all data that was exfiltrated as a result of malicious cyber incidents in Europe was data related to industrial control systems, building schematics and blueprints (FireEye, 2017).

There are a few documented examples[1] of cyber attacks that have led to physical damages, usually as the result of a malware infection that led to system malfunctions or allowed for the takeover of systems through remote access:

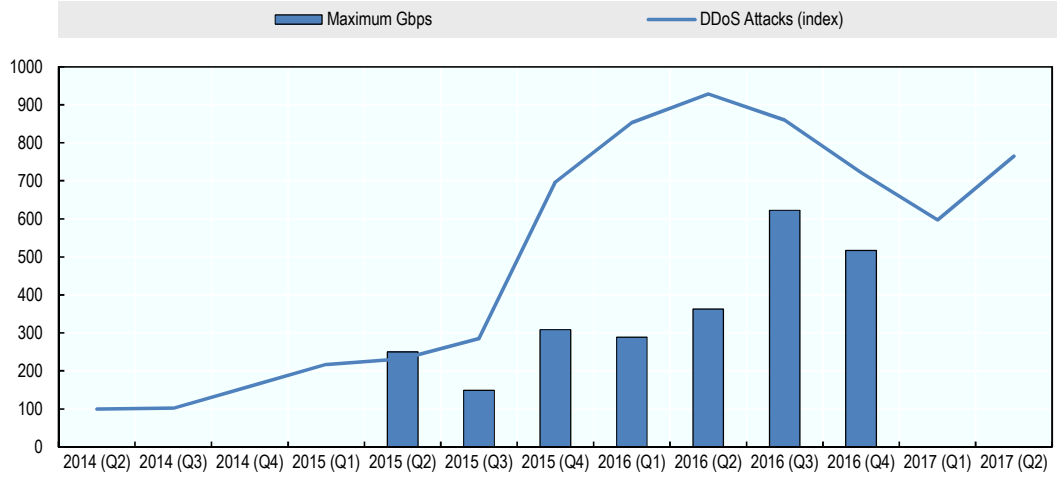
- In August 2008, an explosion occurred along a pipeline in Turkey which has been linked to a cyber attack that increased the pressure of the crude oil flowing through the pipeline while disabling the alarms and communications systems that would normally trigger a response to such an event (Robertson and Riley, 2014).
- In 2010, a computer worm (malware) aimed at sabotaging the operation of centrifuges used for uranium enrichment was discovered in the industrial control systems operating enrichment facilities in Iran. The worm reportedly led to damages to a number of the centrifuges (Kelley, 2013).
- In 2014, an unnamed steel mill in Germany was affected by a cyber attack that disabled the ability to shut down a blast furnace, leading to significant physical damages (Zetter, 2015).
- In 2015, a cyber attack against power distribution control centres in the Ukraine led to approximately 30 substations being taken offline and a loss of power to more than 230 000 residents for a period of one to six hours (Zetter, 2016).A further attack on a control centre that disabled capacity equivalent to about 20% of the city of Kiev's night time energy use was reported in December 2016 (Condliffe, 2016). It has since been reported that the malware used in the latter attack (known as "Crash Override" or "Industroyer") could also be effective in attacks against power grids in Europe and potentially the United States (Finkle, 2017)

Lloyd's (2015) has published an industrial control systems sabotage scenario (developed by the University of Cambridge Centre for Risk Studies) based on an electricity blackout affecting 15 states in the Northeastern United States (including New York City and Washington, D.C.). The scenario is based on a malware infection that causes electricity generators to overload and burn out leading to widespread short-term blackouts with rolling restoration of power over a number of weeks. While deemed improbable, the scenario is reported to be technologically feasible. The scenario estimates economic impacts ranging from USD 243 billion to more than USD 1 trillion and insured losses of USD 21.4 - USD 71.1 billion depending on the severity of the scenario (which, under the more extreme scenarios, involve insured losses that are higher than the most costly ever natural catastrophe - Hurricane Katrina). Insurance claims would be incurred across a number of business lines, including property damage and business interruption at power generation companies, property (cold storage) and business interruption losses at companies in the blackout area and contingent business interruption at companies with suppliers in the blackout area.

1. A series of fires at petrochemical plants and facilities in Iran between June and September 2016 have been reported as potentially caused by malware although this has not been publicly confirmed (Gambrell, 2016).

A specialty provider of DDoS mitigation services for large traffic customers publishes statistics on the number of DDoS attacks, the number of "mega-attacks" (i.e. attacks of over 100 Gbps (gigabytes per second)), average duration and the maximum traffic volumes against websites using its services. According to its estimates, there was an increase in the number of DDoS attacks by a factor of 7.5 between 2014 (Q2) and 2017 (Q2). The number of mega-attacks (i.e., attacks capable of disrupting a website with the infrastructure necessary for 1 billion visits per month (the top 100 global websites)) has been more variable on a quarterly basis (although the number of mega-attacks in 2016 was close to double the number of mega-attacks in 2014, before declining in 2017). The size of the largest attack per quarter has generally increased over time and reached over 600 Gbps for one incident in Q3 2016 (see Figure 2.4). The DDoS attacks on OVH in September 2016 and on Dyn in October 2016 (see Box 2.5) reportedly reached more than 1.0 Tbps (terabytes per second, or 1 000 Gbps) (Paganini, 2016; Woolf, 2016). The sectors that are most commonly targeted by DDoS attacks include government, gaming, software and technology, media and entertainment, internet and telecommunications and financial services (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Akamai, 2016d).

Figure 2.4. **Denial-of-Service attacks**



Source: Akamai State of the Internet - Security reports (2014a,b,c; 2015a,b,c,d; 2016a,b,c,d; 2017a,b). For the index on the number of incidents, 2014 (Q2) = 100 (or 530 incidents). Figures for 2014 (Q2 and Q3) were derived based on the growth rate in incidents published in subsequent reports. Information on the maximum attack size is not available before 2015 (Q2) or after 2016 (Q4).

The main losses from a DoS attack (for the company directly attacked) are likely to be due to business interruption/interruption of operations, including lost profits as well as extra expenses. The magnitude of losses will depend on the length of the disruption as well as the importance of the disrupted website in terms of the impacted company's business (and particularly its revenue generating impact, such as online sales and/or online advertising). Seasonal and time-of-day factors are also likely to have an impact (i.e. a disruption during peak sales times would be more harmful). A recent survey by Arbor Networks (2016) provides estimates of the cost-per minute of downtime across a range of companies (see Figure 2.5).[9] Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) have provided average per event estimates of USD 52 000 for small to medium businesses and USD 444 000 for larger businesses. A study of US

claims found that insurance payouts for most incidents in 2016 were below USD 35 000 although at least one claim involved USD 750 000 in damages, including self-insured retentions (NetDiligence, 2016). Payouts of over USD 1 million (and up to USD 5 million) have been reported in previous years (NetDiligence, 2014).

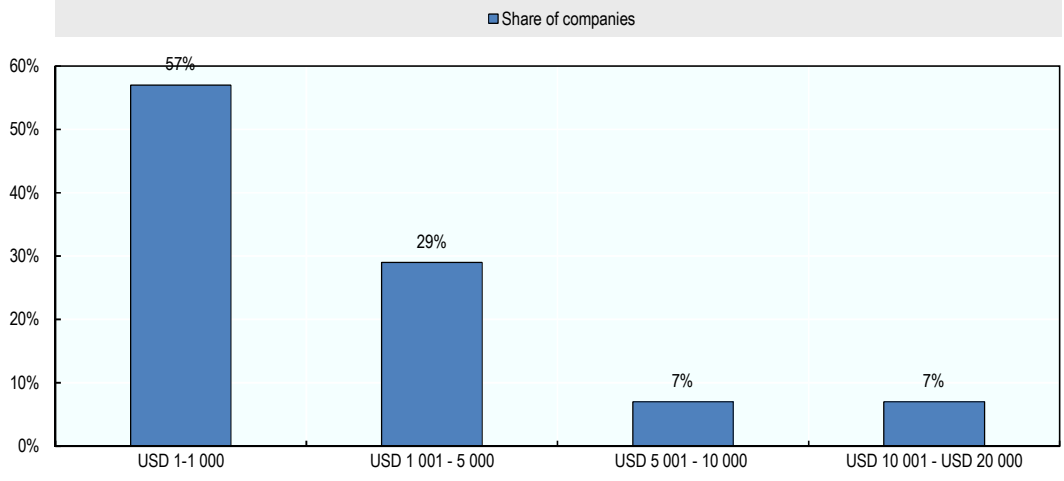
Box 2.5. **Distributed Denial-of-Service attack on Dyn**

On 21 October 2016, a huge DDoS attack against the servers of Dyn, a provider of domain name system (DNS) services, led to the disruption of a number of major websites in the United States and Europe, including Twitter, the Guardian, Netflix, Reddit, CNN and many others (Woolf, 2016). As a DNS service provider, Dyn translates requests for internet content into the IP addresses used to access that content. Therefore, a DDoS attack that overloads the capacity of Dyn to properly direct internet traffic will have a knock-on impact on the companies to whom it is providing its DNS services (i.e. the companies that depend on Dyn to direct traffic towards their content).

According to Dyn, the company was impacted by two DDoS attacks. The first attack initially targeted Dyn servers directing internet traffic in Asia-Pacific, Eastern Europe, South America and the Western United States and then shifted to servers directing traffic in the Eastern United States. The first attack took just over two hours to mitigate (although the actual time disruption to Dyn client websites would have varied). The second attack was targeted more diversely at servers directing internet traffic for users around the world and was mitigated in just over one hour (Hilton, 2016).

The DDoS attacks were reportedly implemented using the "Mirai" botnet which is able to generate requests to targeted servers by internet connected devices (webcams, wifi routers or even baby monitors) as well as computers. The use of such a broad range of devices allowed for an attack strength that apparently reached 1.2 Tbps using tens of millions of different IP addresses, approximately double the strength of the previous most powerful DDoS attack (which also used the same botnet) (Schneider, 2016).The attack on Dyn caused an estimated USD 110 million of (contingent) business interruption losses although very little was expected to have been insured given that most insurance policies use time deductibles that would normally be longer than the disruption caused by these incidents (Calversbert, 2016).

Figure 2.5. **Cost-per-minute of website downtime**



Source: Arbor Networks (2016). Cost-per-minute was not defined in the survey question although a related question on business impacts considered a wide-variety of potential costs, including operational expense, reputation/brand damage, revenue loss, remediation and investigation, loss of customers, loss of executive or senior management, regulatory penalties and/or fines, extortion payments and increases in cyber insurance premiums.

DoS attacks are increasingly used as a distraction aimed at occupying information technology security resources in order to reduce their ability to detect a simultaneous cyber attack (such as an attempt to access the company's internal network). In such cases, the DoS attack might lead directly to some business interruption losses as well as a data confidentiality breach or extortion payment (for example) and the various types of losses associated with those types of incidents. The survey by Arbor Networks (2016) found that extortion payments were made by 4% of respondents as a result of one or more DDoS incidents.

Inadvertent disruption of third-party system

The fourth sub-category of system malfunction identified by the CRO Forum is an inadvertent disruption to a third-party system. This type of malfunction refers to instances where a company's systems or networks are accessed by an unauthorised attacker in order to use those systems and networks to target a third party, for example through the spread of malware or as a botnet involved in a denial-of-service attack. In such cases, the company whose network was used as a botnet or for the transmission of malware could face a third-party liability claim from the company that was affected by the denial-of-service attack or faced damages or losses due to the malware. Under the CRO Forum's loss classification, these losses are defined as network security/security failure [liability] losses. No public information on the magnitude of losses from these types of incidents (or examples of such incidents) has been identified although information security experts report this as a common occurrence (although it is not clear how frequently liability is established). A particular exposure could emerge as a result of the increasing use of connected devices as botnets in DDoS attacks. For example, it is conceivable that a producer of routers used as botnets in a DDoS attack could face a liability claim by those affected by the attack based on an allegation of insufficient security protections.

Disruption of external digital infrastructure

The fifth type of system malfunction incident under the CRO classification is a disruption of external digital infrastructure. This would involve a disruption to a company's business resulting from a disruption to the information technology services provided by a third party (such as a cloud service provider (see Box 4.1) or a DNS service provider such as Dyn, as described in Box 2.5). In such cases, companies that depend on these service providers will face contingent business interruption losses, i.e. business interruption losses that are caused by an interruption at a related third-party (a supplier of information technology services). No public information on the magnitude of losses from these types of incidents was found. It is likely that companies that depended on Dyn to direct traffic to their internet content would have faced some contingent business interruption losses during the period when Dyn's servers were unable to direct traffic as normal (although, as noted, it is likely that these losses did not reach the time threshold for insurance coverage). Some of the disruptions to cloud service providers described in Box 4.1 might also have led to contingent business interruption losses. For information technology service providers, such disruptions could lead to technology errors and omissions liability (for example, if it is determined that the provider was negligent in protecting its systems against disruption).

Data integrity/availability

The CRO Forum classifies incidents involving the deletion, corruption or encryption of either own or third party data into a category on data integrity/availability. Similar to the data confidentiality category, the classification of an incident in this category is based on the detection of deleted, corrupted or encrypted data, rather than the underlying cause. The CRO Forum classification also establishes separate sub-categories for own and third party data. For the purposes of this report, two illustrative examples will be examined: (i) the deletion or corruption of own or third party data due to a software error; and (ii) the encryption of own or third party data as a result of an intrusion by ransomware. There may be some differences in terms of consequences between incidents where the underlying data is own data or third party data although this is most likely valid only in a minority of cases (e.g. where the impacted company has some kind of obligation to maintain a complete and accurate catalogue of third party data).

Deletion or corruption of own or third party data

The data held by a company, whether its own or belonging to a third party, may be deleted or corrupted as a result of human error or malicious attack. There is limited information on examples of this occurring as this kind of incident would normally only have implications for the company whose data holdings were affected (i.e. there would be no need to notify a third party if their own data had been deleted or corrupted unless the affected data holder is the only source of that data). The one well-known example of a malicious attack that resulted in the deletion of data was the 2015 attack on Saudi Aramco (Saudi Arabian state oil company) which led to deletion of data affecting over 30 000 computers (see Box 2.6).[10]

Box 2.6. **Malware attack on Saudi Aramco**

On the morning of 15 August 2015, a malware developed with a "timebomb" set to go off at a specific time began deleting the data on the computer hard drives connected to the internal network of Saudi Aramco, the state oil company. The choice of 15 August - a holy day in Saudi Arabia (Lailat al Qadr) - meant that a large proportion of Saudi Aramco's employees were not in the office (potentially slowing the response to the incident) (Perlroth, 2012). The malware succeeded in deleting data from approximately 75% of all of Saudi Aramco's corporate computers (approximately 35 000 affected computers) and led to days without internet and corporate email access as the network was shut-down to end the spread of the malware. Many of the company's business functions, such as shipping and contracting, were severely affected - although the company's oil production was managed through a separate unaffected network.

While the overall cost to the company of the incident is unknown, reports suggest that the company brought in information technology security experts from around the world to respond to the incident and purchased 50 000 computers to replace those that were affected by the malware (Rashid, 2015). In addition, the disruption to business functions apparently led the company to give oil away for free in order to maintain the continuity of domestic supply (Pagliery, 2015).

In terms of data corruption, there are few (if any) known example of incidents although a scenario has been developed by the University of Cambridge's Centre for Risk Studies (Ruffle et al., 2014) which provides one approximation of the magnitude of potential losses from a significant software sabotage leading to the corruption of data over time (see Box 2.7).

Box 2.7. **Loss potential of a data corruption incident: a scenario**

The Centre for Risk Studies at the University of Cambridge (Ruffle et. al., 2014) developed a sabotage scenario to estimate the loss potential due to the corruption of a widely-used database software. The scenario is based on the corruption of a relational database (i.e. a database structured to recognise relationships between data items) by a malicious (disgruntled) insider which produces small (and therefore less likely to be noticed) computational errors in the stored data over time. In the scenario, computational errors (or a "logic bomb") begin to impact various types of algorithmic processes in various sectors, including, for example, the design of manufactured parts, trading and pricing models, management information systems used for regulatory filings, process control systems used for managing equipment and logistics systems related to the management of supply chains. Broad use of the database across many sectors and processes along with the incremental corruption of data over time (which also means that database backups are corrupted) leads to significant and widespread uncertainty about data integrity. Losses are incurred by the database vendor as a result of the need to compensate their customers for their losses related to data integrity (technology errors and omissions liability) as well as by database users who may face compensation demands and/or lawsuits from customers that have purchased final products developed based on corrupted processes (product liability) and shareholders affected by the declining value of the affected companies' business (directors and officers liability). While the scenario does not include an estimate of losses faced by companies, it does provide an estimate of the share of global GDP at risk, ranging from 8% to 26% depending on the severity of the specific scenario.

Encryption of own or third party data

The encryption of own or third party data by an unauthorised external party would normally only occur as the result of a cyber extortion attack. In such incidents, an attacker will use malware known as "ransomware" to make data unavailable to its users through encryption until a payment is made to the extortionist.[11] In most cases, the encryption is sufficiently strong to ensure that the data is not recoverable without the payment of a ransom (Stransky, 2017). Some have suggested that ransomware may be replacing the sale of stolen data as the most effective way for cyber criminals to profit from network security breaches (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). There is some evidence that the frequency of ransomware attacks is on the rise while the recent WannaCry and NotPetya ransomware attack demonstrates the potential for broad scalability (see Box 2.8). Beazley (2017a and 2017b) reported a quadrupling of ransomware incidents among its clients in 2016 and an increase of 50% in the first half of 2017 (relative to the first half of 2016). AIG's operations in Europe, Middle East and Africa reported that 16% of all cyber claims it received between 2013 and 2016 (up to September) were for encryption ransomware extortion (AIG, 2016). Similarly, the number of worldwide users of a specific ransomware protection software that encountered ransomware rose by 17.7% to over 2.3 million users in the period April 2015 to March 2016 relative to the previous twelve months (April 2014 to March 2015) (Kaspersky Lab, 2016). Among respondents to the OECD questionnaire, the proliferation of ransomware remains among the most important factors in driving the level of cyber risk.

These types of incidents lead to losses classified by the CRO Forum as cyber ransom and extortion losses, including the cost of experts to manage the incident and the amount of any ransom payment made. Information on past losses related to extortion is not generally available as there are almost no disclosure or notification requirements,[12] and important incentives for not disclosing ransom payments (such as the aim of not encouraging further extortion demands). In the United States, an estimated USD 209 million in ransoms was paid by businesses and individuals to hackers in the first

quarter of 2016 alone (compared to a total of USD 25 million in 2015) (Twersky, 2016). For individuals and small organisations, payments related to ransomware are generally below USD 1 000 while most company payments are in the range of USD 10 000 to 50 000 (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). There is some evidence of ransom inflation with reports that the average ransom demand tripled in 2016 to just over USD 1 000 (Sharp, 2017). There are a handful of examples of much larger payments (in USD millions) by large corporations including a reported payment of "several million" by a European telecommunications company and several payments in the USD 3 million to USD 7 million range by companies and financial institutions in Greece, India and the United Arab Emirates (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). Recently, there has been an increase in attacks on hospitals in the United States and Europe, aimed at capitalising on their particular dependence on timely access to patient data (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). A study of US insurance claims found a range of costs from USD 12 500 to USD 75 000 with an average cost of USD 32 000, classified as forensic investigations costs and legal guidance including self-insured retentions (it is not clear whether ransom payments were made and/or reimbursed by insurance companies), (NetDiligence, 2016).

Box 2.8. **WannaCry and NotPetya**

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 (Robertson and Penty, 2017; Risk Management Solutions, 2017). The ransomware took advantage of a known vulnerability in the Microsoft Windows operating system for which a patch had been released in March. Files on infected computers were deleted and replaced with an encrypted version which could only be unlocked upon payment of a ransom of approximately USD 300, with the ransom amount increasing over time (Sherr, 2017). While the overall losses in terms of ransom payments were not significant, a number of organisations faced operational disruptions. For example, some hospitals in the United Kingdom were forced to divert patients while production at some Renault factories was halted in order to stop the spread of the malware (Robertson and Penty, 2017).

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 (this time, through an accounting software commonly-used in the Ukraine), encrypted data and sought a ransom payment of approximately USD 300 in bitcoin in order for the data to be decrypted (Harman, 2017; Satter, 2017) (although access to a decryption key was apparently disabled soon after the attack (Schlangenstein, 2017)). The attack led to disruptions in the operations of major ports in New York/New Jersey and Rotterdam managed by a Maersk subsidiary (Verbyany, Kravchenko and Turner, 2017) with some lasting more than two weeks after the initial attack (Shlangenstein, 2017). Maersk reported to investors that it expected to face costs of USD 200 million to USD 300 million as a result of the operational disruptions (Advisen, 2017d). FedEx's European subsidiary TNT was still reportedly using manual processes for some operations into July (Shlangenstein, 2017). In September, the company reported a USD 300 million reduction in quarterly profits as a result of the disruptions (Johnson, 2017). For manufacturing companies, the main impact was in terms of lost sales, including EUR 35 million for Beiersdorf AG,GBP 90 million for Reckitt Benckiser and EUR 250 million for Cie. de Saint-Gobain (Ricadela, 2017).

While neither event led to significant insured losses (partly due to limited impacts in the United States where more companies are insured against cyber risk), the global reach of "Wanna Cry" and the disruptive force of "NotPetya" are seen as illustrations of the potential for large losses from ransomware attacks (Suess, 2017a).

Malicious activity

The CRO Forum incident classification includes three sub-categories of malicious activity: (i) misuse of system (i.e. misuse of a digital system to distribute defamatory or embarrassing messages); (ii) targeted malicious communication (e.g. phishing attempts aimed at securing confidential information); and (iii) cyber fraud, cyber theft (e.g. an unauthorised financial transfer). For the purposes of this report, two illustrative examples will be examined: (i) the misuse of a system for defamatory statements; and (ii) cyber fraud/theft based on unauthorised network access and/or unauthorised use of financial credentials. One of the most common forms of targeted malicious communications ("CEO-phishing") is usually aimed at cyber fraud/theft and will be addressed in that section.

Misuse of systems for defamatory purposes

This sub-category of malicious activity would cover incidents that involve the misuse of digital systems to distribute defamatory or embarrassing statements/information. In the CRO Forum classification, it specifies that the information that is distributed would be defamatory or embarrassing to the victim, suggesting that this category is meant to cover first party damages and losses, not liability (the section on third party data confidentiality outlines an example of how the release of defamatory confidential information as the result of a breach could lead to third party liability for the organisation that is breached). The description specifically refers to "cyber bullying" and "cyber mobbing" suggesting that this category of incidents is mainly focused on individuals affected by defamatory or embarrassing statements on digital systems such as social media (see Box 3.2 for a brief overview of cyber insurance for individuals). In the case of individuals, losses might be incurred as a result of reputational damage related to distribution of defamatory or embarrassing statements.

Companies could also be affected by defamatory or embarrassing statements on digital systems (including social media) with potential consequences in terms of reputational damage. For example, in 2016, a fake press release claiming that Vinci (a French construction and engineering company) had dismissed its chief financial officer due to accounting irregularities was distributed to financial news outlets, leading to a fall in the company's share price of 18% (although the price later recovered after the company denied the information (Nussbaum, 2016)). In this case, there was no major loss to the affected company (Vinci) although the example provides an indication of the type of defamatory information that could be distributed and the potential for reputational damage.

Cyber fraud/cyber theft

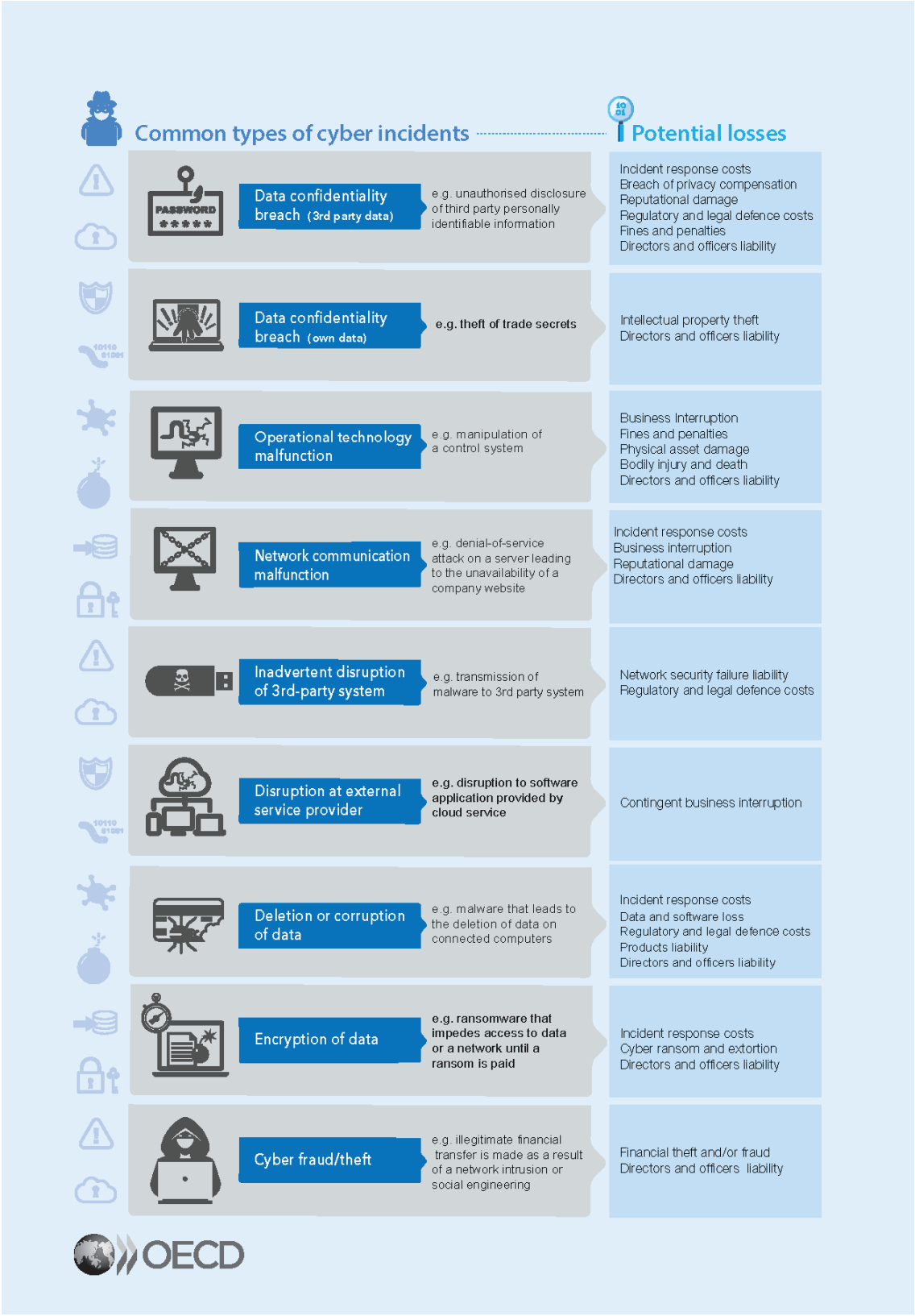
Cyber fraud or theft (i.e. unauthorised or fraudulent transfer of funds) could occur as a result of an intrusion into a company's network, the use of financial credentials to make an unauthorised transfer of funds or through deception (for example, by impersonating a company officer in an email seeking to initiate a transfer of funds). In these cases, the cyber fraud or theft would lead to pure financial losses (categorised as financial theft and/or fraud under the CRO Forum loss classification).

There are a few examples of cyber theft that appear to have resulted from some form of network intrusion, including through unauthorised inter-bank transfers (such as the USD 101 million transferred from the Bank of Bangladesh's account at the New York

Federal Reserve (along with a number of other transfers and attempted transfers attributed to the same criminal gang (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017)) and the creation of bank cards (with manipulated limits) to withdraw cash from Automated Teller Machines (ATMs) (e.g. USD 45 million was withdrawn using pre-paid travel cards from Indian credit card processors in 2013 while JPY 1.8 billion was stolen from ATMs in Japan based on credit card data from the customers of a South African bank in 2016). In 2016, Tesco Bank in the United Kingdom was affected by a cyber attack that resulted inGBP 2.5 million in funds being fraudulently transferred from approximately 9 000 customer accounts (although the details on how this was done have not been publicly disclosed) (Leyden, 2016). There is at least one example from Thailand of thieves loading malware directly onto ATMs in order to withdraw funds from these machines (Lewis, Wieland and Peel, 2016). A number of real estate companies in the United States (amongst others) have also been the victims of unauthorised transactions, usually involving escrow accounts and transfers of USD 1.5 to 2.0 million (Krebs, 2014a; Krebs, 2014b; Krebs, 2013). There are also a number of examples of major thefts of crypto-currencies due to network intrusions. According to one analysis, since the creation of bitcoin in 2009 (up to March 2015), 33% of all bitcoin exchanges that have operated have been hacked, in many cases leading to significant losses for customers of those exchanges (Chavez-Dreyfuss, 2016).

Another approach that is being used to commit cyber fraud or theft is through the use of social engineering (i.e. sending targeted email impersonating a legitimate person) aimed at initiating a financial transaction for the benefit of the attacker. For example, one common approach is to send an email impersonating the CEO or other senior officer of a company and demanding that payment be made to a specific account ("CEO-Phishing"). In 2016, the US Federal Bureau of Investigation (FBI, 2016) issued a press release to warn businesses of this fraud (which they termed "business email compromise") citing USD 2.3 billion in fraudulent payments by 17 642 victims between October 2013 and February 2016 (an average of about USD 130 000 per victim, although with a potential for significant variation). According to one report, the amount of lost funds has increased to USD 5.3 billion up to December 2016 (CNA Financial Corporation, 2017) with a 1 300% increase since 2015 (FBI, 2016). In one case (Ubiquiti Networks), USD 46.7 million in fraudulent transactions was disclosed in one quarter as a result of this type of social engineering (Wickliffe, 2016). In Europe, there have also been several transfers of significant funds as a result of this type of social engineering fraud, including a USD 75 million transfer from a Belgian bank, a USD 50 million transfer from an Austrian aircraft parts manufacturer and a EUR 50 million transfer by a German cable manufacturer (FireEye, 2017; Suess, 2017b). A survey of UK firms in 2016/2017 found that 6% of those surveyed had money stolen as a result of a fraudulent email or website in the previous 12 months (the same percentage as 2015/2016) (Department for Culture, Media & Sport, 2016; Department for Culture, Media & Sport, 2017).

Figure 2.6. **Common types of cyber incidents and resulting losses**



Source: Adapted from OECD (2017)

Notes

1. According to Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), the black market value of US credit card numbers, email account credentials, social security numbers, and basic personal information (name, address, email address, phone number) declined between 2012 and 2015. However, the black market value of bank account access credentials, healthcare records, credit history and certain website account access credentials has increased (substantially in the case of healthcare records and bank account access credentials).

2. According to Swiss Re (2017), the types of credit monitoring services that are often provided in the United States are prohibited in continental Europe (although permitted in the United Kingdom).

3. Public sector entities affected by data confidentiality breaches could also face costs related to the release of confidential information. The US Office of Personnel Management, for example, reportedly faces USD 1 billion in costs for credit monitoring services and identity theft protection over 10 years for employees whose data was accessed as a result of a data confidentiality breach (Advisen, 2017a).

4. According to some reports, the developing jurisprudence from data breach litigation in the United States suggests that the breach of some types of data (e.g. social security numbers, usernames, password) is more likely to lead to harm than others (e.g. name or payment card information given the ability to cancel payment cards) (Soloway and Mohler, 2017).

5. The Payment Card Industry Data Security Standard is a set of standards that retailers must adhere to in order to be able to accept and process payment card payments. The standards were established by the payment card networks who, based on contractual arrangements they enter into with retailers, have the authority to impose fines and assessment on non-compliant retailers. As discussed in Chapter 3, these fines and assessments are contractual (different than administrative fines imposed by regulatory agencies) and may be covered under some stand-alone cyber insurance policies (often as a specific add-on/endorsement).

6. The Ponemon Institute (2017) reports the average cost of a breach segmented by the amount of stolen records. For breaches involving less than 10 000 records, the average cost was USD 1.9 million. For breaches involving more than 50 000 records (i.e. at least 5 times more records), the average cost was USD 6.3 million (i.e. just over 3 times more). This would indicate that the average cost per record is lower for larger breaches.

7. For the purposes of this report, only own system malfunctions due to a technical issue are considered (i.e. not malfunctions that result from physical damage, such as a fire in a data centre). This is consistent with how this damage would normally be covered by insurance as tangible damage caused by a physical peril would normally be covered by a property insurance policy rather than a stand-alone cyber insurance policy (subject to the exclusions outlined in Box 3.1).

8. According to an OECD (2009) definition, "malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners. Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the

information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity".

9. A Ponemon Institute (2012) survey of medium-to-large US-based companies found much higher estimates of the cost of downtime (USD 22 000 per minute on average and USD 1.2 million per event based on an average duration of 54 minutes). This estimate includes "possible lost traffic, end-user productivity and lost revenues" and potentially other costs.

10. This could also be considered a system malfunction incident as the malware that infected the Saudi Aramco computers deleted all data, including the data needed for the computers to operate.

11. Cyber-extortionists may also use the threat of a DoS attack or a data release (resulting from a data confidentiality breach) as another means of extracting a payment from targeted firms.

12. In the United States, an incident involving the encryption of health data is considered to be a data breach incident and subject to the notification requirements under the *Health Insurance Portability and Accountability Act*.

References

Advisen (2017a), "$1 billion in losses possible from Office of Personnel Management breach that affected 22 million federal workers and retirees", *Advisen Cyber Loss Data*.

Advisen (2017b), "$142,000,000 in Response Costs for Anthem", *Advisen Cyber Loss Data*.

Advisen (2017c),"Equifax board weighs clawbacks", *Advisen Cyber FPN : Digest Edition*, 4 October.

Advisen (2017d), "$200M Ransomware (NotPetya) Loss for A.P. Moller-Maersk", *Advisen Cyber Loss Data*.

AIG (2016), "Behind the numbers: Key drivers of cyber insurance claims", AIG White Paper /Claims Intelligence Series, www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-intelligence-cyber.pdf, accessed 14 April 2017.

Alder, W. (2015), Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim, Becker & Poliakoff Legal and Business Strategists, www.becker-poliakoff.com/webfiles/pdf/alder/20151001_alder_data_breaches.pdf, accessed 17 March 2017.

Allianz Global Corporate & Specialty (2015), *Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, Allianz Global Corporate & Specialty SE, Munich, www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

Akamai (2017b), *State of the internet/security (Q2 2017 report)*, Akamai, Cambridge (United States).

Akamai (2017a), *State of the internet/security (Q1 2017 report)*, Akamai, Cambridge (United States).

Akamai (2016d), *State of the internet/security (Q4 2016 report)*, Akamai, Cambridge (United States).

Akamai (2016c), *State of the internet/security (Q3 2016 report)*, Akamai, Cambridge (United States).

Akamai (2016b), *State of the internet/security (Q2 2016 report)*, Akamai, Cambridge (United States).

Akamai (2016a), *State of the internet/security (Q1 2016 report)*, Akamai, Cambridge (United States).

Akamai (2015d), *State of the internet/security (Q4 2015 report)*, Akamai, Cambridge (United States).

Akamai (2015c), *State of the internet/security (Q3 2015 report)*, Akamai, Cambridge (United States).

Akamai (2015b), *State of the internet/security (Q2 2015 report)*, Akamai, Cambridge (United States).

Akamai (2015a), *State of the internet/security (Q1 2015 report)*, Akamai, Cambridge (United States).

Akamai (2014c), *State of the internet/security (Q4 2014 report)*, Akamai, Cambridge (United States).

Akamai (2014b), *State of the internet/security (Q3 2014 report)*, Akamai, Cambridge (United States).

Akamai (2014a), *State of the internet/security (Q2 2014 report)*, Akamai, Cambridge (United States).

Anthem Inc. (2017), *Annual Report on Form 10-K For the Year Ended December 31, 2016*, Anthem Inc.

Arbor Networks (2016), Worldwide Infrastructure Security Report (Volume XI), Arbor Networks Inc., Burlington (Massachusetts), www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf.

Artemis (2017), "Cyber risks and government pools. Too soon?", *Artemis news articles*, 30 March, www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/.

Aschkenasy, J. (2013), "CGL exclusions will fuel cyber purchase trend", *Advisen News* (18 November), www.advisenltd.com/insurance-news/2013/11/18/cgl-exclusions-will-fuel-cyber-purchase-trend/

Auchard, E. and T. Käckenhoff (2016), "Trade Secrets Stolen in Massive Cyber Attack Against Steelmaker ThussenKrupp", *Carrier Management*, 8 December, www.carriermanagement.com/news/2016/12/08/161885.htm.

BakerHostetler (2016), Is your organizations compromise ready?- 2016 Data Security Incident Response Report, Baker Hostetler, New York.

BakerHostetler (2015), 2015 International Compendium of Data Privacy Laws, https://her-consulting.com/wp-content/uploads/2015/12/2015-BakerHostetler-International-Compendium-of-Data-Privacy-Laws.pdf, accessed 16 March 2017.

Basak, S. and J. Surane (2017), "Equifax's Cyber Insurance Reportedly Not Enough to Address Massive Breach", *Carrier Management*, 10 September, www.carriermanagement.com/news/2017/09/10/171030.htm.

Beazley (2017a), "Beazley sees new phishing threats emerge", *Beazley Breach Insights (April)*, www.beazley.com/Documents/Insights/201704-beazley-breach-insights-us.pdf.

Beazley (2017b), " Ransomware attacks steal headlines, but accidental data breaches remain a major cause of loss", *Beazley Breach Insights (July)*, www.beazley.com/Documents/Insights/201707-beazley-breach-insights-us.pdf.

Calvesbert, G. (2016), "From Disaster Scenario to Reality: Modeling the Dyn Cyber Attack", *AIR Worldwide (In Focus)*, 27 October, www.air-worldwide.com/Blog/From-Disaster-Scenario-to-Reality--Modeling-the-Dyn-Cyber-Attack/.

Chavez-Dreyfuss, G. (2016), "Bitcoin Exchanges Face Growing Cyber Hacking Risks", *Carrier Management*, 29 August, www.carriermanagement.com/news/2016/08/29/158302.htm.

CNA Financial Corporation (2017), "How to protect your insurance clients against the latest social engineering scams", *Property Casualty 360°*, 19 September, www.propertycasualty360.com/2017/09/19/how-to-protect-your-insurance-clients-against-the.

Condliffe, J. (2016), "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks", *MIT Technology Review*, 22 December, www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

CRO Forum (2016), *CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk (June)*, CRO Forum, Amsterdam.

CRO Forum (2014), *Cyber resilience: The cyber risk challenge and the role of insurance*, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

De Freltas, I. (2016), "Record Fine for TalkTalk Data Breach", *Berwin Leighton Paisner Expert Legal Insights*, 17 October, www.blplaw.com/expert-legal-insights/articles/record-fine-for-talktalk-data-breach2, accessed 30 March 2017.

Department of Health and Human Services (2017), "$5.5 million HIPAA settlement shines light on the importance of audit controls", *News Release*, 16 February, Department of Health and Human Services, Washington.

Department for Culture, Media and Sport (2017), *Cyber Security Breaches Survey 2017*, Department for Culture, Media and Sport, London.

Department for Culture, Media and Sport (2016), *Cyber Security Breaches Survey 2016*, Department for Culture, Media and Sport, London.

Department for Business, Innovation and Skills (2015), *2015 Information Security Breaches Survey: Technical Report*, Department for Business, Innovation and Skills, London.

Detica and Cabinet Officer (2011), *The Cost of Cybercrime*, Detica Limtied, Surry (United Kingdom).

Drinkwater, D. (2014), "eBay counts the cost after 'challenging' data breach", *SC Magazine UK*, 17 July, www.scmagazineuk.com/ebay-counts-the-cost-after-challenging-data-breach/article/541162/.

eBay Inc. (2017), *Form 10-K For the Year Ended December 31, 2016*, eBay Inc.

Edwards et al. (2014), "Hype and Heavy Tails: A Closer Look at Data Breaches", Workshop on the Economics of Information Security.

European Union (2016), *Directive (EU) 2015/2366 of the European Parliament and the Council of of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

European Union (2015), *Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*, European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

FBI (2016), *FBI Warns of Dramatic Increase in Business E-Mail Scams*, 4 April, US Federal Bureau of Investigation, Phoenix, www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams, accessed 22 March 2017.

FBI (2017), *Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally*, 27 February, US Federal Bureau of Investigation, www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise, accessed 9 October 2017.

Finkle, J. (2017), "Cyber firms warn of malware that could cause power outages", *Reuters*, 12 June, www.reuters.com/article/us-cyber-attack-utilities/cyber-firms-warn-of-malware-that-could-cause-power-outages-idUSKBN1931EG3.

FireEye (2017), *Cyber Threats: A perfect strom about to hit Europe?*, FireEye Inc., Milpitas (California), January.

Gambrell, J. (2016), "Blazes at Iran petrochemical plants raise suspicions of cyberattack", *The Times of Israel*, 22 September, www.timesofisrael.com/blazes-at-iran-petrochemical-plants-raise-suspicions-of-cyberattack/.

Gemalto NV (2016), *It's All About Identity Theft: First half findings from the 2016 Breach Level Index*, Gemalto NV, Meudon, France, www.breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf.

Goel, V. (2017), "Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack", *The New York Times*, 1 March, www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-bonus.html?_r=0.

Goodman, E. (2016), "Risky business: High financial costs for payment breaches at small retailers", *Property Casualty 360°*, 9 September, www.propertycasualty360.com/2016/09/09/risky-business-high-financial-costs-for-payment-br.

Hachman, M. (2011), "PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher", *PCMag*, 23 May, www.pcmag.com/article2/0,2817,2385790,00.asp.

Halliday, J. (2013), "Data watchdog fines Sony £250,000 over PlayStation ID hack", *The Guardian*, 24 January, www.theguardian.com/technology/2013/jan/24/sony-fined-over-playstation-hack.

Harman, P. (2017), "The newest global cyber attack takes down ports, banks and law firms", *Property Casualty 360°*, 30 June,

www.propertycasualty360.com/2017/06/30/the-newest-global-cyber-attack-takes-down-ports-ba.

Harrison, C. (2017), "Yahoo triples likely scope of 2013 hack to 3 billion users", *Property Casualty 360°*, 3 October, www.propertycasualty360.com/2017/10/03/yahoo-triples-likely-scope-of-2013-hack-to-3b-user.

Heartland Payment Systems (2011), *2010 Annual Report*, Heartland Payment Systems.

Herman, B. (2016), "Details of Anthem's massive cyberattack remain in the dark a year later", *Modern Healthcare*, 30 March, www.modernhealthcare.com/article/20160330/NEWS/160339997.

Hilton, S. (2016), "Dyn Analysis Summary of Friday October 21 Attack", *Company News*, 26 October, http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, accessed 20 March 2017.

Howard, P. and O. Guylas (2014), *Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014 (Public Data)*, Center for Media, Data and Society (CMDS), Central European University, Budapest, https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope-publicdata.xlsx (accessed 21 September 2016).

Hurtado, P. (2017), "Target agrees to pay $18.5 million to end data-breach probes", *Property Casualty 360°*, 23 May, www.propertycasualty360.com/2017/05/23/target-agrees-to-pay-185-million-to-end-data-breac.

IDT911 (2016), *Keeping Business Policyholder Data Secure Builds Loyalty and Brand Awareness (White Paper)*, IDT911 Inc., Galway (Ireland).

Identity Theft Resource Centre (2016), *Data Breach Stats Report*, Identity Theft Resource Centre.

Information Commissioner's Office (2015), *Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998*, December, https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf.

Information Security Media Group (2013), "Global Payments Breach Tab: $94 million", *Bank Info Security*, 10 January, www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415, accessed 19 October 2016.

Insurance Information Institute (2014), *Cyber risks: the growing threat*, Insurance Information Institute, New York.

Insurance Journal (2017a), "New York's Cuomo Proposes Regulation in Wake of Equifax Security Breach", *Insurance Journal*, 19 September, www.insurancejournal.com/news/east/2017/09/19/464767.htm.

Insurance Journal (2017b), "Massachusetts' AG Healey Announces Data Breach Bill Following Equifax Hack", *Insurance Journal*, 26 September, www.insurancejournal.com/news/east/2017/09/26/465451.htm.

Jefferson, E. A. (2017), "Insurance experts: WannaCry calls for tougher cyber security", *Property Casualty 360°*, 16 May, www.propertycasualty360.com/2017/05/16/insurance-experts-wannacry-calls-for-tougher-cyber.

Johnson, E. (2017), "FedEx Goes Cyber Insurance Shopping After Profit Takes Hit from Attack", *Insurance Journal*, 20 September, www.insurancejournal.com/news/national/2017/09/20/464842.htm.

JP Morgan Chase & Co. (2016), *Annual Report 2015*, JP Morgan Chase & Co., New York.

Kamaiko, L. (2016), "Business Email Compromise: Which Insurance Policy Pays?", *Carrier Management*, 25 September, www.carriermanagement.com/features/2016/09/25/159183.htm.

Kaspersky Lab (2016), *KSN Report: Ransomware in 2014-2016*, Kaspersky Lab, https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

Kelley, M. (2016), "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", *Business Insider*, 20 November, www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T.

Kerner, S. M. (2014a), "The Real Cost of the eBay Breach", *eWeek*, 17 July, www.eweek.com/blogs/security-watch/the-real-cost-the-ebay-breach.html.

Kerner, S. M. (2014b), "Why JPMorgan Chase Data Breach May Have Financial Fallout", *eWeek*, 5 October, www.eweek.com/security/why-jpmorgan-chase-data-breach-may-have-financial-fallout.

Kerr, D. (2012), "Sony PSN hacking lawsuit dismissed by judge", *CNET*, 23 October, www.cnet.com/news/sony-psn-hacking-lawsuit-dismissed-by-judge/.

Kim, S. and S. Cha (2014), "South Korea to Suspend 3 Credit Card Firms Over Data Theft", *Bloomberg*, 3 February, www.bloomberg.com/news/articles/2014-02-02/south-korea-to-suspend-3-credit-card-firms-over-data-theft.

King, R. (2009), "Lessons from the Data Breach at Heartland", *Bloomberg*, 7 July, www.bloomberg.com/news/articles/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice.

Krebs, B. (2014a), "$1.66M in Limbo After FBI Seizes Funds from Cyberheist", *KrebsonSecurity (blog)*, 25 September, https://krebsonsecurity.com/2014/09/1-66m-in-limbo-after-fbi-seizes-funds-from-cyberheist/, accessed 19 October 2016.

Krebs, B. (2014b), "Feds Charge Calif. Brothers in Cyberheists", *KrebsonSecurity (blog)*, 14 November, https://krebsonsecurity.com/2013/11/feds-charge-calif-brothers-in-cyberheists/, accessed 19 October 2016.

Krebs, B. (2013), "$1.66M in Limbo After FBI Seizes Funds from Cyberheist", *KrebsonSecurity (blog)*, 25 September, https://krebsonsecurity.com/2014/09/1-66m-in-limbo-after-fbi-seizes-funds-from-cyberheist/, accessed 19 October 2016.

LaCroix, K. (2017), "Shareholder Files Data Breach Securities Class Action Lawsuit Against Yahoo", *The D&O Diary*, 25 January, www.dandodiary.com/2017/01/articles/cyber-liability/shareholder-files-data-breach-securities-class-action-lawsuit-yahoo/.

Larson, E. (2016), "Adultery site Ashley Madison pays $1.65M settlement for 2015 data breach", *Property Casualty 360°*, 14 December, www.propertycasualty360.com/2016/12/14/adultery-site-ashley-madison-pays-165m-settlement.

Lee, J. (2014), "South Koreans seethe, sue as credit card details swiped", *Reuters*, 21 January, www.reuters.com/article/us-korea-cards-idUSBREA0K05120140121.

Leigh Day (2016), *Information lawyers welcome record fine for TalkTalk data breach*, 6 October, Leigh Day, London, www.leighday.co.uk/News/News-2016/October-2016/Information-lawyers-welcomes-record-fine-for-TalkT, accessed 15 March 2017.

Lewis, L., D. Weinland and M. Peel (2016), "Asia Hacking: Cashing in on cyber crime", *Financial Times*, London (19 September), www.ft.com/content/38e49534-57bb-11e6-9f70-badea1b336d4.

Leyden, J. (2016), "What went wrong at Tesco Bank?", *The Register*, 10 November, www.theregister.co.uk/2016/11/10/tesco_bank_breach_analysis/.

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

Lord, N. (2016), "A Timeline of the Ashley Madison Hack", *Data Insider*, 14 October, https://digitalguardian.com/blog/timeline-ashley-madison-hack.

Lui, S. (2017), "How Will Australia's New Mandatory Data Breach Notification Laws Impact Your Business?", *lifehacker AU*, https://www.lifehacker.com.au/2017/02/how-will-australias-new-mandatory-data-breach-notification-laws-impact-your-business/, accessed 14 April 2017.

MacLean, P. (2017), "Anthem agrees to $115 million settlement over data breach", *Property Casualty 360°*, 26 June, www.propertycasualty360.com/2017/06/26/anthem-agrees-to-115-million-settlement-over-data.

McCrank, J., D. Voltz and S. Mukherjee (2017), "Equifax CEO Smith Retires After Massive Cyber Attack", *Carrier Management*, 26 September, www.carriermanagement.com/news/2017/09/26/171599.htm.

McGlasson, L. (2009), "Heartland Payment Systems, Forcht Bank Discover Data Breaches", *Bank Indor Security*, 21 January, www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168.

NCCIC/ICS-CERT (n.d.), *NCCIC/ICS-CERT Year in Review (FY 2015)*, Department of Homeland Security National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team, Washington, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

NetDiligence (2016), *2016 Cyber Claims Study*, NetDiligence.

NetDiligence (2015), *2015 Cyber Claims Study*, NetDiligence.

NetDiligence (2014), *2014 Cyber Claims Study*, NetDiligence.

Nussbaum, A. (2016), "Vinci Plunges After Hoax Report on Financial Irregularities", *Bloomberg Markets*, 22 November, www.bloomberg.com/news/articles/2016-11-22/vinci-says-builder-isn-t-revising-acccounts-cfo-isn-t-fired.

OECD (2017), *Supporting an effective cyber insurance market: OECD Report for the G7 Presidency*, 13 May, Paris. www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf.

OECD (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264056510-en.

Osborne, C. (2015), "Anthem data breach cost likely to smash $100 million barrier", *ZeroDay*, 12 February, www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/.

Paganini, P. (2016), "OVH hosting hit by 1Tbps DDoS attack, the largest one ever seen", *Security Affairs*, 25 September, http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html.

Pagliery, J. (2015), "The inside story of the biggest hack in history", *CNN Money*, 5 August, http://money.cnn.com/2015/08/05/technology/aramco-hack/.

Perlroth, N. (2012), "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", *The New York Times*, 23 October, www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Pettersson, E. (2017), "Legal Experts See Room for Deal in Equifax Data Breach Lawsuits", *Insurance Journal*, 25 September, www.insurancejournal.com/news/national/2017/09/25/465299.htm.

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.

Phillips, M. et al. (2017), "Not all data breaches are created equal", *Property Casualty 360°*, 13 February, www.propertycasualty360.com/2017/02/13/not-all-data-breaches-are-created-equal.

Ponemon Institute (2017), *2017 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, Traverse City (Michigan).

Ponemon Institute (2016), *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, Traverse City (Michigan).

Ponemon Institute (2015), *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, Traverse City (Michigan).

Ponemon Institute (2014), *The Aftermath of a Mega Data Breach: Consumer Sentiment*, Ponemon Institute LLC, Traverse City (Michigan).

Ponemon Institute (2012), *Cyber Security on the Offense: A Study of IT Security Experts*, Ponemon Institute LLC, Traverse City (Michigan).

PwC (2016), *Moving forward with cybersecurity and privacy: Key findings from The Global State of Information Security® Survey 2017*, PwC.

Rashid, F. (2015), "Inside The Aftermath Of The Saudi Aramco Breach", *Dark Reading*, 8 August, www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676.

Reuters (2017), " Lawsuits against Equifax pile up after massive data breach", *Reuters*, 11 September, www.reuters.com/article/us-equifax-cyber-lawsuits/lawsuits-against-equifax-pile-up-after-massive-data-breach-idUSKCN1BM2E3.

Ricadela, A. (2017), "WannaCry, Petya Cyber Attacks Cost Europe's Companies Hundreds of millions of Dolllars", *Carrier Management*, 3 August, www.carriermanagement.com/news/2017/08/03/169480.htm.

Risk Management Solutions (2017), "Implications of the WannaCry Cyber-Attack for Insurance", *RMS Blog*, 17 May, www.rms.com/blog/2017/05/17/implications-of-the-wannacry-cyber-attack-for-insurance/, accessed 9 October 2017.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2017), *2017 Cyber Risk Landscape*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

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.

Robertson, J. and R. Penty (2017), "No Monday Morning Reprieve for Cyber Attack Victims", *Carrier Management*, 14 May, www.carriermanagement.com/news/2017/05/14/167107.htm.

Robertson, J. and M. Riley (2014), "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar", *Bloomberg*, 10 December, www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

Rodionova, Z. (2016), "TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers", *The Independent*, 5 October, www.independent.co.uk/news/business/news/talktalk-fine-data-breach-theft-customers-information-stolen-record-penalty-a7346316.html.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol 2 (2), pp. 121-135.

Rose, M. (2011), "Canadian Law Firm Files $1B Lawsuit Against Sony Over PSN Data Breach", *Gamasutra*, 4 May, www.gamasutra.com/view/news/34499/Canadian_Law_Firm_Files_1_Billion_Class_Action_Lawsuit_Against_Sony_Over_PSN_Data_Breach.php.

Rosenthal, B. (2016), "The Ashley Madison Hack — One Year Later", *Logical Operations*, 20 July, http://logicaloperations.com/insights/blog/2016/07/20/405/the-ashley-madison-hack-one-year-later/.

Ruffle, S.J. et al. (2014), *Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe*, Centre for Risk Studies, University of Cambridge, http://cambridgeriskframework.com/getdocument/9.

Satter, R. (2017), "Tax Software Firm at Center of Cyber Attack Knew of Problems; Criminal Liability Possible", *Carrier Management*, 9 July, www.carriermanagement.com/news/2017/07/09/168837.htm.

Schlangenstein, M. (2017), "Cyber Attack Leads to Big Business Interruption, Earnings Issues for FedEx's TNT Unit", *Carrier Management*, 17 July, www.carriermanagement.com/news/2017/07/17/169038.htm.

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

Schneider, B. (2016), "Lessons From the Dyn DDoS Attack", *Security Intelligence*, 1 November, https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/.

SEC (2011), *CF Disclosure Guidance: Topic No. 2 (Cybersecurity)*, U.S. Securities and Exchange Commission, 13 October, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, accessed 17 March 2017.

SecureWorks (2012), "A Famous Data Security Breach & PCI Case Study: Four Years Later", *SecureWorks*, 25 October, www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland.

Sharp, A. (2017), "Hackers' Ransom Demands Rise as Victims Keep Paying: Symantec", *Insurance Journal*, 27 April, www.insurancejournal.com/news/international/2017/04/27/449147.htm.

Sherr, I. (2017), "WannaCry ransomware: Everything you need to know", *CNet*, 19 May, www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

Smith, G. (2017), "HBO Cyber Attack – Latest in Growing Problem for Hollywood", *Insurance Journal*, 1 August, www.insurancejournal.com/news/national/2017/08/11/460853.htm.

Soloway, T. and B. Mohler (2017), "Adultery Site Ashley Madison to Pay $11.2 million for User Data Breach", *Insurance Journal*, 17 July, www.insurancejournal.com/news/national/2017/07/17/457733.htm.

Sony Corporation (2015), *Annual Report Pursuant to Section 13 of 15(d) of the Securities Exchange Act of 1934 For the fiscal year ended March 31, 2015*, Sony Corporation.

Steptoe and Johnson LLP (2016), *Commentary on the General Data Protection Regulation (GDPR): The GDPR from an insurance and financial mediation perspective* , Prepared for BIPAR, July.

Stempel, J. (2017), "Anthem agrees to $115 million settlement over data breach", *Property Casualty 360°*, 26 June, www.propertycasualty360.com/2017/06/26/anthem-agrees-to-115-million-settlement-over-data.

Stransky, S. (2017), "How to Protect Your Data from Being Held for Ransom", *In Focus*, AIR Worldwide, 1 February, www.air-worldwide.com/Blog/How-to-Protect-Your-Data-from-Being-Held-for-Ransom/.

Suess, O. (2017a), "Days of Cyber Insurers Avoiding Costly Claims May Be Numbered: Expert", *Insurance Journal*, 7 July, www.insurancejournal.com/news/international/2017/07/07/456896.htm.

Suess, O. (2017b), "Cyber crime fears drive up demand for anti-hacker insurance", *Property Casualty 360°*, 10 May, www.propertycasualty360.com/2017/05/10/cyber-crime-fears-drive-up-demand-for-anti-hacker.

Swiss Re (2017), *Cyber liability: data breach in Europe*, Swiss Re, Zurich.

TalkTalk Group (2016), *Annual Report 2016*, TalkTalk Telecom Group PLC, London.

Target Corporation (2017), *2016 Annual Report*, Target Corporation, Minneapolis.

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

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

The Associated Press (2017), "Yahoo Security Breaches Cost Marissa Mayer millions in Bonus, Stocks", *NBC News*, 2 March, www.nbcnews.com/tech/internet/yahoo-security-breaches-cost-marissa-mayer-millions-bonus-stocks-n728021.

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

Tsangaris, H. (2016), "5 essentials of a Cyber liability insurance policy", *Property Casualty 360°*, 31 May.

Tsukayama, H. (2016), "Could Yahoo be in trouble with the SEC", *The Washington Post*, 28 September.

Twersky, D. (2016), "How to respond to cyber extortion demands", *Property Casualty 360°*, 26 August.

US Census Bureau (2016), *Retail Excluding Motor Vehicle and Parts Dealers*, www.census.gov/retail/marts/www/adv4400a.txt (accessed 22 November 2016).

Vaas, L. (2014), "South Korea punishes three credit card firms over data heist", *naked security*, 18 February, https://nakedsecurity.sophos.com/2014/02/18/south-korea-punishes-three-credit-card-firms-over-data-heist/.

Verbyany, V., S. Kravchenko and G. Turner (2017), "Global cyberattack hits telecoms, retailers, Chernobyl nuclear plant", *Property Casualty 360°*, 27 June, www.propertycasualty360.com/2017/06/27/global-cyberattack-hits-telecoms-retailers-chernob.

Verizon (2016), *2016 Data Breach Investigations Report*, Verizon, www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

Verizon (2015), *2015 Data Breach Investigations Report*, Verizon.

Wickliffe, R. (2016), "Gone phishing: CEO fraud costs companies millions", *Property Casualty 360*, 7 September, www.propertycasualty360.com/2016/09/07/gone-phishing-ceo-fraud-costs-companies-millions, accessed 18 October 2016

Woolf, N. (2016), "DDoS attack that disrupted internet was largest of its kind in history, experts say", *The Guardian*, 26 October, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Zetter, K. (2015), "A cyberattack has caused confirmed physical damage for the second time ever", *Wired*, www.wired.com/2015/01/german-steel-mill-hack-destruction/.

Zetter, K. (2016), "Inside the cunning, unprecedented hack of Ukraine's power grid", *Wired*, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Chapter 3

The cyber insurance market

This chapter provides an overview of the cyber insurance market, including the types of losses that are commonly covered across stand-alone cyber insurance policies and traditional policies and also the losses that are more difficult to cover. It provides some data on the size of the stand-alone cyber insurance market, penetration levels and pricing, as well as information on how insurers underwrite cyber insurance coverage approach and the additional risk mitigation and crisis response services that are often offered with cyber insurance policies.

Coverage for losses and damages resulting from cyber incidents may be provided as stand-alone coverage for certain cyber risks or as a specific endorsement (either on a primary or difference-in-conditions basis[1]) on existing policies (e.g. errors and omissions/professional indemnity, general liability, property or others). Such coverage might also be included in other coverages (without a specific endorsement) either unintentionally (such as in the case of a court-imposed legal interpretation of policy language) or intentionally (where insurance companies themselves interpret their policy language as including coverage for some cyber security related losses). In general, cyber insurance buyers are commercial entities, although some coverage for cyber risks faced by individuals is starting to emerge (see Box 3.2).

While the market for cyber insurance is generally perceived as being in its infancy, specific cyber insurance products have been available for nearly 20 years in some countries, particularly in the United States. The initial focus of the cyber insurance market was on providing errors and omissions coverage for companies providing technology-based services (Fitch Ratings, 2017; Bolot and Lelarge, 2008). The increasing occurrence of cyber incidents and, in particular, the establishment of privacy breach notification requirements and penalties (beginning in 2003 in the US state of California) resulted in new exposures to first party losses (such as incident response costs) and third party liability claims that insurers had not considered when underwriting property and liability coverage. As a result, a number of exclusions have been developed and written into traditional insurance policies - leading to the development of stand-alone cyber insurance products to address risks excluded from traditional policies (see Box 3.1).

Box 3.1. **Common cyber-related exclusions to traditional policies**

Cyber incidents have emerged as potential sources of damage, theft and liability that were not previously considered in the underwriting of property, crime, kidnap and ransom, liability and other traditional policies. For some types of policies (e.g. named peril property insurance policies), cyber-related losses would normally be excluded unless a cyber incident leads to a named peril such as fire. In other traditional business lines (including all-risk policies and specialty lines), the scope of any coverage for cyber risk may be defined by the use of specific exclusions (although there is limited information on how frequently these exclusions are applied). There are three main types of general exclusions (in addition to individual loss types that may be excluded from individual policies):

- *General exclusion for all losses resulting from a cyber attack:* The Institute Cyber Attack Exclusion Clause CL380 is the broadest exclusion clause, stating that "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system".[1] This exclusion is sometimes - but not consistently - used in property policies, as well as in sectoral specialty line policies (e.g. marine, energy) (Quy, 2014) and appears to provide an exclusion from coverage for all of the main types of losses normally generated by a malicious cyber attack.[2] Another means of excluding certain types of incidents is found in the NMA Information Technology Hazards Clarification Clause and Electronic Data Endorsements 2912. The NMA 2912 exclusion ("endorsement") clarifies that the loss, alteration, damage or reduction in functionality of a computer system, hardware, or software is not considered an insured event (unless it arose from another covered peril (e.g. fire)).

- *General exclusion for losses related to specific types of incidents (i.e. data breach)*: Beginning in 2014, the Insurance Services Office (ISO), which provides standardised forms for insurance policies in the US market, has included the “Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability - Limited Bodily Injury Exception Not Included" in its standard commercial general liability policy forms (these policies, and specifically coverage for "Personal and Advertising Injury Liability", have often been the basis for claims in litigation involving victims of past data breaches). This exclusion states that the insurance will not apply in the case of "Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability" and will not cover "*damages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.*" It further sets out a list of commonly incurred costs related to third party data confidentiality breaches (such as notification expenses, credit monitoring, forensic investigation, etc.) that will not be covered when this exclusion is included (Anderson, 2013a; Aschkenasy, 2013). Liability resulting from bodily injury and property damage, while not specifically listed, might also be excluded based on the second clause (and title) of the ISO exclusion (Watkins, n.d.).

- *General exclusions for specific types of losses (i.e. data and software loss):* There are also general exclusions used to exclude the costs of reinstating damaged, altered or lost data (i.e. data and software loss) such as the NMA Information Technology Hazards Clarification Clause and Electronic Data Endorsements 2914 and 2915 and ISO's Electronic Data Exclusion. The NMA exclusions exclude coverage for *loss, damage, destruction, erasure, corruption or alteration of electronic data from any cause whatsoever*. The ISO Electronic Data Exclusion limits the definition of property damage to damage to *tangible* property where electronic data is not included within the definition of tangible property (Malecki, 2004; Aon, 2013). The robustness of electronic data exclusions have been tested in litigation in the United States - although judgments have been made both supporting and invalidating the exclusions depending on the circumstances of the given event (Anderson, 2013c).

Box 3.1. **Common cyber-related exclusions to traditional policies** (cont.)

In addition, many traditional policies include an exclusion for loss or damage caused by acts of war or terrorism. For example, since 2002 in the United States, standard ISO exclusions have been applied to property and general liability policies that preclude coverage for damages and losses above a certain threshold resulting from acts of terrorism (Woodward, 2002). As a result, damages and losses resulting from cyber terrorism events that meet the definition of acts of terrorism in property and liability policies (as well as any thresholds) could be excluded from coverage.

Responses to the OECD questionnaire provided some anecdotal insight into the use of these general exclusions in various countries:

- Property policies: Respondents from the United States, United Kingdom, Australia and New Zealand indicated that physical asset damage and business interruption losses caused by cyber attack and data and software losses were often excluded from property policies (suggesting use of named peril policies, the general CL 380 or NMA exclusions as well as the NMA or ISO electronic data exclusions). In Australia, standard industrial special risks policies (known as "Mark IV and Mark V") for large businesses exclude property damage resulting from unauthorised access to the insured's computer system (Australian Reinsurance Pool Corporation, 2016). Respondents from continental Europe also indicated that data and software losses and losses other than those caused by physical peril were excluded but that business interruption without material damage may not be excluded. That said, commercial property policies for large industrial risks are rarely standardised and therefore cyber incidents may be treated differently across large commercial policies (Lathrop, 2016). In addition, there are reports that a number of insurance companies have begun eliminating these exclusions from large commercial property policies (i.e. covering cyber risks in large commercial property policies). Finally, the CL 380 exclusion only applies to malicious cyber attacks so some property policies may provide coverage for damage to property (and potentially business interruption) resulting from unintentional information technology failures - unless the policy was written on a named perils basis excluding cyber incidents as a peril (i.e. the property only covered specific listed (non-cyber) perils).

- General liability policies: A number of respondents (especially in the United States and Australia) indicated that losses related to third party data confidentiality breaches (incident response costs, breach of privacy compensation, etc.) as well as inadvertent disruption of third party systems (i.e. transmission of malware and the resulting network security failure liability) are excluded from general liability policies suggesting use of the ISO commercial general liability exclusion or the broader CL 380 cyber attack exclusion in many general liability policies. In the UK market, general liability policies excluded these types of losses in some cases although many traditional policies do not include these exclusions. The exclusions are not generally used in continental Europe either as general liability policies with a pure financial loss extension would be expected to cover these types of losses[3] although in France (and potentially in other European countries) some policies will apply exclusions or other limits on cyber-related losses (Fédération française de l'assurance, 2017).

1. Institute clauses are developed by the "London Market", comprising Lloyd's and the International Underwriting Association.
2. Importantly, the CL380 does not exclude loss, damage or liability resulting from an unintentional system malfunction.
3. Pure financial loss coverage can be added to general liability/professional indemnity policies in continental Europe and elsewhere and provides coverage for liability arising out of events where no physical damage or bodily injury has been caused.

Stand-alone cyber insurance market

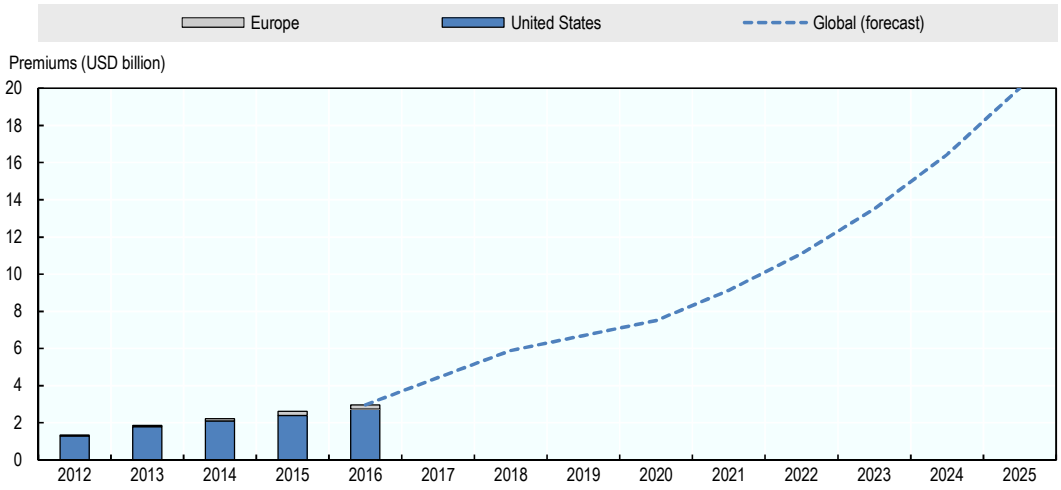
Market size and scope

The size of the stand-alone cyber insurance market in 2016 is estimated to be in the range of USD 2.5 billion to USD 3.5 billion in gross written premiums (which excludes premiums collected for cyber risk coverage included in other policies as companies do not generally provide breakdowns of premiums by individual perils). The US market accounts for an estimated 85% to 90% of all gross written premiums (USD 2.5 billion to USD 3.0 billion) (PwC, 2015; Betterley, 2015; Marsh, 2016b), while the European market is estimated to account for approximately 5% to 9% (USD 150 million to USD 400 million in gross written premiums (Thomas and Finkle, 2014; Marsh, 2016b; Wong, 2017)) - including an estimated EUR 90 million in Germany (Segger and Lorscheid, 2017) and EUR 30 million in France (Thevenin, 2017). Asia-Pacific accounts for approximately USD 50 million in gross written premiums (Wong, 2017).

In many countries, the market is growing at an extremely fast pace with some projecting that it could reach USD 5 billion in the United States (PwC, 2015) and EUR 900 million in Europe (Insurance Information Institute, 2015) by 2018 and USD 20 billion in global premiums by 2025 (Swiss Re, 2017). Based on data from Eling and Wirfs (2016), the global market grew at a compound annual growth rate of almost 25% between 2012 and 2015 and most estimates of the future size of the market predict a similar rate of growth over the next decade (see Figure 3.1). However, it is also possible that the market could grow even quicker. A recent survey by CFC Underwriting, for example, found that more than 40% of respondents had seen growth in their cyber coverage book of more than 50% over 2016 (Hancock, 2017a). There is also substantial room for growth given that the stand-alone cyber insurance market is only a fraction of the size of other markets, despite the high-level of potential exposure to cyber risk (Swiss Re, 2016b). In OECD countries, for example, USD 277 billion in premiums were written for fire and property damage (commercial and residential) and USD 171 billion for general liability insurance in 2015 (OECD, 2017b), relative to the estimated USD 2.5 billion in stand-alone cyber insurance premiums that year.

The level of future demand will depend on the frequency of high-profile cyber incidents as well as the evolving legislative and regulatory environment for privacy protections in many countries. The implementation of the General Data Protection Regulation (GDPR) in the European Union could lead to significant growth in take-up with some reports suggesting that the EU market could eventually equal the size of the US market (Marsh, 2016b).

Figure 3.1. **Estimates of global premium volume**



Source: The premium data for Europe and the United States for 2012 to 2015 is from Advisen, reported in Eling and Wirfs, 2016. The 2016 figure for the United States is the mid-point of estimates by PwC, 2015; Betterley, 2015; Marsh, 2016b. The 2016 figure for Europe is the mid-point for estimates by Thomas and Finkle, 2014; Marsh, 2016b. The projections for the global market are from PwC, 2015 (US, 2018); Insurance Information Institute, 2015 (Europe, 2018); the mid-point of Allianz, Advisen, PwC and ABI as reported in Swiss Re, 2017 (global, 2020) and Allianz as reported in Swiss Re, 2017 (global, 2025). Other years were calculated based on the compound annual growth rate between two projections.

In the US market, cyber insurance coverage is generally available from approximately 70 insurance companies, which may include coverage available on both a stand-alone basis and through cyber-specific endorsements to traditional policies (Harrington, 2017). That said, over 500 companies responded to the US National Association of Insurance Commissioner's most recent "Cybersecurity Annual Statement Supplement" which collects information on premiums collected - and losses paid - for cyber insurance coverage suggesting that a much larger number of insurance companies are providing coverage for some risks that can be interpreted as "cyber" risks. The US market is dominated by a few large providers, including AIG, Chubb and XL Group which account for approximately 40% of the market (Fitch Ratings, 2017). Travelers Companies, Beazley Insurance, CNA Financial, Liberty Mutual, BCS Insurance, Axis Capital and Zurich American Insurance are also significant providers of coverage. According to one recent estimate, approximately 10 companies collect more than USD 100 million in annual written premiums and approximately 10 others collect USD 25 million to USD 100 million in annual written premiums (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

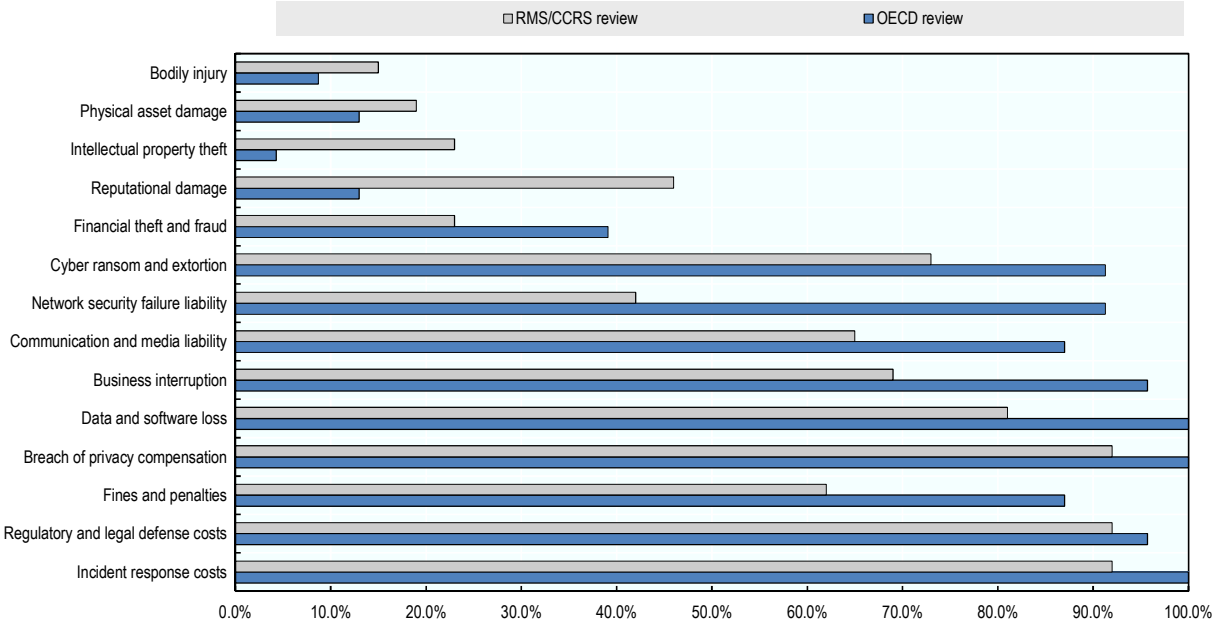
Lloyd's (2016a) has reported that 63 syndicates are writing cyber insurance coverage (GBP 322 million in gross written premiums in 2015), of which more than 80% is earned for providing coverage to US-domiciled companies. In Germany, there are reportedly 15 insurance companies that offer some form of cyber insurance coverage to German companies (up from 4 in 2014), including many of the same companies offering this coverage in the United States (Allianz, AIG, Chubb, XL Catlin, Zurich) as well as AXA, ARAG, ERGO, HDI, Hiscox, Swiss Re, Tokio Marine (List, 2015). According to one report, there were 11 insurance companies offering this coverage in France (Parsoire, 2014). Respondents to the OECD questionnaire revealed that insurance companies are providing stand-alone cyber coverage in Australia, Belgium, Canada, Ireland, Israel, New Zealand, and South Africa. Significant stand-alone cyber insurance markets also exist in

Japan, Singapore and Hong Kong (China) although no responses were received from companies specifically operating in those economies. In India, recent data confidentiality breaches at a number of banks is expected to lead to an increase in companies offering cyber insurance coverage, and also in demand for such coverage (Howard, 2016), with some companies reportedly developing stand-alone products (Advisen, 2017). In mid-2017, two global insurance companies announced a partnership for providing coverage and crisis response services in Brazil (Insurance Journal, 2017i).

Coverage provided

The coverage provided by stand-alone cyber insurance policies for commercial entities (coverage for individuals is described in Box 3.2) can vary significantly across providers, prompting one analyst to suggest that "if you have seen one cyber policy, you have seen one cyber policy" (Nordman, 2012). According to one recent (US-based) estimate, there are at least 65 different policy forms in use for the coverage of cyber risk (Laurie and Vitkowsky, 2017). The abundance of policy forms may be partly due to the common practice of offering a menu of possible coverage options across the same categories of potential losses - allowing policyholders to tailor their policy terms based on their particular level of exposure (e.g. companies that do hold significant amounts of personally-identifiable information are able to secure coverage focused on this cyber risk, as well as business interruption or cyber fraud/theft). Despite coverage differences, there is sufficient convergence to allow companies to seek price quotes for a defined coverage need (Aon, 2013).

Figure 3.2. **Loss categories commonly included in stand-alone policies**



Source: "OECD review" includes: (i) eight policies provided or described in the context of the OECD's survey questionnaire (SHA and Hollard from South Africa; QBE Europe and CFC Underwriting from the United Kingdom; Munich Re (Corporate Solutions) from Germany; General Re from the United States; Zurich Insurance from Switzerland; and Delta Insurance from New Zealand); and (ii) publicly available information on fifteen policies provided by insurance companies, brokers and other related providers (CNA Insurance, QBE North America, AIG , Chubb, ISO, Tokio Marine HCC and XL Catlin from the United States; Tokio Marine Kiln, Marsh, Hiscox and Beazley from the United Kingdom; Hiscox from France; Allianz Global Corporate and Specialty from Germany; and Swiss Re (Corporate Solutions) from Switzerland). "CCRS/RMS review" is from Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) and includes 26 stand-alone policies. In the case of both the OECD review and the CCRS/RMS review, many (but not all) of the policies are those that are made available on a global basis.

Box 3.2. **Cyber coverage for individuals**

While the focus of this study is on the commercial market, cyber risks are also an increasing concern for individuals who could face many of the same types of losses as commercial entities. Identity theft insurance, which provides coverage to individuals for expenses, expert assistance as well as credit monitoring services has been available in many countries for several years (approximately 10 years in the United States) (Cullina, 2017). However, the scope of potential losses that individuals could face is quickly expanding:

- Individuals (particularly high- and mid- net worth individuals) are increasingly targeted by ransomware and fraud attempts (Insurance Journal, 2017d) based on both the increasing amounts of personal information freely available online, as well as through attempts to access personal information that is not publicly available - leading to potential financial losses and costs related to investigating unauthorised access and data restoration;
- Individuals can become victims of social media impersonation which could lead to various types of social engineering (such as solicitations to relatives for money (Cullina, 2017)) and potential liability claims (similar to communication and media liability faced by companies);
- Individuals may fall victim to cyber bullying or other online reputational harm, leading to costs (and assistance needs) to respond to harmful statements; and
- Connected home devices could be affected by malware that causes malfunction. A survey of US consumers found that 10% had been affected by cyber attacks on non-computing home systems and smart appliances, often leading most often to malware infection and/or damage to software or operating systems. Among those affected, 87% faced financial losses including 42% that spent between USD 1 000 and USD 5 000 (Insurance Journal, 2017b).

A number of insurers are beginning to respond to these emerging risks to individuals:

- In Europe, some companies are beginning to offer insurance coverage for e-reputation which provides coverage for identity theft as well as reputational harm resulting from content that is posted online. One company is also considering an insurance coverage for data recovery (which can also be endorsed in some residential property policies).
- In the United States, identity theft insurance is being expanded by some companies to also include coverage for extortion, online fraud and cyber bullying (Carrier Management, 2016a; Insurance Information Institute, 2014; Insurance Journal, 2016a). Insurers are also starting to develop coverage for expenses resulting from cyber attacks on computers and connected devices as well as cyber extortion (Insurance Journal, 2017b). Similar to the commercial market (see section below on "additional services"), a number of insurers are also offering risk mitigation services (Simpson, 2017).
- In the United Kingdom, coverage for cyber bullying is available from some London underwriters and an insurance company while at least one broker and one Lloyd's syndicate are offering coverage for cyber extortion, fraud and social media reputation harm focused on high-net worth individuals.
- In South Africa, at least one insurer is providing liability, extortion and identity theft coverage for individuals.

There is limited information on the penetration of such coverage although some insurers are offering coverage for cyber risks as an endorsement to existing property or other homeowner policies.

Figure 3.2 provides an overview of coverage for different categories of cyber-related losses included in stand-alone policies. The overview is based on responses to the OECD questionnaire as well as an OECD review of selected publicly-available descriptions of

policies from major providers (total of 23 providers based in 7 countries, although often the policies offered are available on a global basis). For comparison, it also shows the results of a similar exercise undertaken by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) of 26 stand-alone policies.

In general, the stand-alone cyber insurance policies provide coverage, either on a standard-basis or as an optional add-on, for most of the main types of losses that could result from the following types of incidents:

- *Data confidentiality breaches:* The **incident response costs**, **regulatory and legal defence costs**, **breach of privacy compensation** and, to a lesser extent, **fines and penalties** that may result from a third party confidentiality breach (often termed a "data breach" or "privacy breach"), are usually covered in stand-alone cyber insurance policies. Most policies were designed with a focus on breaches involving personal data, although many also cover losses related to breaches of third party corporate data (such as the trade secrets of a third party corporate).

  Some policies will not cover **fines and penalties** or will only provide such coverage where permissible by law. This is becoming a more significant issue in the context of the implementation of the GDPR in the European Union which could involve significant fines that may be uninsurable and/or far above the amounts currently provided in cyber insurance policies (Fitch Ratings, 2017; Reactions, 2017).[2]There are also varying levels of coverage for contractual penalties, such as the assessments that could be imposed by payment card networks to recover costs related to card replacement and fraudulent transactions. According to some reports, these Payment Card Industry (PCI) assessments are not normally included in stand-alone cyber insurance coverage despite accounting for a significant component of the cost of responding to a data confidentiality breach involving payment card data (Johnson, 2016). Just over 40% of the policies reviewed provided coverage for PCI assessments (often as an add-on to standard coverage). *System malfunctions:* The **business interruption** losses that might result from a denial-of-service attack (and other system malfunctions) as well as the liability that may be established as a result of an inadvertent disruption to a third-party system (e.g. malware transmission - often referred to as "**network security failure [liability]**") are usually covered in stand-alone cyber insurance policies.[3] Some reports suggest that the business interruption coverage provided in stand-alone cyber insurance policies is less robust than coverage provided in property policies (e.g. more limited scope of coverage, lower limits or no coverage for extra expense) (Johnson, 2016). Among the policies reviewed, just under 60% provided explicit coverage for extra expense (i.e. the additional cost of doing business) which is normally included in property policy coverage for business interruption. Stand-alone policies are also increasingly covering accidental system malfunctions although at least two of the policies reviewed were limited to malicious cyber attacks.

- *Data integrity/availability:* The **data and software** losses resulting from the deletion or corruption of data as well as the **cyber ransom and extortion** losses involved in responding to the encryption of data by ransomware are generally covered.

In the case of **cyber ransom and extortion**, there is some variation in the types of losses covered (e.g. one major provider will only cover costs related to efforts to avoid paying a ransom, not the payment of a ransom itself) as well as whether the coverage includes both incidents and threats of incidents (i.e. whether a ransom payment would be also covered in the context of a threat of harm such as a data confidentiality breach). One impediment to providing insurance coverage for ransom payments is the difficulty in attributing the source of the ransomware and the possibility that the ransom payments could be made to a named terrorist organisation (the International Association of Insurance Supervisors has noted that compensation for ransom payments made to a named terrorist organisation could be considered a violation of United Nations sanctions). Insurance companies may also choose not to provide such coverage in order to be consistent with government policies that are explicitly opposed to making ransom payments in response to kidnapping/extortion.

Malicious activity: The **communication and media [liability]** that could result from the misuse of a system for defamatory purposes (often referred to as "media liability") is also usually covered in stand-alone cyber insurance policies.

However, certain categories of losses that could result from various incident types are less consistently (or even rarely) covered by stand-alone cyber insurance policies:

- *Data confidentiality breaches:* Coverage for breach of the confidentiality of own data (such as trade secrets) was provided in very few of the policies reviewed by the OECD (less than 5%).[4] **Intellectual property theft** is challenging to insure given the difficulties related to valuing lost opportunity (Freedman, 2014; Insurance Journal, 2017j). For example, the theft of a design for a new product or the pirating of a film before its release would very likely cause significant harm to the owners of that intellectual property in terms of lost future revenue although the amount of that loss is extremely difficult to estimate. In the OECD review of policies, only one policy explicitly provided coverage for losses of own intellectual property theft (as an optional add-on to its "standard" coverage). As noted above, the theft of a third party's intellectual property, by contrast, is more commonly insurable and is covered by many of the stand-alone cyber insurance policies reviewed, as the value of any stolen intellectual property would be determined by the value of the claim against the insured (once proven).

  Data confidentiality breaches (and other types of incidents) can also lead to **reputational damage**. A number of stand-alone cyber insurance policies will cover costs aimed at minimising reputational harm (e.g. by covering the cost of engaging a public relations firm) although only a small minority will provide any coverage for lost business resulting from longer term reputational damage (i.e. beyond the period of disruption). It should be noted that the lack of coverage for lost business related to reputational harm is not exclusively an issue for cyber incidents - such coverage is not generally available for other perils either (Freedman, 2014). However, the risk may be more significant in the case of cyber incidents (particularly data confidentiality breaches involving personal information) which have often had negative reputational impacts on those impacted (although, as noted in Chapter 2, these impacts may be declining as acceptance of data breaches increases). Some companies are responding to this gap in coverage by developing specific coverage for loss of revenue with limits of up to USD 100 million (Aon, 2013). Three of the policies reviewed by the

OECD included specific coverage (standard or add-on) for lost profits due to brand or reputational damage.[5]

- *System malfunctions:* Given the general focus of stand-alone cyber policies on addressing losses from data confidentiality breaches (and extortion), **physical asset damage** resulting from cyber incidents has not normally been included in stand-alone policies. This is beginning to change however. In 2013, a Lloyd's syndicate began offering coverage for physical damage (including for data restoration) and business interruption losses resulting from a cyber attack to supervisory control and data acquisition (SCADA) control systems (i.e. systems that monitor and control processes, commonly used in the electricity and other utility sectors) (JLT Mining, 2014). Another Lloyd's Managing General Agent has begun providing specific coverage tailored towards cyber risks to industrial systems and operational technologies with the potential to cause physical damage (Cohn and Saul, 2017). One company began offering up to USD 100 million in coverage for property damage caused by cyber attack in 2014 (on a primary, excess or difference-in-conditions basis) with other insurers also indicating an interest in providing such coverage (Basak, 2015). In the OECD review of policies, only three of the policies examined offered coverage for physical asset damage. Similarly, few stand-alone cyber insurance policies provide coverage for **bodily injury** resulting from a cyber incident. The OECD review identified two policies that offer such coverage while the CCRS/RMS review identified approximately four providers with one company reportedly offering up to USD 100 million in coverage for bodily injury (Basak, 2015).

  Business interruption resulting from the disruption of a third party digital service provider (i.e. **contingent business interruption** in a cyber context) is covered by one third of the policies examined by CCRS/RMS. The OECD questionnaire did not seek specific information on this category of losses although the review of policy documents identified only one that provided coverage for this type of loss and only in the case of a cloud service provider disruption. The inclusion of sub-limits on contingent business interruption coverage is also common. In the cloud service failure scenario developed by Lloyd's and Cyence (2017) (see Box 4.1), sub-limits ranging from 20% of annual revenues for small companies to 50% for large companies were used to reflect this market practice.

- *Malicious activity*: Less than half of the policies reviewed by the OECD (and less than a quarter of the policies reviewed by CCRS/RMS) provided coverage for **financial theft and fraud**. The low level of coverage may be because many traditional crime policies provide coverage for financial theft without any exclusion of cyber-related incidents (therefore limiting the need for coverage in stand-alone cyber insurance policies) (ABI, 2016). Some stand-alone cyber policies that do provide coverage for financial theft and fraud have developed coverage specifically for social engineering fraud (i.e. theft resulting from the impersonation of a responsible executive within an organisation with instructions to transfer funds or provide access credentials) (Ydstie, 2015) as there may be exceptions to coverage of this type of fraud under traditional crime policies limited to unintentional acts (as a transfer of funds, even where initiated under false pretences, still involves an intentional act by an employee - which has led to numerous claims disputes).[6] At least one major broker has also developed specific coverage to bridge the gap between crime/fidelity and stand-alone cyber policies

(Carrier Management, 2016b) while one company has started offering excess coverage for social engineering fraud (Insurance Journal, 2017k).

Stand-alone cyber insurance policies also make varying use of the terrorism exclusion that is normally included in other types of commercial policies (although all policies continue to include a war exclusion). Some of the policies reviewed by the OECD were silent on the coverage of terrorism (i.e. did not specifically exclude (or include) terrorist acts as an insured peril). In two policies, a specific terrorism exclusion was included in the policy although cyber terrorism was carved-out of that exclusion. In one policy, affirmative coverage is provided for business interruption resulting from an act of terrorism. According to Allianz Global Corporate and Specialty (2016), the insurance industry has been eliminating terrorism exclusions from cyber insurance coverage in recognition of the challenges of attributing individual cyber incidents. This has potential implications for the coverage provided by terrorism insurance programmes established in a number of countries (see Box 4.2).

These findings are consistent with other analyses of the coverage provided by the stand-alone cyber insurance market (Aon, 2013; Cyber Risk Insurance Forum, n.d.; IRT System X, 2016; ENISA, 2016) and also confirm that stand-alone cyber coverage is responding to many of the gaps in coverage that have emerged in traditional policies (damage to intangible assets, business interruption without material damage, etc.). It should be noted that no significant divergence in the coverage offered by stand-alone policies across different regions was observed which may be because many policies are offered on a global basis.

Penetration of stand-alone cyber insurance

Estimates of the penetration of stand-alone cyber insurance coverage vary widely. Most estimates are based on responses to surveys of what can be very different business communities. These surveys also formulate questions in a way that could lead to disparate responses. For example, a survey might specifically ask about the take-up of stand-alone cyber insurance coverage or, more generally, might ask whether the company has insurance coverage for cyber risks - which could lead to very different estimates of the share of companies that have actually purchased stand-alone cyber insurance policies or endorsements.

Estimates of cyber insurance penetration rates across countries generally find higher levels of penetration in the United States than in the United Kingdom, continental Europe or Asia-Pacific (no information on penetration levels outside of these countries was found):

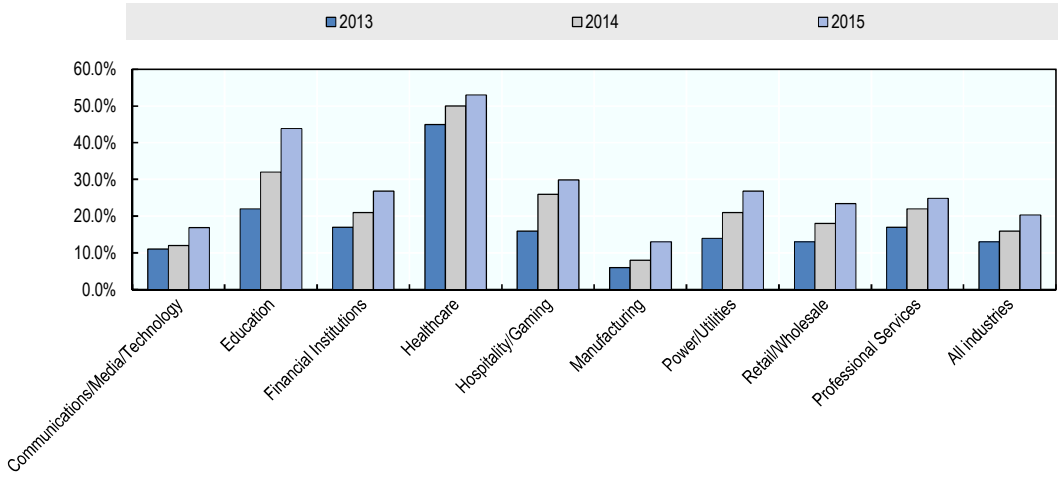
- In the United States, some estimates suggest that approximately 20% to 35% of all companies have specific cyber insurance coverage (PwC, 2015, S&P Global Market Intelligence, 2015; Council of Insurance Agents & Brokers, 2017) although other more recent reports have found higher penetration levels, from 55% (Hiscox, 2017) to 65% (up from 35% in 2011) (Advisen, 2016). According to one estimate, approximately 72% of companies with coverage for cyber risks purchase stand-alone coverage (up from 64% in 2015) while 28% rely on coverage in existing policies (including through endorsements) (Council of Insurance Agents & Brokers, 2015a and 2017).

- In the United Kingdom, estimates of penetration range from less than 2% (Z/Yen Group, 2015) to 20.6% (Marsh, 2016c) to 36% (Hiscox, 2017) to 38% of companies (Department for Culture, Media and Sport, 2017).
- According to Marsh (2016b), 24% of organisations in continental Europe had purchased, or were in the process of applying for, cyber insurance coverage in 2016 (up from 20% in 2015). Hiscox (2017) found a penetration level of 30% among German companies in its survey. A recent estimate suggested that penetration among the largest companies in France was close to 60% to 70%, falling to 40% among mid-to-large companies and 2% to 3% among SMEs (Thevinin, 2017).
- There are fewer estimates about the level of penetration of cyber insurance coverage in Asia-Pacific although Chubb has suggested that it is below 1% (Wong, 2017).

Penetration is reportedly higher among health, education, retail and technology companies (approaching 50% (PwC, 2015; Insurance Information Institute, 2015) or even 80% in the US retail healthcare and financial services sectors according to some surveys (Council of Insurance Agents and Brokers, 2016b; Advisen, 2016)). A global insurance broker, Marsh, publishes take-up rates for stand-alone cyber insurance and growth in take-up rates by sector among its brokerage clients (with a concentration of US companies). According to its estimates, take-up rates are highest in the healthcare, education and hospitality and gaming sectors (see Figure 3.3). The increasing availability of coverage for business interruption and other first party costs is driving increasing demand in sectors less concerned with third party (personal) data confidentiality breaches. For example, there are some reports that cyber insurance purchasing by manufacturing firms almost doubled between 2015 and 2016 (Insurance Journal, 2017a).

Some of the insurance companies and brokers that responded to the OECD questionnaire provided details on the types of companies that have purchased cyber insurance coverage. In the United States, respondents noted demand from all sectors of the economy although with some variation in terms of the type of coverage being sought (i.e. those holding significant amounts of personally-identifiable information were most concerned with coverage related to a third party data confidentiality breach whereas sectors such as manufacturing were more concerned with business interruption, intellectual property theft and extortion and fraud coverage). Among respondents from the United Kingdom, policyholders were generally concentrated in the retail, healthcare, and financial services sectors, although companies in other sectors also purchase cyber insurance coverage. Larger companies account for a larger share of all policyholders among respondents from continental Europe, in many of the same sectors identified in other countries/regions (with the addition of the communications, media, technology and hospitality sectors). For respondents from other countries (Australia, Canada, New Zealand and South Africa), the distribution of policyholders was also concentrated in retail, healthcare, technology and financial services as well as among professional services companies (such as law firms) which could be targeted for information on strategies or acquisition plans of their larger clients.

Figure 3.3. **Estimated stand-alone cyber insurance take-up rates by sector (Marsh clients)**



Source: Marsh (2015b) reported take-up rates in 2013 and 2014 among its clients. Marsh (2016a) only reported growth in take-up among its clients so the estimated take-up rate in 2015 is derived from reported growth rates.

Most surveys have found a much lower level of coverage among SMEs - for example, a survey of US small businesses (10 or fewer employees) in April 2015 found that only 5% had cyber insurance coverage (Endurance International Group, 2015). There is some evidence that coverage levels among SMEs are increasing. The recent Advisen (2016) survey, for example, also found a high-level of penetration among smaller firms. In the United Kingdom, one study found that the penetration of cyber insurance among SMEs had increased from 2.1% in 2014 to 13.7% in 2016 (Hancock, 2017b). In the United States, the penetration rate for cyber insurance among small companies reportedly increased 26 percentage points between 2011 and 2016 (Advisen, 2016). More than 95% of the 22 insurance companies and brokers that provided details on the characteristics of their clients indicated that they have - or are developing - specific products tailored to the needs of smaller businesses (lower limits, less extensive underwriting process). SMEs accounted for 50% or more of policyholders for approximately 60% of the 14 companies that provided breakdowns of their portfolio by size of companies.

Level of coverage

The most common level of coverage available from a single insurer for a single policyholder is estimated to be around USD 25 million (Council of Insurance Agents & Brokers, 2015a), although some individual companies and joint ventures are reportedly willing to offer coverage of USD 75 million to USD 100 million to certain individual clients (Finkle, 2015; Insurance Journal, 2017a; Faulkner, 2017).

Among respondents to the OECD questionnaire, four insurance companies indicated that they had capacity to provide coverage of more than USD 25 million while seven indicated a maximum available level of coverage between USD 5 and USD 15 million. For larger companies, coverage towers involving a number of insurers can be constructed with reported limits as high as USD 700 million for most industries and up to USD 500 million for the financial services, retail and healthcare sectors (Marsh, 2014). In 2017, a USD 600 million tower for stand-alone coverage was reportedly developed with the involvement of 40 cyber underwriters (Hemenway, 2017). Coverage limits do not

vary significantly across regions as limits of up to EUR 500 million have been reported as possible, for example, in Germany and Austria (List, 2015). A major broker has also launched a product aimed at providingGBP 500 million in cyber insurance coverage to mid- to large-sized companies outside the United States (Insurance Journal, 2017c).

The average coverage limit purchased in 2016 among Marsh (mostly US-based) clients was USD 16.9 million, up from USD 11.3 million in 2013. This is much higher than the average coverage limit of USD 6 million reported by the Council of Insurance Agents and Brokers (which has doubled since October 2016) (2016a, 2016b, 2017) and theGBP 1 million toGBP 5 million in coverage limits that have been commonly purchased in the United Kingdom (as reported in 2012) (Airmic, 2012). In France, most companies seek limits of USD 25 million or less while SMEs will normally purchase EUR 150 000 to EUR 200 000 in coverage. In Europe more generally, a survey of risk managers found that 25% of responding companies purchased less than EUR 50 million in cyber insurance coverage, 7% purchased between EUR 50 million and EUR 100 million in coverage and 5% purchased more than EUR 100 million in coverage (FERMA, 2016).

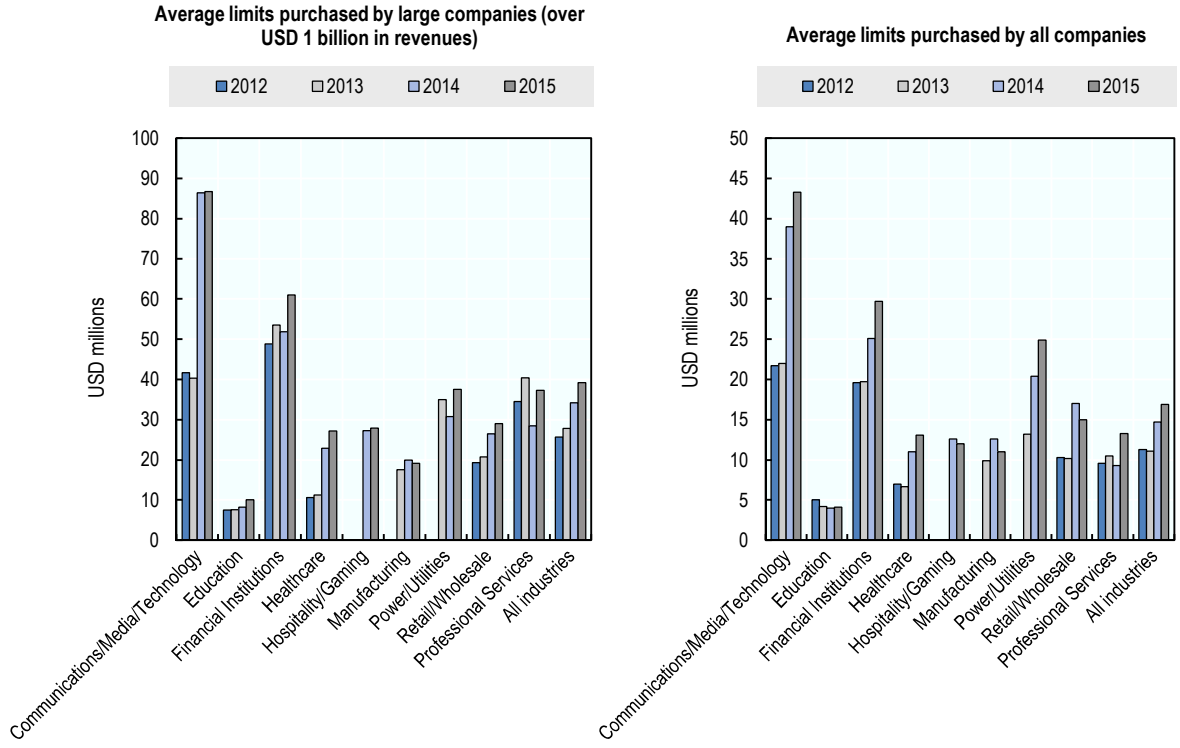
On average, most companies are not purchasing limits near the reported maximum coverage levels available although large companies in some sectors are purchasing more than what is normally available from a single insurer for a single client. Among Marsh clients, coverage limits purchased have been generally increasing annually although with some signs of recent stabilisation among large companies in those sectors that have been purchasing the highest limits (communications/media technology and financial institutions) (see Figure 3.4). The Council of Insurance Agents and Brokers survey (2016b) of US brokers also found that US companies were generally increasing their coverage limits (and that the share of companies increasing their levels of coverage accelerated in the second half of 2016). Despite the growth in the amount of coverage purchased, limits remain well-below comparable policies covering property risks. For example, a typical US company with revenues over USD 5 billion would normally purchase over USD 500 million in property coverage (Lathrop, 2016).

Most reports on the adequacy of coverage limits (focused on the US market) have found sufficient capacity for smaller companies that typically purchase about USD 25 000 in coverage (S&P Global Market Intelligence, 2015), particularly in sectors that have been generally less targeted by cyber attacks. However, companies in high-risk sectors such as health care, education (and to a lesser extent, retail, financial services, technology and hospitality) have reportedly faced capacity constraints as a result of reduced offers of coverage and the exit of some providers in the aftermath of large data confidentiality breaches (Betterley, 2015; Council of Insurance Agents & Brokers, 2016a; Council of Insurance Agents & Brokers, 2016b; Council of Insurance Agents & Brokers, 2017; Sclafane, 2015). PwC (2015) suggests that most large companies have difficulty securing anything above USD 300 million in coverage. According to a recent survey of companies worldwide, 16% indicated that they had purchased the maximum amount of coverage available on the market (Ponemon Institute, 2017).

Some insurers are also placing sub-limits on component parts of the policy coverage and/or imposing deductibles. Among OECD questionnaire respondents, full limits were generally offered for each sub component. Typical reported deductibles in the US market range from USD 5 000 to USD 100 000 for smaller companies and USD 250 000 to USD 10 million for larger companies (Aon, 2013) (although Anthem Insurance reportedly faced a USD 25 million deductible on USD 100 million in insurance coverage

after being impacted by a major data confidentiality breach in 2015 (Finkle, 2015)). OECD questionnaire respondents reported similar ranges for deductibles although some companies offer deductibles below USD 1 000. Most respondents indicated that they would vary deductibles with the level of risk while many insureds also seek higher deductibles in order to reduce the cost of insurance (Sclafane, 2015). Business interruption coverage usually includes a minimum outage time deductible of between 8-to-12 hours (with a shift towards lower time deductibles) although some respondents to the survey offered coverage from 6 hours onwards while others offered coverage only after 24 hours or longer (some business interruption coverage is offered without a time deductible, replaced with a higher value deductible in its place). A survey of cyber insurance policies in Sweden found a wide variety of time deductibles imposed, including a 2-hour deductible provided by one insurer on a negotiated basis (Franke, 2017).

Figure 3.4. Cyber insurance limits purchased by large and all companies (Marsh clients)



Source: Marsh (2014, 2015b, 2016a)

Pricing

A limited amount of information is available on the cost of cyber insurance coverage in different countries and sectors, and for companies of different sizes:

- A 2013 report by Aon indicated that, in the United States, the price of USD 1 million in coverage ranged from USD 5 000 to USD 10 000 for smaller firms to USD 10 000 to USD 50 000 for large firms with an average cost of about USD 10 000 to USD 25 000 per USD 1 million in coverage (Thomas and Finkle, 2014). One brokerage firm that responded to the OECD questionnaire indicated

that prices are now significantly lower for smaller US firms, with premiums starting below USD 1 000 for USD 1 million in coverage. This is consistent with another recent estimate of premiums of USD 5 000 to USD 7 000 for a "comprehensive policy" to meet the needs of companies with USD 5 million to USD 8 million in revenues (Tsangaris, 2016). One company offered a USD 100 000 estimate of the cost of USD 10 million in coverage for energy companies against data breach incidents (and up to USD 700 000 for USD 10 million in coverage that includes physical damage) (Saul and Cohn, 2017).

- A 2012 report by Airmic (a group representing risk managers, usually from larger firms) estimated the price ofGBP 1 million in coverage in the United Kingdom to beGBP 30 000 whileGBP 10 million in coverage would normally be priced atGBP 15 000 per million (orGBP 150 000 in total forGBP 10 million in coverage).

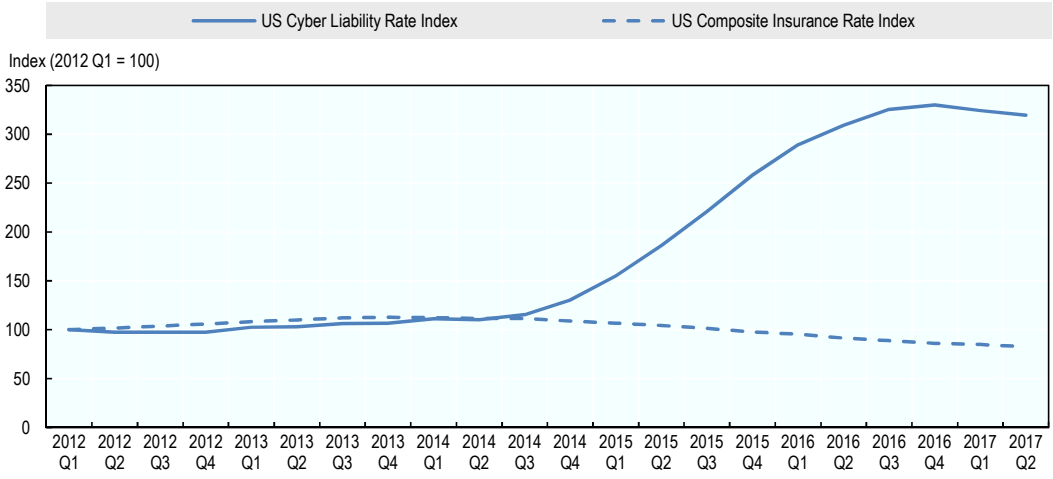
- In Europe, the cost per EUR 1 million in coverage is approximately EUR 2 000 to EUR 5 000 for EUR 50 million to EUR 90 million in coverage (Thomas and Finkle, 2014). In Germany, the reported cost of EUR 1 million in coverage ranges from EUR 7 000 to EUR 15 000 while the cost of EUR 5 million in coverage ranges from EUR 4 000 to EUR 24 000 per million (List, 2015). The survey of policies offered in Sweden found a cost ranging from SEK 5 000 to SEK 15 000 per SEK 1 million in coverage although with some coverage available for less than SEK 5 000 per SEK 1 million (Franke, 2017).

The cost of cyber insurance coverage is expensive relative to other types of insurance coverage - it has been reported that cyber insurance coverage (for the same amount of coverage) is three times more expensive than general liability coverage (PwC, 2015) and six times more expensive than property coverage (Z/Yen Group, 2015). There is also some evidence that the cost of cyber insurance has been increasing more quickly, leading to a widening gap in the cost of cyber insurance relative to commercial property and casualty insurance. The cost per million of cyber liability insurance has increased by over 200% since Q1 2012 relative to a 17% decline in US commercial property and casualty pricing (on a composite basis - see Figure 3.5). However, there are recent signs of a stabilisation in pricing After large increases in 2015, rates stabilised in 2016 and declined in 2017 in the United States for most companies (only 15% of companies surveyed by the Council of Insurance Agents and Brokers (2017) indicated that they had faced price increases in the first quarter of 2017 while 31% saw a decline in rates charged). Pricing for SMEs has generally been more stable as a result of higher levels of competition in that market (Betterley, 2015). . Some reports have suggested that pricing for cyber insurance is relatively flat as a result of the limited ability of insurance companies to differentiate across risks (Swiss Re, 2017). However, reports on pricing in the United States indicate some differentiation. For example, in 2015, increased prices for cyber insurance particularly targeted the US health care and retail sectors (ranging from a 10% to 200% increase in the cost of coverage in 2015 (Betterley, 2015)), as a result of major breach experiences and differing values for the personally-identifiable data held by health care and retail companies (i.e. the higher value of health care information and social security numbers) (Marsh, 2015a; Sclafane, 2015; Betterley, 2015).

Several respondents to the OECD questionnaire indicated that they also differentiate premiums based on the level of cyber security. For example, London market respondents indicated that credits or premium discounts are sometimes provided for compliance with

standards, audits, penetration tests as well as staff training initiatives. Broker respondents from other countries also suggested that security factors played an important role in pricing (and that they often helped their clients improve security practices before seeking insurance quotes). In Sweden, many of the insurers providing cyber insurance coverage take security parameters into account and vary premiums accordingly (Franke, 2017). In addition, some retail and healthcare organisations have reportedly been able to avoid premium increases imposed on other organisations in their sector based on better security controls (Willis Towers Watson, 2017).

Figure 3.5. **US Commercial and Cyber Insurance Price Indices**



Source: OECD calculations based on rate changes reported by Marsh (2017) (2012 Q1=100).

There is also some evidence that uncertainty about the level of exposure could be leading to relatively high levels of variation in pricing (Taylor, 2017). 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 while a pharmaceutical company in the United States was quoted premiums that varied by 300% for a defined set of coverage (Sclafane, 2015).

Underwriting approach

The underwriting of insurance coverage is based on an analysis of the probability that covered incidents of different severities might occur (taking into account the level of protection) and the implications in terms of claims payments (taking into account the level of retention). This kind of analysis can provide various estimates that insurance companies use when establishing prices, including average annual loss and probable maximum loss. These kinds of assessments are usually based on historical experience in terms of the frequency and severity of incidents combined with expert judgement and/or scientific evidence that allow for adjustments to be made to account for changes in frequency or severity (such as, for example, a changing climate in the context of natural hazards, or a material development in terms of preventative technology).

The limited availability of data on cyber incidents (and the evolving nature of the risk itself - see Chapter 4) has made it difficult to develop full probabilistic models for use in pricing cyber insurance cover. While a few insurance companies, brokers and other

companies (see Chapter 5) have developed pricing models that provide probabilistic estimates of potential losses, the vast majority of insurers continue to use deterministic or scenario-based approaches for estimating the potential frequency and severity of cyber incidents. Assessments of frequency and severity are usually based on publicly available data on past incidents, enhanced by the underwriter's own claims experience. There are a few commercial companies that collect and market data on past incidents and at least one annual report that provides an overview of claims experience based on data provided by a number of insurance companies (see Chapter 4).

In the case of data confidentiality breaches, data on past breaches provides insurance companies with a basis to assess the level of risk based on different company characteristics (e.g. size, sector, geographical footprint) and estimate the per record cost of a breach (as noted in Chapter 2, these costs can vary depending on the type of record, the number of records stolen and other factors). Therefore, part of the underwriting process involves understanding the business activities and number and types of information records held by the company. Given the longer experience with data breach notification laws and the more developed stand-alone cyber insurance market, much of the available data is based on experience in the United States.

Insurance companies also focus significant attention on the company's security practices and policies, depending on company size and amount of coverage being sought. For smaller companies/coverage amounts, the underwriting process will focus on basic cyber security practices such as use of a firewall, anti-virus/malware software and data encryption, as well as frequency of data backups and use of intrusion detection tools. In some cases, applications may ask about compliance with specific standards, such as the International Organization for Standardization/International Electrotechnical Commission standard on Information Security (ISO/IEC 27001); the US National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*; or the UK *Cyber Essentials*. Companies that hold payment card information might also be asked about their compliance with the *PCI Data Security Standard* while US companies with health records might be asked about their compliance with *Health Insurance Portability and Accountability Act* security requirements. Some stand-alone cyber insurance applications also request information on plans and policies, such as data protection policies, network access policies, internal auditing policies, disaster recovery plans, etc., as well as governance processes in place for those policies (leadership, frequency of update, etc.). Information on outsourcing of information technology and other operational services is also commonly sought as part of the application process. Larger companies (or companies seeking larger limits) would face additional scrutiny, potentially involving on-site interviews, security audits and/or penetration testing. Risk and vulnerability assessments by external security consultants are offered by some companies as an additional service included as part of the insurance policy (see next section).

Insurance companies use the information gathered through the underwriting process to determine premium levels (or whether to provide coverage at all). Some insurers may also establish minimum security standards that must be maintained through the coverage period in order for coverage to be maintained, such as timely patching of vulnerabilities and/or other software updates (although these types of requirements are usually discouraged by brokers and prone to claim disputes). The May 2017 "WannaCry" ransomware attacks, which capitalised on a vulnerability for which a security patch had been made available (see Box 2.8), may offer a test of the validity and relevance of these types of requirements.

Robust underwriting of cyber insurance coverage can contribute to reducing cyber risk at an aggregate level by disseminating and ensuring compliance with good security practices (similar to the market for large commercial property coverage where insurance companies play a valuable risk consulting role (Betterley, 2015)). A survey of US security professionals in early 2016 found that 91% of companies had to make adjustments to their security practices or policies in order to secure cyber insurance coverage, including implementing and updating policies and processes, acquiring new technical controls and/or implementing a data/information governance programme (Filkins, 2016). However, efforts to gain market share based on lower underwriting standards could undermine this contribution (there are some reports that certain sectors in the United States are being underwritten with very little review (Council of Insurance Agents & Brokers, 2016b)).

There are also significant concerns related to the level of information available to underwriters - which could have implications for the quality of underwriting. Insurers have raised concerns about access to information on security controls while some risk managers are sometimes impeded from providing underwriters (or their security consultants) with the full access they seek due to concerns about providing access to sensitive data (Airmic, 2012).

Additional services provided with stand-alone policies

In addition to providing insurance coverage for the expenses incurred as a result of a cyber incident, many insurance companies provide additional services with their policies, either as risk management advice during the underwriting process, as a means to reduce vulnerability to cyber incidents during the period of coverage or in order to reduce the impact of cyber incidents that occur. The first two types of services are often referred to as pre-breach services or risk mitigation services while the latter type is identified as post-breach or response services. Some insurance companies have developed significant internal expertise and offer these types of services directly, while others have developed networks and/or partnerships with a variety of service providers, often involving some form of discounted pricing for its policyholders (e.g. information technology security consultants, legal firms, public relations firms, etc.) (see Figure 3.6).

As noted in the previous section, some insurance companies provide specific risk assessment services as part of the underwriting process (sometimes even if no insurance coverage is entered into) ranging from online or onsite security assessments to advice on security policies and practices, to vulnerability scans and penetration testing which should benefit both the insurance company and the company's risk management (Insurance Information Institute, 2014; Carrier Management, 2016d). Insurance companies are also offering an assortment of risk mitigation services during the coverage period, including threat and intelligence warnings and detection, access to specialised protection technologies, preparation and testing of contingency plans, helplines or information portals and employee training (Betterley, 2015; Swiss Re, 2017; Wells Fargo Insurance Services, 2016; Insurance Journal, 2017e).

A range of services for managing the impact of a cyber incident are also being offered, including forensic investigative services necessary to identify the source of any breach, legal assistance to help manage legal and regulatory requirements and potential liability, providers of call centre capacity, notification services, credit monitoring and/or identity theft protection to support interaction with affected clients, and public relations companies to minimise the reputational impact of cyber incidents (Betterley, 2015; Swiss Re, 2017; Insurance Journal, 2017e).

Figure 3.6. **Additional services offered with stand-alone cyber insurance policies**

According to one survey, 70% of insurers provide (or plan to provide) cyber risk mitigation or response services (Swiss Re, 2016a). Seventeen of the 23 policies reviewed by the OECD advertised access to risk mitigation and/or response services, including (among other services):

1. in-house risk management advice (35%);

2. specific external risk mitigation services such as periodic penetration testing, table-top exercises, assessments of security practices, or back-up cloud storage (30%); and

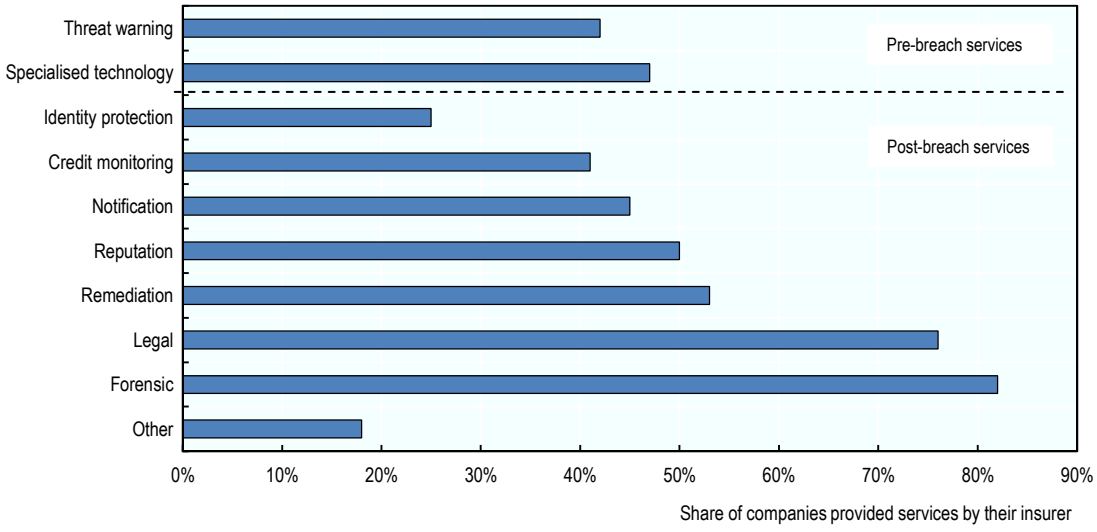
3. response service providers including forensic investigators and legal assistance (66%), public relations advisors (60%); call centre providers (30%), credit monitoring services providers (20%), notification services providers (13%) and even data restoration services (7%).

A recent survey found that a large proportion of companies have access to various response services through their insurance provider and that 40% to 50% have access to risk mitigation services (see Figure 3.7).

There is some evidence that companies see value in these additional services (Swiss Re, 2016a). A survey found that a large share of companies use external providers for risk mitigation and response services, particularly 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 (Advisen, 2016). Some surveys have found that additional service offerings (risk mitigation and response together) are as important as risk transfer in motivating insurance purchase among US SMEs (Council of Insurance Agents & Brokers, 2016c) and are also the most important driver for more than 30% of large US companies (Council of

Insurance Agents & Brokers, 2017). These services might also have a positive impact in terms of reducing the cost of responding to breaches (by as much as 30% according to one estimate (NetDiligence, 2015)). One report suggested that companies without access to these services could pay as much as three times more for the same service (and without the benefit of knowing that the service provider has been previously vetted by the insurance company) (Donlon, 2015).

Figure 3.7. **Companies provided with risk mitigation and response services by their insurer**



Source: Ponemon Institute, 2017

Coverage for cyber-related losses in existing (traditional) policies

As noted above, some insurance coverage for losses resulting from cyber incidents may exist in traditional insurance lines, including property, general liability, directors and officers, errors and omissions/professional indemnity, crime and all-risk policies for owners of small businesses (known as "business owner's policies" in the United States or "business pack" policies in Australia) (Simpson, 2016a) (see Figure 3.8) and potentially even in individual homeowner policies (see Box 3.2). The inclusion of this coverage may be explicitly understood by the insurance companies that are providing it (as well as the policyholders) - through the inclusion of a specific endorsement or, potentially, an intentional decision not to apply one of the common exclusions for cyber-related incidents. For example, many insurance companies will specifically provide endorsements of some of the exclusion clauses described in Box 3.1 above. In other cases, cyber losses may be implicitly covered under traditional policies and only "discovered" as a result of claims disputes and/or litigation. The following provides some examples of how cyber-related losses may be explicitly or implicitly covered in traditional policies:

- *Property insurance policies*: As noted above, property insurance policies may exclude losses resulting from a cyber incident through the use of named perils policies or general exclusions covering all cyber attacks (i.e. CL 380) or all events resulting from loss, alteration, damage or reduction in functionality of a computer system, hardware, or software (i.e. NMA 2912).[7] They may also

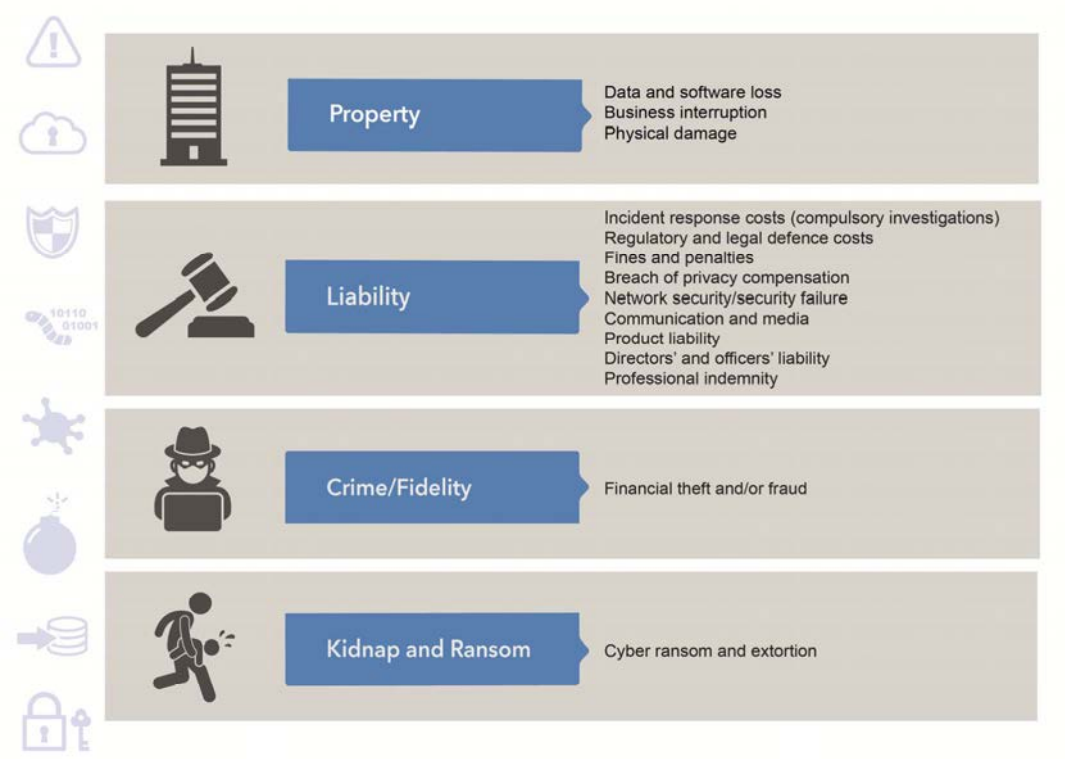
exclude coverage for damage to intangible assets (ISO Electronic Data Exclusion and NMA 2914 and 2915). At least one insurance company or broker respondent from each of the main markets represented in the responses (United States, United Kingdom, continental Europe, Australia, New Zealand and South Africa) indicated that losses due to business interruption without material damage and data losses were excluded in traditional policies, suggesting some use of named peril policies and/or exclusions in all of these markets.

However, the increasing recognition of the potential for physical asset damage and business interruption to result from cyber incidents and the need for coverage of intangible assets has led some providers to specifically include such coverage in traditional policies. For example, some property policies are offering endorsements based on these exclusions, thereby reinstating coverage that would have otherwise been excluded (according to the Insurance Information Institute (2014), property policies often include these endorsements). Also, if not specifically excluded, it is possible that insurance coverage for cyber-related losses (e.g. property damage, data restoration or business interruption caused by a cyber incident) could be found in all-risk property insurance policies. Traditional policies will usually have larger limits for property damage and business interruption than those available in stand-alone cyber policies which means that coverage (and exposure) for these losses could be higher in traditional policies without exclusions (property policies regularly provide limits of USD 500 million or more which would be an exceptional level of coverage for a stand-alone cyber insurance policy (Marsh & McLennan Companies, 2016)).

- *General liability policies*: A number of different types of liability coverage provided in stand-alone cyber insurance policies could potentially be found (or might still be found) in general liability policies, particularly network security failure liability and communication and media liability. Prior to the use of exclusions (as described in Box 3.1 above), implicit coverage of breach of privacy compensation had been found through litigation in the United States (although not consistently).[8] Physical damage (and bodily injury) caused to a third party are also usually included in general liability policies.

  Many general liability policies now exclude claims related to many types of cyber incidents. In the United States, the exclusion is focused on liability resulting from data confidentiality breaches involving third party personal or commercial information although, as noted in Box 3.1, the exclusion may also apply to physical damage and/or bodily injury liability related to a cyber incident. A specific exclusion of liability related to data confidentiality breaches is less common in the United Kingdom and continental Europe (where there is limited experience in finding liability for breach of privacy). That said, at least one insurance company and/or broker respondent from each of the main markets indicated that exclusions related to both data confidentiality breaches and virus transmission were applied in general liability policies. As in the case of property policies, some insurers will allow for coverage of cyber risks to be added back into general liability policies as an endorsement, although often with sublimits and restrictions on the types of expenses covered (Betterley, 2015; Lloyd's and Cyence, 2017).

Figure 3.8. **Potential coverage for cyber risk in traditional policies**



Source: Adapted from OECD (2017a)

- *Directors and Officers liability policies*: Companies impacted by a significant cyber incident with implications for business performance could face lawsuits from shareholders over the role of company executives or the company's board in ensuring appropriate management of cyber risks (including response to a breach and, for US public companies, the level of risk disclosure relative to the SEC's disclosure guidance) (Augustinos, Deem and Kamaiko, 2014) - although so far, such lawsuits have rarely led to findings or settlements in favour of shareholders in the United States (Vitkowski and Laurie, 2017). In New York State, a director or senior officer of a financial institution is now required to certify compliance with the state's *Cyber Security Requirements for Financial Services Companies* which could provide a new avenue for shareholder claims (Carrier Management, 2017).

  Currently, there is no general exclusion of cyber-related losses in directors and officers policies which suggests that such losses would normally be covered. However, some analysts believe that an exclusion for application in directors and officers policies will likely be developed with some anecdotal evidence that individual companies may be aiming to exclude cyber risks from individual policies (e.g. through the use of a clarification letter) (Barker, 2016). In other cases, insurance companies are affirming (or enhancing) the coverage of cyber incidents in their directors and officers policies (Insurance Journal, 2017f). The importance of this issue outside of the United States is likely to increase due to: (i) the spread of securities (and other) class action lawsuits to the United Kingdom, continental Europe and countries in Asia (Randall, 2017); (ii) the

recent precedent of large (USD 1 billion) directors and officers settlements in the United Kingdom (LaCroix, 2017); and (iii) the implementation of the General Data Protection Regulation (GDPR) in 2018 which should lead to more widespread publication of data confidentiality breaches in Europe (CGI Group, 2017). The GDPR requires the establishment of a Data Protection Officer with responsibilities that could lead to liability and some insurers have accordingly extended their definition of insured persons to include Data Protection Officers.

- *Errors and Omissions liability/Professional Indemnity policies*: In terms of cyber risks, errors and omissions/professional indemnity policies are mostly (although not only)[9] relevant for technology companies who may be found liable for damages should the professional services (technology) that they provide play a role in a damaging cyber incident for one of their clients (e.g. in the case where the technology provided included vulnerabilities that were later exploited). Cyber liability is usually excluded from the errors and omissions policies offered to technology companies in the United States but can be added through an endorsement (Insurance Noodle, n.d.). For example, one company has begun offering coverage for data confidentiality breaches and malware transmission to its professional liability products for some professions (e.g. architects and engineers) (Carrier Management, 2016c). Professional indemnity/liability policies in Australia, New Zealand, the United Kingdom and many other countries normally include coverage for cyber incidents. In continental Europe, at least one company has started specifically including some cyber-related liabilities (communication and media liability due to online publishing) in its professional indemnity coverage (Insurance Journal, 2017g).

- *Crime (fidelity):* As noted above, crime or fidelity insurance policies often provide coverage for cyber fraud/theft (Insurance Journal, 2017h). However, traditional crime policies may consider the act of transferring funds, even under fraudulent circumstances, an intentional act by a company's employee that is excluded from coverage - which has led to the inclusion of specific social engineering coverage in some stand-alone cyber insurance policies.

- *Kidnap and Ransom*: The costs related to addressing a ransomware attack (including, in some cases, a ransom payment) could be covered by a traditional kidnap and ransom policy where the definition of an insured event includes a threat to damage or destroy data or insert a malicious code in a computer network (Weyland, 2016) and many providers of traditional kidnap and ransom insurance provide some coverage for cyber extortion (Wells Fargo Insurance Services, 2016). However, the increase in ransomware attacks is leading some to amend their policy language to exclude coverage for costs resulting from ransomware attacks, impose specific deductibles for ransomware incidents and/or limit coverage for some of the losses that may be caused by ransomware, such as business interruption (Barlyn and Cohn, 2017).

- *All-risk/business owner's policies*: Many smaller companies and certain types of companies (e.g. construction contractors) use all-risk insurance policies to cover both property and liability-related risks. In the United States, many business owner's policies for small businesses will include a cyber incident as a covered event and offer coverage for costs related to incident response, data and software restoration, cyber ransom and extortion and business interruption (whether as a standard inclusion, offered endorsement or combination) (Insurance Information

Institute, 2014; Insurance Information Institute, 2015). One US business owner's policy reviewed also included coverage for communication and media liability and network security failure liability.

There is very little information available on the extent of explicit or implicit coverage of cyber-related risks in traditional policies. Lloyd's completed a consultation on cyber attack exposures with Lloyd's Market Association underwriters for all lines of business ("LMA panels") and received responses suggesting that there is some cyber exposure in all of its classes of business. A Swiss Re (2016a) survey of insurers from around the world found that 27% provided coverage for cyber risks in existing policies (rather than as separate coverage), while 10% provided both stand-alone coverage and coverage in traditional policies (with little variation across regions). Most (65%) of the respondents to the OECD questionnaire (including 80% of North American and 75% of European insurance sector respondents) perceive the coverage in existing policies of cyber risks to be a moderate or high risk factor which suggests that a significant share of overall coverage for cyber risks remains in traditional policies.

Notes

1 Some stand-alone cyber insurance policies and endorsements provide coverage on a "difference-in-conditions" basis, which means that coverage is only provided where the loss or damage is excluded from existing (primary) coverage. This type of insurance coverage is specifically provided to address gaps in existing coverage.

2. In many jurisdictions, the insurability (from a legal perspective) of a fine or penalty will depend on the circumstances. For example, the insurability of regulatory fines and penalties has been tested in a number of court cases in the United States based on the legal principle of *ex turpi causa non oritur actio* (from a dishonourable cause an action does not arise) - i.e. insureds should not receive the benefit of an insurance payout from an intentional wrongful or negligent act. Similarly, some respondents questioned whether fines imposed by the UK Information Commissioner's Officer would be legally insurable, while a working group led by IRT System X (2016) examining the coverage provided by cyber insurance in France found that regulatory penalties and fines may be uninsurable. Some insurance companies will not provide any cover for regulatory fines and penalties on principle, whether or not permissible by law (Gordon, 2014; Iole and Divelbiss, 2015).

3. The difference in the share of policies providing coverage for business interruption and network security liability between the RMS/CCRS review and the OECD review is likely linked to the timing of each review. A more recent review by RMS/CCRS found an increase in the inclusion of both of these types of losses (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

4. The RMS/CCRS review found a much higher share of policies providing coverage for intellectual property theft (23%). However, this may be explained by the difference in timing between the reviews as an update published in 2017 found a significant decline in the coverage of this type of loss (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

5. The RMS/CCRS review found that 46% of the policies reviewed included coverage for "reputational damage", defined in the review as "loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly

attributed to the publication of a defined security breach event." This was much higher than the share of policies offering this coverage observed in the OECD review of policies - which only included specific coverage for loss of profits (not coverage related to managing reputational damage) in its review.

6. For example, one US insurance company denied coverage for funds transferred as a result of a social engineering fraud on at least two occasions in 2015 and 2016 (and faced litigation in both cases). In at least one of the two examples, the disputed coverage was in a crime/fidelity policy (not a cyber insurance policy) (Krebs, 2016). Two other recent cyber insurance policy disputes related to social engineering that led to fraudulent transfers came to contradictory conclusions with one court finding in favour of the policyholder and the other in favour of the insurer denying coverage (based on slightly different policy wordings) (Collins, 2017). Recently, a court in the Canadian province of Alberta found that an insurer was not liable under a commercial crime policy for fraudulent payments made to a bank account by an employee deceived by an individual impersonating a supplier (Dunbar, 2017). A social engineering fraud incident at Leoni AG was partially covered under the company's fidelity policy and not covered under its cyber insurance policy which only covered financial losses caused by a network breach (Suess, 2017).

7. Some reports suggest that physical damage due to a covered peril (such as fire) resulting from a cyber incident could be covered under traditional policies (Gen Re, 2016) although it is not clear whether this would be the case where either the CL 380 or NMA 2912 exclusions were applied. No cases were identified where this was tested. As a result of the complexity of this issue, insurance companies that provide coverage for physical damage under stand-alone cyber insurance policies often do so on a difference-in-conditions basis. Similarly, business interruption coverage provided in stand-alone cyber insurance policies is often provided based on a disruption to information systems (i.e. non-material damage).

8. For example, a federal appeals court in the US state of Virginia upheld a lower court's decision obligating Travelers to cover costs related to defending Portal Healthcare Solutions against claims related to a privacy breach under its commercial general liability policy (Simpson, 2016b). This contradicts an earlier court decision which found that Zurich had no obligation under its commercial general liability policy to cover defence costs incurred by Sony as a result of a privacy breach (Insurance Information Institute, 2015).

9. For example, a professional services firm that has custody of client funds that are later lost to fraud could potentially seek coverage under an errors and omissions or professional indemnity policy (Kamaiko, 2016).

References

ABI (2016), *Making Sense of Cyber Insurance: A Guide for SMEs*, Association of British Insurers, London.

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).

Advisen (2017),"Insurers in India designing customized cybersecurity policies", *Advisen Cyber FPN: Digest Edition*, 4 October.

Airmic (2012), *Airmic Review of Recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products*, Airmic, London.

Allianz Global Corporate & Specialty (2016), *Megacities: Pushing the Boundaries of our Industry*, Allianz Global Corporate & Specialty SE, Munich, www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Megacities_The_future_risk_landscape.pdf.

Anderson, R. (2013a), "ISO's Newly-Filed Data Breach Exclusions Provide Yet Another Reason To Consider "Cyber" Insurance", *K&L Gates Legal Insight (26 September)*, www.klgates.com/files/Publication/5d32e369-a293-4cc0-b9da-a7aecf6e824e/Presentation/PublicationAttachment/4c155b35-ea6e-425f-9cc6-b04f39c9a9a5/Insurance_Coverage_Alert_09262013.pdf.

Anderson, R. (2013b), "Insurance Coverage for Cyber Attacks: Part Two of a Two-Part Article", *K&L Gates Legal Insight (June)*, www.klgates.com/files/Publication/ad055263-b16b-4637-8735-049cab81c2a9/Presentation/PublicationAttachment/239ee296-257f-4025-8231-09816fe61efa/Insurance_Coverage_for_Cyber_Attacks_Part_Two.pdf.

Anderson, R. (2013c), "Insurance Coverage for Cyber Attacks: Part One of a Two-Part Article", *K&L Gates Legal Insight (May)*.

Aon (2013), *Network Security and Privacy: Risk Management and Insurance to address Legal Exposures and Financial Statement Protection (2013 Update)*, Aon plc.

Aschkenasy, J. (2013), "CGL exclusions will fuel cyber purchase trend", *Advisen News* (18 November), www.advisenltd.com/insurance-news/2013/11/18/cgl-exclusions-will-fuel-cyber-purchase-trend/

Augustinos, T., M. Deem and L. Kamaiko (2014), "Cyber Risks: An Ever-Evolving Landscape", *International Underwriting Association (26 February)*, Edwards Wildman Palmer, LLP.

Australian Reinsurance Pool Corporation (2016), *Cyber Terrorism and Australia's Terrorism Insurance Scheme: Physically destructive cyber terrorism is a gap in current insurance coverage (March)*, Australian Reinsurance Pool Corporation, http://arpc.gov.au/files/2016/03/ARPC-Cyber-Terrorism-Discussion-Paper-FINAL.pdf.

BaFin (1998), Guidelines on the provision of ransom insurance (BAV Circular 3/1998), Bundesanstalt für Finanzdienstleistungsaufsicht, www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_9803_va_loesegeldversicherung_en.html, accessed 2 November 2016.

Barker, B. (2016), "Told You So! The Impact of Cyber Risk on D&O Insurance", *Cyber Governance Journal*, 18 April, www.cybernance.com/told-impact-cyber-risk-insurance/.

Barlyn, S. and C. Cohn (2017), "Companies Without Cyber Cover Relying on Kidnap Insurance to Recoup Ransomware Losses", *Carrier Management*, 19 May, www.carriermanagement.com/news/2017/05/19/167321.htm.

Basak, S. (2015), "Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy", *Bloomberg*, 22 July, www.bloomberg.com/news/articles/2015-07-22/worried-about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy, accessed 4 November 2016.

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

Bolot, J. and M. Lelarge (2008), "Cyber Insurance as an Incentive for Internet Security", Presented at WEIS 2008, Seventh Workshop on the Economics of Information Security, 25-28 June, Hanover (United States), www.di.ens.fr/~lelarge/papiers/2008/cyber-surv.pdf.

Carrier Management (2017), "Pending New York Cybersecurity Regs Risk Raising Loss Potential: Fitch Ratings", *Carrier Management*, 13 February, www.carriermanagement.com/news/2017/02/13/164154.htm.

Carrier Management (2016a), "Munich Re, Hartford Steam Boiler and CNA Launch New Products", *Carrier Management*, 28 June, www.carriermanagement.com/news/2016/06/28/155933.htm.

Carrier Management (2016b), "The Latest Launches From Chubb, Willis Towers Watson and XL Catlin", *Carrier Management*, 3 November, www.carriermanagement.com/news/2016/11/03/160717.htm.

Carrier Management (2016c), "The Latest Launches From XL Catlin, AXIS and Take1 Insurance", *Carrier Management*, 17 October, www.carriermanagement.com/news/2016/10/17/159999.htm.

Carrier Management (2016d), "The Latest Launches From Chubb, Beazley and Allianz", *Carrier Management*, 13 June, www.carriermanagement.com/news/2016/06/13/155366.htm.

CGI (2017), "Severe cyber breaches cost PLCs 1.8% of company value or £120 million, according to new CGI study", *Media Centre*, 12 April, www.cgi-group.co.uk/news/cost-of-cyber-breach-to-plcs-cgi-study.

Cohn, C. and J. Saul (2017), "Shipping Insurance Policies Fall Short, Exposing Industry to Cyber Threats", *Carrier Management*, 12 January, www.carriermanagement.com/news/2017/03/10/165134.htm.

Collins, B. (2017), "Evolving cyberinsurance coverage for phishing attacks", *Property Casualty 360°*, 20 September, www.propertycasualty360.com/2017/09/20/evolving-cyberinsurance-coverage-for-phishing-atta.

Council of Insurance Agents & Brokers (2017), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (May).

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

Council of Insurance Agents & Brokers (2015a), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (October).

Council of Insurance Agents & Brokers (2015b), 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.

Cullina, M. (2017), "Evolving cyber concerns create gaps in homeowners' coverage", *Property Casualty 360°*, 11 January, www.propertycasualty360.com/2017/01/11/evolving-cyber-concerns-create-gaps-in-homeowners.

Cyber Risk Insurance Forum (n.d.), *Sample CRIF Cyber Risk Chart - UK only*, www.cyberriskinsuranceforum.com/sites/default/files/pictures/CRIF%20EventImpact%20Chart_0.pdf, accessed 31 October 2016.

Department for Culture, Media and Sport (2017), *Cyber Security Breaches Survey 2017*, Department for Culture, Media and Sport, London.

Donlon, R. (2015), "Small, mid-sized businesses hit by 62% of all cyber attacks", *Property Casualty 360°*, 27 May, www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber.

Dunbar, C. (2017), "Social engineering fraud: Significant coverage gap under commercial crime policy", *Mondaq Business Briefing*, 6 September, www.mondaq.com/canada/x/626468/Insurance/Social+Engineering+Fraud+Significant+Coverage+Gap+Under+Commercial+Crime+Policy.

Eling, M. and J.H. Wirfs (2016), *Cyber Risk: Too Big to Insure?*, Institute of Insurance Economics, University of St. Gallen.

Endurance International Group (2015), "New Survey Finds A Vast Majority Of U.S. Small Business Owners Believe Cybersecurity Is A Concern And Lawmakers Should Do More To Combat Cyber-Attacks", *Press Releases*, 4 May, http://newsroom.endurance.com/2015-05-04-New-Survey-Finds-A-Vast-Majority-Of-U-S-Small-Business-Owners-Believe-Cybersecurity-Is-A-Concern-And-Lawmakers-Should-Do-More-To-Combat-Cyber-Attacks.

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

Faulkner, M. (2017), "Munich Re Syndicate targets deeper cyber exposure", *Insurance Day*, 13 April, www.insuranceday.com/ece_incoming/munich-re-syndicate-targets-deeper-cyber-exposure.htm.

Fédération française de l'assurance (2017), *Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise : TPE, PME, vous êtes concernées!*, Fédération française de l'assurance, Paris, www.ffa-assurance.fr/content/anticiper-et-minimiser-impact-un-cyber-risque-sur-votre-entreprise-tpe-pme-vous-etes-0?parent=79&lastChecked=384.

FERMA (2016), *European Risk and Insurance Report 2016*, Federation of European Risk Management Associations, Brussels, www.ferma.eu/app/uploads/2016/09/FERMA-European-risk-and-Insurance-Report-2016.pdf.

Filkins, B. (2016), *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, SANS Institute, www.sans.org/reading-room/whitepapers/legal/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062.

Finkle, J. (2015), "Cyber insurance premiums rocket after high-profile attacks", *Reuters Technology News*, 12 October, www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012.

Fitch Ratings (2017), "Cyber Insurance - Risks and Opportunities", *Fitch Ratings Report*, September, www.fitchratings.com/site/re/903074.

Franke, U. (2017), "The cyber insurance market in Sweden", *Computers and Security*, Vol. 68 (2017), pp. 130-144, http://dx.doi.org/10.1016/j.cose.2017.04.010.

Freedman, A. (2014), "Top Five Uninsurable Risks", *Risk & Insurance*, 2 September, www.riskandinsurance.com/top-five-uninsurable-risks/.

Gen Re (2016), *Cyber and Insurance: Do You Know Where Your Cyber Exposure Is?* General Reinsurance Corporation, Stamford (Connecticut).

Gordon, S. (2014), " Cyber risk and the extent of cover for “legally insurable” fines", *Simmons & Simmons elexica*, 2 July, www.elexica.com/en/legal-topics/insurance/24-cyber-risk-and-insurability-of-fines, accessed 18 November 2016.

Hancock, R. (2017a), "Surge in demand for cyber insurance being driven by 'fear factor'", *Insurance Day*, 5 January, www.insuranceday.com/ece_incoming/surge-in-demand-for-cyber-insurance-being-driven-by-fear-factor.htm.

Hancock, R. (2017b), "Cyber insurance penetration deepens in UK SME market", *Insurance Day*, 24 March, www.insuranceday.com/ece_incoming/cyber-insurance-penetration-deepens-in-uk-sme-market.htm.

Harrington, J. (2017), "Cyber Insurance: Many Choices Now That There Is No Choice", *MyNewMarkets.com*, 27 April, www.mynewmarkets.com/articles/182994/cyber-insurance-many-choices-now-no-choice.

Hemenway, C. (2017), "Willis Towers Watson uses 40 underwriters to build $600 million cyber insurance tower", *Advisen Special FPN*, 27 April, www.advisen.com/tools/fpnproc/fpns/articles_new_22/P/281830215.html?rid=281830215&list_id=22, accessed 27 April 2017.

Hiscox (2017), *The Hiscox Cyber Readiness Report 2017*, Hiscox, London.

Howard, L.S. (2016), " 2017 Predictions Part II: InsurTech, Australia D&O and India Cyber Insurance", *Carrier Management*, 20 December, www.carriermanagement.com/news/2016/12/20/162319.htm.

Insurance Information Institute (2015), *Cyber risk: threat and opportunity*, Insurance Information Institute, New York.

Insurance Information Institute (2014), *Cyber risks: the growing threat*, Insurance Information Institute, New York.

Insurance Journal (2017a), " Munich Re, Beazley Partner to Provide Enhanced Cover for Large Cyber Risks", *Insurance Journal*, 20 April, www.insurancejournal.com/news/international/2017/04/20/448519.htm.

Insurance Journal (2017b), "Connected Homes Heighten Need for Personal Cyber Insurance", *Insurance Journal*, 27 January, www.insurancejournal.com/news/national/2017/01/27/440073.htm.

Insurance Journal (2017c), "Marsh Launches Cyber Risk & Data Breach Cover for Non-US Clients", *Insurance Journal*, 6 February, www.insurancejournal.com/news/international/2017/02/06/440995.htm.

Insurance Journal (2017d), "UK MGA Plum Launches High Net Worth Home Cyber Cover", *Insurance Journal*, 7 April, www.insurancejournal.com/news/international/2017/04/07/447243.htm.

Insurance Journal (2017e), "Travelers Adds Symantec Cybersecurity Services to Cyber Policies", *Insurance Journal*, 10 April, www.insurancejournal.com/news/national/2017/04/10/447421.htm.

Insurance Journal (2017f), "UK's Allianz Insurance Enhances D&O Cover", *Insurance Journal*, 1 March, www.insurancejournal.com/news/international/2017/03/01/443259.htm.

Insurance Journal (2017g), "XL Catlin Expands Professional Indemnity Offering in Iberia", *Insurance Journal*, 17 March, www.insurancejournal.com/news/international/2017/03/17/444763.htm.

Insurance Journal (2017h), "XL Catlin Launches Five Financial Institutions Insurance Solutions in Iberia", *Insurance Journal*, 2 March, www.insurancejournal.com/news/international/2017/03/02/443415.htm.

Insurance Journal (2017i), "Beazley to Manage Data Breaches for Generali Brazil's Cyber Insurance Clients", *Insurance Journal*, 29 September, www.insurancejournal.com/news/international/2017/09/29/466000.htm.

Insurance Journal (2017j), "Intellectual Property Risks May Not Be Covered by Traditional Products: TMK Expert", *Insurance Journal*, 29 June, www.insurancejournal.com/news/international/2017/06/29/456111.htm.

Insurance Journal (2017k), "Beazley Expands Coverage for Social Engineering, Online Fraud Scams", *Insurance Journal*, 30 August, www.insurancejournal.com/news/national/2017/08/30/462733.htm.

Insurance Journal (2016a), "Chubb Adds Cyber Bullying Insurance for U.S. Homeowners", *Insurance Journal*, 5 April, www.insurancejournal.com/news/national/2016/04/05/404202.htm.

Insurance Journal (2016b), "AIG, Chubb, XL Lead in $1 billion U.S. Cyber Insurance Market: Fitch", *Insurance Journal*, 29 August, www.insurancejournal.com/news/national/2016/08/29/424684.htm.

Insurance Noodle (n.d.), *Errors And Omissions (E&O) Insurance (website)*, www.insurancenoodle.com/commercial-coverages/errors-and-omissions-insurance, accessed 8 November 2016.

Iole, J. and M. Divelbiss (2015), "United States: Understanding "Fines And Penalties Coverage" Under Cyber Insurance", *Jones Day*, 3 March,

www.mondaq.com/unitedstates/x/378842/Insurance/Understanding+Fines+And+Penalties+Coverage+Under+Cyber+Insurance, accessed 18 November 2016.

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).

JLT Mining (2014), *Heap Leaching and Hacktivists: Cyber Security in the Mining Industry*, JLT Mining, London.

Johnson, T. (2016), "Competition will drive cyber insurance cover evolution", *Insurance Day*, 8 December.

Kamaiko, L. (2016), "Businesss Email Compromise: Which Insurance Policy Pays?", *Carrier Management*, 25 September, www.carriermanagement.com/features/2016/09/25/159183.htm.

Krebs, B. (2016), "Firm Sues Cyber Insurer Over $480K Loss", *KrebsonSecurity (blog)*, 18 January, https://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/, accessed 28 March 2017.

LaCroix, K. (2017), " RT ProExec's LaCroix: European Settlements Lead D&O Claims Surge", *A.M. Best TV*, 9 February, www3.ambest.com/ambv/displaycontent/video.aspx?rc=lacroix217.

Lathrop, A. (2016), "Does traditional coverage apply when cyber attacks cause physical damage?", *Property Casualty 360°*, 29 December, www.propertycasualty360.com/2016/12/29/does-traditional-coverage-apply-when-cyber-attacks.

Laurie, R. and V. Vitkowsky (2017), "The Wild West of cyber insurance wording", *Insurance day*, 6 April.

List, T. (2015), "Schutz vor Cyber-Risiken: Nachfrage nach Deckungen wächst rasant", *Börsen-Zeitung*, 30 September, www.boersen-zeitung.de/index.php?li=1&artid=2015187017&titel=Schutz-vor-Cyber-Risiken.

Lloyd's (2016), *Facing the cyber risk challenge: A report by Lloyd's*, Lloyd's, London.

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

Malecki, D. (2004), "Risk Management--Electronic data exclusion", *Rough Notes Magazine*, www.roughnotes.com/rnmagazine/search/commercial_lines/04_07p48.htm, accessed 7 November 2016.

Marsh (2017), *Global Insurance Market Index (Second Quarter 2017)*, Marsh LLC, www.marsh.com/content/dam/marsh/Documents/PDF/eu/en/Global%20Insurance%20Market%20Index%20-%20Q2%202017.pdf.

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

Marsh (2016b), *Continental European Cyber Risk Survey: 2016 Report*, Marsh LLC, October.

Marsh (2016c), *UK Cyber Risk Survey Report: 2016*, Marsh LLC, September.

Marsh (2015a), *Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers*, Marsh LLC, October.

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

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

Marsh & McLennan Companies (2016), *MMC Cyber Handbook 2016: Increasing resilience in the digital economy*, Marsh & McLennan Companies.

Quy, T. (2014), "Maximising value from emerging cyber reinsurance", *Insight from Miller*, Miller Insurance Services LLP, www.miller-insurance.com/Insight/2014/January/Reinsurance-cyber.aspx.

NetDiligence (2015), *2015 Cyber Claims Study*, NetDiligence.

Nordman, E. (2012), "Managing Cyber Risks", *CIPR Newsletter (October)*, National Association of Insurance Commissioners and The Center for Insurance Policy and Research, Kansas City (Missouri).

OECD (2017a), *Supporting an effective cyber insurance market: OECD Report for the G7 Presidency*, 13 May, Paris. www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf.

OECD (2017b), "Insurance business written in the reporting country", *OECD Insurance Statistics (database)*, http://stats.oecd.org/Index.aspx?DatasetCode=INSIND, accessed 10 May 2017.

Parsoire, D. (2014), "Cyberassurance: offres et solutions", *Risques: Les cahiers de l'assurance*, No. 101, pp. 61-65, Paris, http://revue-risques.fr/revue/PDF/revue-risques-101.pdf.

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

Poole-Robb, S. (2015), "Here's why the cyber insurance industry is worth £55.6 billion", *ITProPortal*, 7 February, www.itproportal.com/2015/02/07/heres-cyber-insurance-industry-worth-55-6-billion/.

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

Randall, B. (2017), "Insurers face bumpy ride as class actions take hold", *Insurance Day*, 2 March.

Reactions (2017), *Analysis: GDPR fines likely uninsurable – cyber panel*, Reactions, 28 June, https://reactionsnet.com/articles/3590014/analysis-gdpr-fines-likely-uninsurable-cyber-panel.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2017), *2017 Cyber Risk Landscape*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

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.

Saul, J. and C. Cohn (2017), "Shipping Insurance Policies Fall Short, Exposing Industry to Cyber Threats", *Carrier Management*, 12 January, www.carriermanagement.com/news/2017/01/12/163026.htm.

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

Segger S. and B. Lorscheid (2017), "Fragmentation of German cyber policies risks coverage gaps", *Insurance Day*, 30 March.

Simpson, A. (2017), "AIG Latest to Bring Cyber Insurance to Personal Lines High-Net Worth Clients", *Insurance Journal*, 3 April, www.insurancejournal.com/news/national/2017/04/03/446641.htm.

Simpson, A. (2016a), "Fallout from the Travelers CGL Cyber Ruling: Insurance Buyers and Sellers Beware", *Carrier Management*, 25 April, www.carriermanagement.com/news/2016/04/25/153569.htm.

Simpson, A. (2016b), "Federal Court Rules CGL Insurance Covers Data Breach", *Insurance Journal*, 12 April, www.insurancejournal.com/news/national/2016/04/12/404881.htm.

S&P Global Market Intelligence (2015), *Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool*, Standard & Poor's, www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11.

Suess, O. (2017), "Cyber crime fears drive up demand for anti-hacker insurance", *Property Casualty 360°*, 10 May, www.propertycasualty360.com/2017/05/10/cyber-crime-fears-drive-up-demand-for-anti-hacker

Swiss Re (2016a), *Cyber: in search of resilience in an interconnected world*, Swiss Re, Zurich.

Swiss Re (2016b), *Global insurance review 2016 and outlook 2017/18*, Swiss Re, Zurich.

Swiss Re (2017), "Cyber: getting to grips with a complex risk", *sigma*, No. 1/2017, Swiss Re, Zurich.

Taylor, E. (2017), "The changing world of cyber liability insurance", *Property Casualty 360°*, 4 August, www.propertycasualty360.com/2017/08/04/the-changing-world-of-cyber-liability-insurance.

Thevinin, L. (2017), " Le premier vrai test pour un marché de la cyberassurance en plein essor", *Les Echos*, 15 May, https://www.lesechos.fr/finance-marches/banque-assurances/0212089405169-le-premier-vrai-test-pour-un-marche-de-la-cyberassurance-en-plein-essor-2086949.php#.

Thomas, L. and J. Finkle (2014), "Insurers struggle to get grip on burgeoning cyber risk market", *Reuters Technology News*, 14 July, www.reuters.com/article/us-insurance-cybersecurity-idUSKBN0FJ0B820140714.

Tsangaris, H. (2016), "4 tips to sell more cyber liability policies to small businesses", *Property Casualty 360°*, 4 November, www.propertycasualty360.com/2016/11/04/4-tips-to-sell-more-cyber-liability-policies-to-sm.

Vitkowsky, V. and R. Laurie (2017), "How directors and officers can reduce cyber liability exposure", *Property Casualty 360°*, 27 June, www.propertycasualty360.com/2017/06/27/how-directors-and-officers-can-reduce-cyber-liabil.

Watkins, J. (n.d.), "Is There a Cyber Gap in Your Coverage for Bodily Injury and Property Damage Claims?", Thompson Hine, http://www.thompsonhine.com/uploads/1137/doc/Is_there_Cyber_Gap_in_Your_Coverage_-_Watkins.pdf, accessed 14 November 2016.

Wells Fargo Insurance Services (2016), *2017 Insurance Market Outlook: Insights from our national practice leaders*, Wells Fargo Insurance Services.

Weyland, T. (2016), "Ransomware", *Arthur J. Gallagher & Co. Advisor (May)*, www.ajg.com/media/1699126/advisor-ransomware-may-2016.pdf.

Willis Towers Watson (2017), *Marketplace Realities 2017: The search for growth*, Willis Towers Watson.

Wong, S. (2017), "Cyber Risk Insurance", Presented at NAIC-OIC-OECD Roundtable on Insurance and Retirement Savings in Asia, 20-21 September, Bangkok, www.oecd.org/daf/fin/insurance/oecd-insurance-retirement-asia-2017.htm.

Woodward, J. (2002), "The ISO Terrorism Exclusions: Background and Analysis", *International Risk Management Institute's Expert Insight*, www.irmi.com/articles/expert-commentary/the-iso-terrorism-exclusions-background-and-analysis.

Ydstie, J. (2015), "As Cybercrime Proliferates, So Does Demand For Insurance Against It", *National Public Radio*, 12 October, www.npr.org/sections/alltechconsidered/2015/10/12/445267832/as-cybercrime-proliferates-so-does-demand-for-insurance-against-it.

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

Chapter 4

Cyber insurance market challenges

This chapter provides an overview of the main challenges to the development of the cyber insurance market in terms of both insurers' willingness to provide coverage and the demand from companies to acquire insurance coverage. The lack of historical experience and evolving nature of cyber risk create significant challenges for quantifying cyber risk. These challenges, along with concerns about the potential for accumulation risk, lead to higher prices and limited coverage levels. At the same time, the complexity of stand-alone cyber insurance policies, as well as the potential for coverage of cyber risk in traditional policies, leads to significant misunderstanding about the insurance coverage available for cyber risk. There are also concerns about whether cyber insurance policies are responding to the most pressing needs of policyholders.

The insurability of a given risk is usually economically viable only where certain criteria (or "principles of insurability") are generally met (Insurance Europe, 2012).[1] These criteria include:

- Risks must be quantifiable: the probability of occurrence of a given peril, its severity and its impact in terms of damages and losses must be assessable.
- A sufficiently large community with assets at risk can be established to share the risk (mutuality), allowing for sufficient diversification of the risk based on differences across the community in terms of risk exposure (i.e. a limited amount of correlation across the risks covered).
- Risks must occur randomly: the time and location of an insured event must be unpredictable and the occurrence must be independent of the will of the insured.

The extent to which the characteristics of a given risk exposure meets these criteria (among other factors) will impact whether insurance companies can collect the amount of premiums necessary to cover the total losses of a community of insureds (along with administrative costs and returns to investors, where provided by private insurance companies). For insurance to be economically viable, the actuarially-sound premium rates charged to policyholders must be both within their willingness-to-pay for protection and provide sufficient funds in aggregate to cover losses and other costs. The following sections will outline: (i) factors that drive up prices for cyber insurance coverage; and (ii) factors that lower the willingness-to-pay of consumers.

Factors affecting the price of cyber insurance

There are several factors that affect the price at which insurance companies are willing to offer coverage for a given risk, including the level of uncertainty in estimating expected losses (quantifiability), the size of expected losses (economic viability) and the diversity of the pool of risks covered (limited correlation). In the case of cyber insurance, the difficulties in quantifying a relatively new (and evolving) risk, and the potential for significant correlation across insureds (accumulation risk), are the most critical challenges in underwriting cyber risk. This uncertainty is reflected in lower limits offered, higher deductibles and the higher cost of coverage of cyber insurance relative to other types of insurance coverage (where there is more confidence in exposure quantification and a lower probability of correlated exposures). Limited availability (or uncertainty in the availability) of reinsurance coverage may also be a factor leading to a higher cost for coverage as primary insurers may face limits on their ability to transfer risk to reinsurance markets (reinsurance companies face the same challenges in underwriting coverage).

Quantifiability of cyber risk

Of the 36 insurance sector respondents to the OECD questionnaire that commented on challenges to extending coverage for cyber risks, almost two-thirds identified the ability to quantify cyber exposure as a concern (in general or in terms of certain elements required for quantification). There are three main challenges to the quantification of cyber risk: (i) lack of historical data on cyber incidents; (ii) changing nature of cyber risk (and the relevant legal framework); and (iii) access to corporate security information that is necessary for underwriting individual risks.

- *Limited availability of historical data*: As outlined in Chapter 2 (and in the section on underwriting in Chapter 3), the relatively recent emergence of cyber risk as a peril means that there is insufficient historical data to allow for accurate pricing of insurance premiums (Insurance Information Institute, 2015; A.M. Best, 2014; Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). This lack of data is exacerbated by the general unwillingness of the victims of cyber incidents to share information on these events and their impacts (unless required) out of concern for potential reputational impacts (CRO Forum, 2014; Young et al., 2016). For example, one estimate suggests that only 250 000 of the 5 million fraud and 2.5 million cyber-related crimes that occur annually in the United Kingdom are reported (White, 2016). Others have suggested that anywhere from 60% to 89% of all cyber incident go unreported (Edwards et al., 2014).

  Many insurance companies have entered into partnerships with information technology security firms to improve their access to information on incidents although, so far, few have reported that these partnerships have provided sufficient data and expertise to quantify cyber risk (although the value of these partnerships appears to be improving over time) (Council of Insurance Agents and Brokers, 2016a; Council of Insurance Agents and Brokers, 2017). While more data is becoming available as a result of increasing claims experience, the limited amount of cyber insurance coverage underwritten (partly as a result of the limited data for underwriting) reduces the utility of past claims data, leading to a vicious circle that hinders the ability to address data challenges (Deloitte, 2017). There were only 176 claims with an aggregate value of USD 114 million reported in the most recent NetDiligence (2016) study on US cyber insurance

claims experience (relative to the more than USD 1 trillion in gross claims payments made by US non-life insurers in 2015 (OECD, 2017)). Information sharing initiatives have also been established, although the lack of a shared taxonomy (as well as the different objectives for collecting information) are limiting the potential contribution that these initiatives could make to improving quantification (see Chapter 5).

- *Changing nature of cyber risk*: A potentially more significant challenge is that - even if more data were available - that data may become quickly out-of-date as a result of the fast-evolving nature of cyber risk (CRO Forum, 2014; Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Eling and Wirfs, 2016). The perpetrators of cyber attacks can be expected to continue to improve their methods of attack (e.g. new data exfiltration methods, increased denial-of-service capacity or new technologies to support financial fraud and extortion (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Deloitte, 2017)) and find new ways to evade cyber security defences - which will have impacts on any estimates of frequency and severity based on historical cyber attacks. There are inherent challenges to estimating with any significant level of confidence the probability/frequency of incidents caused by human behaviour which can change based on learning from past experience. In the context of cyber risk, this is exacerbated by the involvement of state-sponsored actors whose motivations may be more difficult to understand. Technology and security practices developed to protect against cyber incidents are also constantly evolving, making it extremely difficult to quantify the effectiveness of different protective measures.

  In addition to changing tactics, increasing dependence on digital technologies for new applications and the resulting pervasiveness of connected devices is leading to new exposures (as well as providing additional capacity for malware transmission and DDoS traffic (Howard, 2017) - see Box 2.5). Some estimate that 3 trillion devices could be connected to the internet by 2020 (Allianz Global Corporate & Specialty, 2015), of which an estimated 70% are vulnerable to being compromised as a result of security weaknesses (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). The increasing application of connected technologies in areas such as vehicles, medical devices and building (including residential) control systems, such as thermostats, creates potential for future exposure to physical damages and bodily injury (JLT Re, 2017). Almost all of the insurance sector respondents to the OECD questionnaire rated the emergence of the "Internet of Things" as a significant driver of the changing nature of cyber security risk (97% rated it as a moderate or important driver of the overall level of risk). The increasing use of bring-your-own-device as well as the increasing effort to provide new service platforms, such as mobile applications, could also increase the number of targets (CRO Forum, 2014). There is also an increasing amount of confidential data available to be compromised - one report suggests that the cost of data confidentiality breaches could increase by a factor of four by 2019 (relative to 2015) as a result of the continued "digitisation" of personal information (Cullina, 2017).

  Regulatory developments, such as the proliferation of notification and disclosure requirements will have an impact on the costs (and related penalties) involved in responding to data confidentiality breaches (see Box 2.2). In addition, compensation practices in the context of litigation (i.e. amounts due to injured

parties) continue to evolve (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). For example, litigation in the US state of Florida created a precedent in 2013 for injury (and rights to damages) from the theft of personally-identifiable information without evidence that the losses were due to an identity theft (in this case, the opening of trading and banking accounts) that directly resulted from the breach - a significant departure from the previous practice of dismissing class action suits where no injury could be proven (Chalmers, 2013). A number of insurance sector respondents to the OECD questionnaire identified uncertainty (or evolutions) in the legal framework as a challenge to providing insurance coverage for cyber incidents, particularly in countries with no existing legislation on data confidentiality breach notification (and also as a result of differences in notification requirements across - and sometimes within - different countries).

- *Access to corporate security information*: A number of insurance companies identified the lack of transparency about security practices and past incidents as a significant obstacle to underwriting coverage (while brokers and risk managers raised concerns about the volume of information required and inconsistencies in the information required by different insurance companies). In particular, the results of penetration tests, as well as complete findings from forensic investigations were identified as information that insureds are reluctant to share with their insurers. For insurance companies, this creates a risk of asymmetric information and adverse selection (i.e., where the insured has a better understanding of the risk being underwritten than the insurance company). For the insured, sharing such information could create disclosure risks, should the insurance company be unable to protect against unauthorised access to the sensitive information or in the event of legal proceedings resulting from a cyber incident.

Accumulation risk

Building a large pool of diversified risks (independent and randomly-occurring losses) allows insurers to spread losses over a large number of insureds and mitigates the potential for a large share of the pool to be affected by losses simultaneously. All things being equal, a smaller pool, or a pool with higher dependencies across the risks covered, will lead insurers to require higher premiums (Schwarze and Wagner, 2007). In the case of cyber risk, there is significant potential for losses to be correlated across insureds and across different types of coverages provided to a single insured ("accumulation risk"). Unlike other perils, it is also more difficult to build a diversified pool of risks based on geography or even industry sector given dependencies on the same infrastructure, software and services (Fitch Ratings, 2017). According to some reports, the potential for accumulation risk across policyholders is the primary reason that insurers limit the coverage available for cyber risk (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Z/Yen Group, 2015; Lloyd's, 2015). Respondents to the OECD questionnaire (particularly those from the public sector) identified accumulation risk as one of the most important drivers of cyber risk and it was identified as a concern by more than 60% of the insurance sector respondents that provided information on challenges to providing cyber insurance coverage. Some respondents suggested that a catastrophic event (i.e. an event involving losses to many policyholders, such as the simultaneous exploitation of a vulnerability in a commonly-used software or system, or a disruptive incident at a major cloud services provider) 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). Others suggested that accumulation risk exists across many insurance lines (i.e. it is not unique to cyber) and that the early recognition of this issue in the case of cyber risk is a positive in terms of the sector's ability to manage it.

The most commonly cited sources of accumulation risk (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Allianz Global Corporate & Specialty, 2015; Insurance Information Institute, 2015) include:

- *Common software vulnerability*: A vulnerability in a commonly-used software that, if exploited, could result in widespread data corruption (see the loss scenario described in Box 2.7), encryption (as in the May 2017 "WannaCry" attacks, see Box 2.8) or data confidentiality breach (for example, what could have occurred as a result of the "Heartbleed"[2] vulnerability disclosed in 2014). This risk is exacerbated by what one analyst has described as the "monoculture" apparent in the use of similar software, security programmes and information technology infrastructure (Z/Yen Group, 2015). A scenario analysis by Lloyd's and Cyence (2017) of a vulnerability in a commonly-used operating system that led to exfiltration of first and third party confidential data estimated potential losses ranging from USD 9.68 billion to USD 28.72 billion, including notification and breach of privacy compensation costs and business interruption losses (among other costs).

- *Information technology services disruption*: Attacks on common information technology service providers, such as a cloud service provider (see Box 4.1), the domain name system (DNS) that underpins the functioning of the internet (see Box 2.5), or even the physical infrastructure on which digital technologies rely (such as undersea cables[3] or power supply) that could lead to disruptions in the operations of many insureds simultaneously. One analysis of an insured portfolio found that policyholders had a high-level of shared dependence on certain service providers, including two DNS providers (77% and 50% of policyholders used their services), a cloud service provider (55%) and two verification services providers (64% and 59%) (BitSight, 2016).

- *Critical infrastructure provider*: A cyber incident leading to the disruption of critical infrastructure services that are reliant on digital technologies (power supplies, payment systems, satellites or air traffic control systems) could lead to a broad range of losses across many business lines (see, for example, the blackout scenario described in Box 4.1).

- Given the levels of potential cyber risk in different types of policies (as discussed above), accumulation risk is also possible across policies covering a single customer (Z/Yen Group, 2015). For example, a cyber incident that leads to the malfunction of a critical component of a manufacturing process could cause property and business interruption as well as liability claims by shareholders (directors and officers) and customers if the malfunction leads to defective intermediate or final products (errors and omissions/professional indemnity, product liability). It is also possible that an investigation into a cyber incident could lead to the discovery of past attacks with implications for multiple insurers (depending on the terms and conditions of past policies and assuming the insured had placed cover with different companies over time) (Z/Yen Group, 2015).

Box 4.1. **Accumulation risk in cloud service providers**

Cloud service providers supply an increasing number of services to an increasing number of companies (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016), including:

- software-as-a-service (SaaS) which provides companies with software accessible through cloud service and accounts for approximately half of cloud-related business volume;
- platform-as-a-service (PaaS) which provides companies with an environment for developing and managing their web applications and accounts for around 25% of cloud-related business; and
- infrastructure-as-a-service (IaaS) which provides companies computing power and resources such as servers and back-up services and accounts for around 20% of cloud-related business.

There are over 100 companies that provide various types of cloud services although the commercial market is dominated by Amazon Web Services, Microsoft, IBM and Google which account for approximately half of the overall market (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016). Since 2011, the market for public cloud services has grown by almost 18% annually (Gartner, 2016) to over USD 100 billion (Statista, 2016) and by a further 53% in 2016 (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). A 2015 survey of information technology specialists worldwide found that 37% of companies depend on cloud services to provide over 25% of their information technology services (including 11% that depend on the cloud for over 50% of their services) and this is expected to grow to over 80% in the next 2-3 years (Spiceworks, 2015) (a more recent survey found that 63% of companies run information technology operations in the cloud (PwC, 2016b)).

While there are some risk management benefits related to the increasing use of cloud-based services (as the level of security provided by cloud service providers can be better than at individual companies), there is also a significant accumulation risk should the services provided by one of the main cloud service providers be disrupted or should the data that they hold be breached (Allianz Global Corporate & Specialty, 2015). The increasing use of cloud services was identified as being a moderate to important driver of the level of cyber risk by 95% of the insurance sector respondents to the OECD questionnaire. A survey of cyber security and risk experts in late 2016 identified a distributed denial-of-service attack on a cloud service provider as the "systemic cyber event" most likely to occur in the near future (i.e. a single event impacting 500 or more companies) (AIG, 2017). A key concern for insurance companies is the level of responsibility that cloud providers will accept in the case of a data confidentiality breach. Some have suggested that cloud service providers will bear only limited liability and that much of the costs of a data confidentiality breach could be borne by its clients (and their insurers) (Deloitte, 2017; Tsangaris, 2016).

This risk has so far been avoided on a large-scale (the four large cloud service providers generally achieve a 99.9% rating for reliability of service from third party rating services) although disruptions have occurred, including an 8-hour disruption to Amazon Web Services in 2011 (along with a 5-hour disruption in 2015 and a 5-hour disruption in 2017), a 4-day disruption to Google Cloud Gmail services in 2010, a 36-hour disruption to the Intuit cloud service (a provider of SaaS services for tax forms) in 2011 and a 24-hour disruption to Symantec's cloud-based security services (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016; Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). A similar accumulation risk is present in managed service providers that manage the applications, networks and/or systems infrastructure of other companies. In 2017, security researchers announced that managed service companies had been targeted by a particular hacking group in order to gain access to their clients' networks. While no information was available on the impact of the resulting data confidentiality breaches, the attacks reportedly affected organisations across 15 countries in Europe, North America, South America, Africa and Asia (Trend Micro, 2017).

In 2017, Lloyd's and Cyence (2017) released a scenario based on the inclusion of malicious code in open-source generated "hypervisor"[1] software commonly-used in operating cloud services. Under the scenario, sophisticated companies using "Tier 1" cloud service providers face an outage of at least 55 hours while less sophisticated organisations dependent on "Tier 2" cloud service providers face an outage of up to 5 days and 19 hours. Based on the scenario and estimates of dependence on cloud service providers across different sectors (as well as the availability of alternative business processes), they estimate that losses in terms of lost income and extra expense (i.e. losses that could normally be insured under cyber insurance policies with coverage for cloud service disruptions) would range from USD 4.6 billion ("large loss") to USD 53.05 billion ("extreme loss") depending on the ultimate duration of the outage. When levels of cyber insurance penetration, as well as the sub-limits commonly applied to contingent business interruption coverage, are taken into account, the report estimates insured losses ranging from USD 620 million under the large loss scenario to USD 8.14 billion under the extreme loss scenario.

1. A hypervisor is a type of software that provides a virtual machine platform for executing and monitoring multiple operating systems. In the context of cloud services, hypervisors are used to separate and maintain the privacy of separate virtual machines and are therefore a critical component of the cloud services infrastructure (Lloyd's and Cyence, 2017).

Reinsurance availability

The lack of historical experience, a changing risk landscape - and particularly the potential for accumulation risk - will also impact the availability of reinsurance coverage for cyber risk. Some reports have suggested that there is limited reinsurance availability for cyber risks, that this may be an impediment to the capacity of primary insurers to provide cover, and that a catastrophic cyber event might require a government backstop (Z/Yen Group, 2015; Insurance Information Institute, 2015; Lloyd's as reported by Mitchell, 2015; Swiss Re as reported by Faulkner, 2017). However, very few OECD questionnaire respondents (4 of the 28 insurance sector respondents (excluding reinsurers)) identified availability of reinsurance capacity as an impediment to providing coverage. A number of recent reports have also suggested that there is significant capacity (and appetite) in the reinsurance market for cyber risks (JLT Re, 2017), evident in the growing range of coverage structures available, including both proportional (quota share) and non-proportional (aggregate stop-loss, per risk excess-of-loss and per event excess-of-loss (Swiss Re, 2016b; Aon Benfield, 2016; JLT Re, 2017)).

The offering of reinsurance coverage for cyber risk does face some structural challenges given the mix of first party (property) and third party (liability) coverage that is usually included in stand-alone policies (Parsoire, 2014). As a result, most reinsurance coverage for US cyber risk has been embedded into other treaties such as specialty casualty, errors and omissions and directors and officers (S&P Global Market Intelligence, 2015). Reinsurers may also be providing significant amounts of implicit (silent) coverage through their traditional lines as exclusions are not commonly applied in casualty (liability) reinsurance programmes, while the cyber exclusions that are sometimes applied by reinsurers on property reinsurance coverage are generally untested (JLT Re, 2017; Prudential Regulation Authority, 2016).

Stand-alone reinsurance coverage has begun to emerge. Five reinsurance companies provided responses to the OECD questionnaire and two provided some details on the types of losses that they would cover. Coverage is available from both reinsurers for crisis management, data restoration and the major types of liability (breach of privacy compensation, network security failure and communication and media), although only one reinsurer provided coverage for extortion and fraud. One of the two reinsurers noted that their reinsurance coverage was provided both on a stand-alone basis and in combination with other perils.

There are some reports that reinsurance coverage is being provided cautiously through the use of sub-limits and event limits (i.e. placing limits on payouts linked to a particular "event") in order to manage the potential for accumulation risk (S&P Global Market Intelligence, 2015; Deloitte, 2017). Much of the coverage that has been made available, especially in terms of stand-alone coverage, has been provided as quota share (proportional reinsurance) (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017; Héon and Parsoire, 2017). As noted, non-proportional stop-loss and per event/occurrence excess-of-loss coverage (which may be better positioned to address accumulation risk) is becoming increasingly available (although excess-of-loss structures must overcome the challenge of defining the event for which the coverage applies).

According to some estimates, there are 20 reinsurers offering some coverage for cyber risk (S&P Global Market Intelligence, 2015). One estimate suggested that there was approximately USD 500 million in reinsurance premiums collected for cyber risk in 2015 (Héon and Parsoire, 2017). The market is generally stable, with few new large entrants, and a significant share of overall capacity provided by three large reinsurers.

Similar to the primary market, reinsurance pricing appears to be generally defying the soft pricing in other business lines with reports of a hardening market in 2015 and 2016 (particularly for sectors such as retail and healthcare) (Swiss Re, 2016b) and some continued price increases in loss-affected programmes in 2017 (although with some loss-free programmes renewed at a discount (JLT Re, 2016)). There are some reports suggesting significant potential for transfer of peak cyber risks to capital markets through insurance-linked security structures (Artemis, 2017; Yoder and Nocera, 2016). One bank's transfer of operational risk (including cyber risk) to capital markets in 2016 provides relevant experience (see Box 5.5).

Box 4.2. **Coverage of cyber-related losses by terrorism insurance programmes**

A number of countries have established terrorism insurance programmes to provide coverage for losses resulting from terrorist attacks. These programmes are generally structured to include some level of retention by the insurance industry supported by a layer of re/insurance coverage provided by a publicly-backed pool. In many cases, the coverage is triggered based on a statutory definition of a terrorism event (often tied to a government declaration that a given event was a terrorist attack). In some countries, the definition of a terrorism event might include attacks using information technology or attacks on information technology.

In 2016, the OECD undertook an informal survey among its contacts at terrorism insurance programmes to determine the extent to which losses from a cyber terrorism attack might be covered by the insurance offered by these programmes - focused on denial-of-service attacks and malicious system malfunctions affecting industrial control systems (see Table 4.1). In some countries, including Australia, Germany and the United Kingdom, cyber attacks are specifically excluded from the definition of an event that would trigger programme coverage. In Russia, the underlying policies reinsured by the terrorism insurance programme consistently exclude cyber as an eligible peril for coverage. Coverage from the Terrorism Risk Insurance Program (TRIP) in the United States also depends on the nature of the underlying coverage provided which, in some cases (e.g. property, liability and worker's compensation), may provide some coverage of losses resulting from cyber attack. The US Treasury published guidance in December 2016 on the inclusion of cyber liability as a class of insurance that could be eligible for TRIP coverage (US Department of the Treasury, 2016). In France and Spain, there is some potential for coverage for physical (material) damage (including intangible assets in Spain) resulting from a cyber attack as well as, in the case of Spain, for business interruption arising from direct damages (where business interruption is explicitly included in the underlying policy). In France, the terrorism reinsurance pool (*Gestion de l'Assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme* (GAREAT)) modified its internal regulations in 2017 to clarify that non-material damages resulting from an act of cyber terrorism are excluded from its coverage. Bodily injury resulting from a cyber attack would also be covered in Spain. A number of countries are examining the appropriateness of the coverage currently provided by terrorism insurance programmes for cyber terrorism (see for example: Australian Reinsurance Pool Corporation, 2016).

Table 4.1. **Terrorism insurance programme coverage of cyber-related losses (DDoS, system malfunction): selected countries**

	Physical damage	Business interruption (without material damage)	Data and software loss	Bodily injury
Australia	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
France				
Germany	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
Russia	*----------cyber attacks are excluded from coverage in underlying policies----------*			
Spain				
United Kingdom	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
United States				

Likely covered Potentially covered Not covered

In the case of cyber attacks related to terrorism, some re/insurance coverage may be available through terrorism insurance programmes (see Box 4.2), although a significant challenge lies in (openly) attributing a cyber attack to a terrorist organisation (or otherwise defining it as a terrorism event) (CRO Forum, 2014). Lloyd's has indicated an interest in examining the extent to which existing war and terrorism exclusions have been - and should be - extended to cover cyber terrorism (Lloyd's, 2016). The terrorism pool in the United Kingdom (Pool Re) has reportedly had discussions with the government and industry about extending the coverage it provides to cyber terrorism (Cohn, 2017). Some reports have suggested that the US insurance industry is also asking the US Congress to consider a government backstop for major cyber attacks similar to the Terrorism Risk Insurance Program (Basak, 2015).

Factors affecting the willingness-to-pay for cyber insurance coverage

While the level of uncertainty in quantifying cyber risk and the high potential for accumulation risk will lead to higher prices for cyber insurance coverage, a number of factors are likely to reduce the demand/willingness-to-pay for coverage, including a lack of awareness of potential losses from cyber risk, misunderstandings about the need for coverage as well as a potential mismatch between the coverage offered and what companies are seeking.

Lack of awareness of potential cyber losses

While cyber risk has often been identified as an underestimated risk with limited attention from senior executives and directors, many more recent surveys have suggested that this is changing even outside of the United States where awareness levels have already been generally high for many years.[4] In the United Kingdom, annual surveys of cyber risk perceptions and incident experience found a substantial increase in the number of companies that considered cyber to be a top-10 risk between 2015 and 2016 (from 45.8% to 71.8%) and the share of companies' whose senior management consider cyber security as high or very high priority (from 68% in 2016 to 74% in 2017) (Department for Culture, Media and Sport, 2017; Department for Culture, Media and Sport, 2016). In continental Europe, the share of companies that included cyber as a top-5 risk on their risk registers increased from 19% in 2015 to 32% in 2016 (while the share of companies not including cyber on their risk survey declined from 23% to 9%) (Marsh, 2016a). Similarly, another recent survey of European business executives found a significant shift in responsibility for issues such as cyber protection and data breach plans from the Chief Information Officer to the Chief Executive Officer as shareholders increasingly expect CEOs to take responsibility mitigating cyber as risk to financial performance (Lloyd's, 2016).

Although the level of awareness of cyber risk and senior management attention to cyber security appear to be increasing, there appears to be a gap in terms of translating cyber risk into estimates of potential losses which would normally be a prerequisite to any decision on the purchase of insurance coverage. In continental Europe, a recent survey found that just over half of companies had identified potential loss scenarios, although only 40% had evaluated potential financial impacts and strategies for funding those losses (Marsh, 2016a). A survey in the United Kingdom found that the share of companies that had estimated the potential financial impact of a cyber incident actually declined from 39.9% in 2015 to 35.4% in 2016 (Department for Culture, Media and Sport, 2016). This is consistent with 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 incidents was the biggest impediment to purchase. It might also be a factor in the relatively low proportion of companies that evaluate the adequacy of their insurance coverage on the basis of internally-generated risk assessments (13% based on a survey of global companies (Ponemon, 2017)) and that use return-on-investment analysis in decisions on security investments (6% based on a survey of UK companies (Department for Culture, Media and Sport, 2017)). This lack of understanding of financial exposure has led many companies to make insurance purchase decisions based on industry benchmarking (i.e. *how much insurance has my competitor bought?*) rather than an assessment of actual needs.

Misunderstandings about coverage

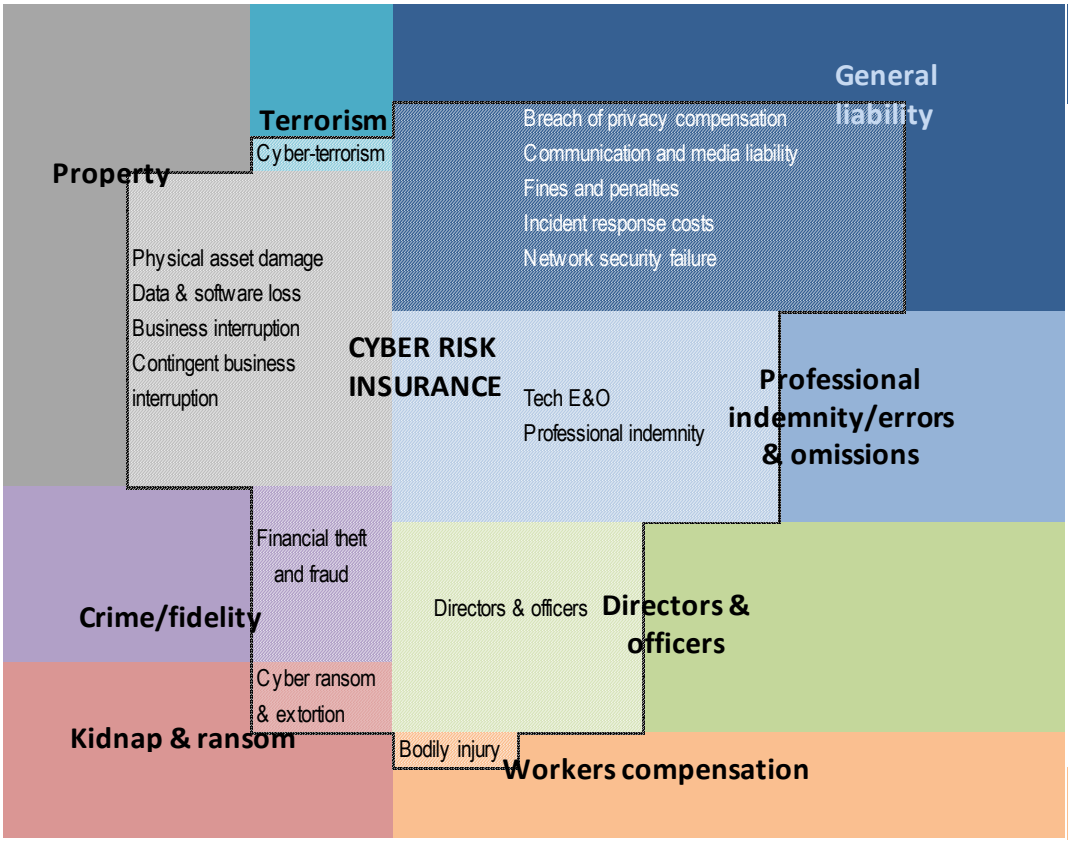
Misunderstandings about insurance coverage for cyber risk, beginning with a lack of awareness about the availability of specific coverage for cyber risks, are widespread. For example, a 2016 survey of European businesses found that 50% were unaware that cyber coverage for data confidentiality breaches was available (Lloyd's, 2016). There are also significant misunderstandings about the level of coverage provided by traditional policies for cyber risks as well as challenges in understanding the specific conditions and coverage limitations in different cyber insurance policies.

As noted in Chapter 3, depending on the exclusions applied, a number of traditional policies could provide some coverage for losses related to cyber incidents, including property, general liability, directors and officers, errors and omissions/professional indemnity, crime and kidnap and ransom. The expectation of coverage (or misunderstanding about the level of coverage) in traditional lines is often cited as a major reason for low levels of cyber insurance take-up (Deloitte, 2017; ENISA, 2012; Swiss Re, 2016a). A recent global survey found that 30% of respondents perceived that their existing property and casualty policies provided sufficient coverage for cyber risks (Ponemon Institute, 2017). This makes it difficult for companies to determine what coverage gaps they may face as a result of cyber risks and how best to address these gaps. Even companies that seek the assistance of brokers may receive different advice. There are conflicting reports, for example, on whether brokers are increasingly advising their clients to purchase stand-alone cyber insurance policies (Council of Insurance Agents and Brokers, 2016a) or seek endorsements on existing policies (Z/Yen, 2015).

These challenges are unlikely to be addressed in the near-term, as some insurers are expanding the scope of stand-alone cyber insurance to cover a broader range of risk while others are expanding the scope of traditional coverage to include cyber risk (Moynihan, 2017). Figure 4.1 provides an illustration of the potential for overlapping coverage between stand-alone cyber policies and various traditional policies (i.e. the centre of the illustration shows the component parts of stand-alone cyber insurance policies and where that coverage might be (or have been) provided in traditional policies).

There are also significant differences in the types of coverage, exclusions and conditions applied in different stand-alone cyber insurance policies (ENISA, 2012; Deloitte, 2017) - and rapid changes as policy language evolves to respond to claims experience, legal interpretations and competitive imperatives (Carbone and Ryan, 2016). Among the stand-alone policies recently reviewed by the Risk Management Solutions and the Cambridge Centre for Risk Studies (2017), only two were found to offer the same set of coverages.

Figure 4.1. **The potential for overlapping coverage for cyber risk in stand-alone and traditional policies**



Source: OECD based on JLT Re (2017).

There are also a number of differences in the specific terms and conditions of stand-alone cyber insurance policies. For example, the triggers for payment among policies offered by the respondents to the OECD questionnaire vary significantly in terms of the time basis for payment (i.e. date that a claim is made ("claims-made basis"), date that the attack took place ("occurrence basis") and date that the attack was discovered ("discovery basis")), as well as whether or not retroactive coverage was offered (a critical issue given that it took an average of 191 days in 2016 for a company to identify that a malicious privacy breach had occurred on its network (Ponemon Institute, 2017)). Some respondents provided retroactive coverage for liability claims made while others provided retroactive coverage relative to the occurrence date and only for first party losses - with varying levels of retroactivity offered (usually 1-3 years). There are also important differences in terms of: (i) coverage of non-malicious acts, including human error (as noted specifically in the case of fraudulent fund transfers); (ii) coverage for voluntary (vs. mandatory) notification costs; and (iii) scope of coverage provided in the definition of "computer system" (i.e. whether outsourced systems are included) (Lloyd's and Cyence, 2017).

Various surveys of brokers, who play a critical role in helping companies understand the coverage being offered, have identified frustrations due to the lack of harmonisation across policy offerings (definitions, terminology, limits, endorsements, exclusions, etc.) and the resulting difficulty in comparing offers without a detailed review of terms and

conditions (Advisen, 2014; Council of Insurance Agents and Brokers, 2015a). As a result, some brokers have reportedly reduced the number of insurance companies that they work with on cyber insurance (Council of Insurance Agents and Brokers, 2016a), with potential implications for the competitiveness of the market.

While these differences in coverage may provide more choice for the insureds, the lack of harmonisation of policy language and conditions also seems to reduce the attractiveness of cyber insurance policies. A recent survey found that, for 27% of respondents, too many exclusions, restrictions and/or uninsurable risks were driving factors in their decision not to purchase cyber insurance coverage (Ponemon Institute, 2017). Policy complexity and lack of harmonisation may also be creating trust issues among policyholders - 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).

However, there are some signs that the situation is improving – including reports of increasing harmonisation in the US market (Harrington, 2017) as well as a declining share of brokers that feel there is insufficient clarity on what is covered and what is excluded (55%, down from 71% in 2015) (Council of Insurance Agents and Brokers, 2016b).

Coverage that is not suited to the needs of policyholders

A third factor impeding the willingness-to-pay for cyber insurance coverage is the perception that the products being offered do not provide sufficient coverage for the most important costs that result from a cyber incident. In a survey of UK firms, 77% of companies that provided an opinion on whether insurance coverage for cyber incidents met their coverage needs indicated that it only partially met (or did not meet) their needs (Marsh, 2016b). A global survey of companies found that inadequate coverage relative to exposure was an important driver of the decision not to purchase cyber insurance for 36% of respondents (Ponemon Institute, 2017).

Although the specific reasons why insurance is not meeting all the needs of companies were not identified, limited coverage for reputational damages (i.e. loss of profits due to customer churn) and own intellectual property theft are likely important reasons. Surveys regularly find that the reputational damage resulting from cyber incidents is a key concern for companies (only behind business interruption) while recent surveys of European and UK companies have found reputational damage to be a growing concern (Allianz Global Corporate & Specialty, 2017; Marsh, 2016a; Marsh, 2016b). As noted in Chapter 3, the gap in coverage for reputational damage and intellectual property theft is not specific to cyber insurance. In addition, actual reputational damage from cyber incidents may be less significant than perceived (as outlined in Chapter 2), particularly as more and more companies are affected by serious incidents.

Notes

1. The discussion of insurability in the cited report is undertaken in the context of natural catastrophes although the principles are transferrable to other types of risks.
2. 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).

3. In 2013, damage to several undersea cables led to a disruption of the internet in Africa that lasted almost one day and had a broad range of impacts including, for example, an interruption to the communications necessary for processing foreign payment card transactions (The Geneva Association, 2016).

4. For example, PwC's annual survey on economic crime (2016a) consistently finds more experience with cyber crime and particularly losses from cyber crime in North America relative to other regions. The 2016 survey found that 46% of North America respondents had experienced cyber crime within the last 24 months, relative to 42% in Western Europe and 32% globally. In addition, 31% of surveyed companies in North America had experienced losses over the previous 24 months of more than USD 100 000 (including 14% that had experienced a loss of more than USD 1 million) relative to 13% of Western European respondents and 16% of global respondents that had experienced losses in excess of USD 100 000.

References

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

AIG (2017), *Is Cyber Risk Systemic?*, American International Group, www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf.

Allianz Global Corporate & Specialty (2017), *Allianz Risk Barometer: Top Business Risks 2017*, Allianz Global Corporate & Specialty SE, Munich.

Allianz Global Corporate & Specialty (2015), *Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, Allianz Global Corporate & Specialty SE, Munich, www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

A.M. Best (2014), "Cyber Security Presents Challenging Landscape for Insurers and Insureds", *Best's Special Report, Issue Review*, 5 December.

Aon Benfield (2016), *Reinsurance Market Outlook: Capacity Gap Narrows as Demand Picks Up*, September, Aon plc.

Artemis (2017), "Cyber risks and government pools. Too soon?", *Artemis news articles*, 30 March, www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/.

Australian Reinsurance Pool Corporation (2016), Cyber Terrorism and Australia's Terrorism Insurance Scheme: Physically destructive cyber terrorism is a gap in current insurance coverage (March), Australian Reinsurance Pool Corporation, http://arpc.gov.au/files/2016/03/ARPC-Cyber-Terrorism-Discussion-Paper-FINAL.pdf.

Basak, S. (2015), "Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy", *Bloomberg*, 22 July, www.bloomberg.com/news/articles/2015-07-22/worried-about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy, accessed 4 November 2016.

BitSight (2016), *Risk Degrees of Separation: The Impact of Fourth party Networks on Organizations*, BitSight, Cambridge (Massachusetts)

Carbone, W. and T. Ryan (2016), "Cyber liability insurance: As the market heats up, is it time to cool off in a pool?", *Milliman Insight*, 23 May, http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/.

Chalmers, H. (2013), "Recent Ruling Could Prove Costly for Hacked Businesses", *The Privacy Advisor*, 1 April, https://iapp.org/news/a/2013-04-01-recent-ruling-could-prove-costly-for-hacked-businesses/, accessed 9 November 2016.

Cohn, C. (2017), "Terrorism Reinsurance Fund in UK Wants to Add Cyber Cover", *Carrier Management*, 10 March, www.carriermanagement.com/news/2017/01/12/163026.htm.

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 (2015a), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (October).

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

CRO Forum (2014), *Cyber resilience: The cyber risk challenge and the role of insurance*, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

Cullina, M. (2017), "Evolving cyber concerns create gaps in homeowners' coverage", *Property Casualty 360°*, 11 January, www.propertycasualty360.com/2017/01/11/evolving-cyber-concerns-create-gaps-in-homeowners?.

Deloitte (2017), *Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market*, Deloitte University Press.

Department for Culture, Media and Sport (2017), *Cyber Security Breaches Survey 2017*, Department for Culture, Media and Sport, London.

Department for Culture, Media and Sport (2016), *Cyber Security Breaches Survey 2016*, Department for Culture, Media and Sport, London.

Edwards et al. (2014), "Hype and Heavy Tails: A Closer Look at Data Breaches", Workshop on the Economics of Information Security.

ENISA (2012), *Incentives and barriers of the cyber insurance market in Europe*, European Network and Information Security Agency, Heraklion (Greece).

Faulkner, M. (2017), "Swiss Re calls for government cyber backstop ", *Insurance Day*, 2 March.

Fitch Ratings (2017), "Cyber Insurance - Risks and Opportunities", *Fitch Ratings Report*, September, www.fitchratings.com/site/re/903074.

Gartner (2016), *Market growth forecast for public IT cloud services worldwide from 2011 to 2016*, accessed from Statista, www.statista.com/statistics/203578/global-forecast-of-cloud-computing-services-growth/ on 10 November 2016.

Harrington, J. (2017), "Cyber Insurance: Many Choices Now That There Is No Choice", *MyNewMarkets.com*, 27 April, www.mynewmarkets.com/articles/182994/cyber-insurance-many-choices-now-no-choice.

Heartbleed.com (2014), *The Heartbleed Bug (website)*, http://heartbleed.com/, accessed 21 November 2016.

Héon, S. and D. Parsoire (2017), "La couverture du cyber-risque", *Revue trimestriellle de l'association d'économie financière*, No. 126 (2e trimestre), pp. 169-182.

Howard, L.S. (2017), "Hackers Will Become More Cunning in 2017 as Cyber Risks Intensify: Report", *Carrier Management*, 11 January, www.carriermanagement.com/news/2017/01/11/162963.htm.

Insurance Europe (2012), *Insurance Europe key points for insurers regarding natural catastrophes in Europe*, Insurance Europe, 27 November.

Insurance Information Institute (2015), *Cyber risk: threat and opportunity*, Insurance Information Institute, New York.

JLT Re (2017), *Unlocking the potential of the cyber market: JLT Re Viewpoint*, JLT Re, London.

JLT Re (2016), *Renewal Retrospective: In the balance*, JLT Re, London.

Lloyd's (2016), *Facing the cyber risk challenge: A report by Lloyd's*, Lloyd's, London.

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

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

Marsh (2016a), *Continental European Cyber Risk Survey: 2016 Report*, Marsh LLC, October.

Marsh (2016b), *UK Cyber Risk Survey Report: 2016*, Marsh LLC, September.

Mitchell, S. (2015), "Lloyd's Calling For Government Cyber Backstops", *Cyber Roundup by the Council*, Council of Insurance Agents & Brokers, 16 July, https://cyber.ciab.com/2015/07/16/lloyds-calling-for-government-cyber-backstops/, accessed 10 November 2016.

Moynihan, S. (2017), "Cyber (in)security: Can insurance solutions keep pace with threats?", *PropertyCasualty360°*, 18 January, www.propertycasualty360.com/2017/01/18/cyber-insecurity-can-insurance-solutions-keep-pace.

NetDiligence (2016), *2016 Cyber Claims Study*, NetDiligence.

OECD (2017), "Gross claims payments", *OECD Insurance Statistics (database)*, http://stats.oecd.org/Index.aspx?DatasetCode=INSIND, accessed 19 May 2017.

Parsoire, D. (2014), "Cyberassurance: offres et solutions", *Risques: Les cahiers de l'assurance*, No. 101, pp. 61-65, Paris, http://revue-risques.fr/revue/PDF/revue-risques-101.pdf.

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

Ponemon Institute (2017), *2017 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, Traverse City (Michigan).

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 (2016a), *Global Economic Crime Survey 2016 - Adjusting the Lens on Economic Crime: Preparation brings opportunity back into focus*, PwC. www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/data-explorer1.html.

PwC (2016b), *Moving forward with cybersecurity and privacy: Key findings from The Global State of Information Security® Survey 2017*, 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 (2017), *2017 Cyber Risk Landscape*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

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.

Schwarze, R. and G. Wagner (2007), "The Political Economy of Natural Disaster Insurance: Lessons from the Failure of a Proposed Compulsory Insurance Scheme in Germany", *European Environment*, Vol. 17, pp. 403–415.

S&P Global Market Intelligence (2015), *Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool*, Standard & Poor's, www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11.

Spiceworks (2015), *Diving into IT Cloud Services*, accessed from Statista, www.statista.com/statistics/541975/north-america-emea-cloud-based-it-services-usage-current-and-planned/ on 10 November 2016.

Statista (2016), *Total size of the public cloud computing market from 2008 to 2020 (in billion U.S. dollars)*, Statista, www.statista.com/statistics/510350/worldwide-public-cloud-computing/, accessed 10 November 2016.

Swiss Re (2016a), *Cyber: in search of resilience in an interconnected world*, Swiss Re, Zurich.

Swiss Re (2016b), *Global insurance review 2016 and outlook 2017/18*, Swiss Re, Zurich.

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

Trend Micro (2017), "Operation Cloud Hopper: What You Need to Know", *Tend Micro Cyber Attacks*, 10 April, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know, accessed 13 April 2017.

Tsangaris, H. (2016), "4 tips to sell more cyber liability policies to small businesses", *Property Casualty 360°*, 4 November, www.propertycasualty360.com/2016/11/04/4-tips-to-sell-more-cyber-liability-policies-to-sm.

US Department of the Treasury (2016), "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program", *Federal Register*, Vol. 81, No. 248 (27 December), https://www.gpo.gov/fdsys/pkg/FR-2016-12-27/pdf/2016-31244.pdf.

White, L. (2016), "British Banks Underplay Cyber Attacks, Fearing Bad Publicity or Punishment", *Carrier Management*, 26 October, www.carriermanagement.com/news/2016/10/16/159980.htm.

Yoder, J. and J. Nocera (2016), "8 ways to improve cyber insurance", *Property Casualty 360°*, 30 November, www.propertycasualty360.com/2016/11/30/8-ways-to-improve-cyber-insurance.

Young, D. et al. (2016), "A framework for incorporating insurance in critical infrastructure cyber risk strategies", *International Journal of Critical Infrastructure Protection*.

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

Chapter 5

Addressing challenges to cyber insurability

This chapter examines ways to address the challenges that impede the development of the cyber insurance market. The development of probabilistic models for cyber risk could improve underwriting and reduce uncertainty although this will require improved data on past incidents and their impact as well as on the relative effectiveness of security policies and practices. There are several potential sources of data that could support probabilistic modelling and a few initiatives aimed at sharing this data within the insurance sector and between the government and the private sector. However, a lack of harmonisation limits the contribution of these efforts. The insurance sector and governments in several countries are also examining ways to improve understanding of the insurance coverage available for cyber risk and at least one country has implemented a regulatory intervention to encourage greater transparency.

A number of initiatives are being established to help address the various challenges to the development of the cyber insurance market by governments, the insurance industry and through public-private cooperation. This chapter provides an overview of the initiatives focused on two critical issues for the further development of the market: (i) improving the capacity to quantify cyber risk; and (ii) addressing the challenges in understanding cyber insurance coverage. This is followed by a short discussion of other approaches that could support the development of further market capacity.

Improving the capacity to quantify cyber risk

As outlined in Chapter 4, the limited availability of data on past cyber incidents, the rapid pace of change in the nature of cyber risk, uncertainty about the effectiveness of different security technologies in terms of risk reduction, and the potential for accumulated losses have a negative impact on the supply of insurance coverage for cyber risk and lead to higher premiums for the coverage offered. In the case of other perils, such as natural hazards and terrorism, the development of models has made an important contribution to reducing uncertainty and managing accumulation risk, ultimately improving market efficiency (see Box 5.1).

Box 5.1. **The modelling of natural hazard and terrorism risk**

While there are a number of important differences in the nature of these risks, the development and use of data and modelling infrastructure to support the underwriting of insurance coverage for natural hazards and terrorism (as well as the management of the exposure transferred to reinsurance and capital markets) could provide lessons for the cyber insurance market.

Modelling of natural catastrophe risks began in the late 1980s (Swiss Re, 2017b) and accelerated in the aftermath of Hurricane Andrew in 1992 as a result of large (unexpected) losses across the insurance sector that clearly demonstrated the significant gap in the understanding of exposures to hurricanes (and other natural perils). Natural catastrophe models use data on hazards and their physical parameters (wind speed, ground-shaking), assets-at-risk (i.e. buildings and infrastructure), damage functions (i.e. the likely level of damage that would result from the impact of a given physical parameter, such as wind speed or water level/velocity) and insurance coverage to provide estimates of insured exposure for a range of natural perils. These models incorporate estimates of the probability of a broad-range of different events occurring, allowing for an insurer to estimate their annual average loss and their probable maximum loss for a given return period. These estimates are used for underwriting (and pricing) insurance coverage, transferring risks to reinsurance and capital markets and for the calculation of capital requirements.

The first probabilistic models for terrorism risk were developed following the September 11th terrorist attacks in the United States (which also led to significant unexpected losses across the re/insurance sector). These models provide estimates of frequency using an inventory of potential targets (based on symbolic or economic significance) and the relative likelihood of different attacks based on the complexity of preparing the attack and the probability of success (including a suppression factor based on an assessment of government's ability to prevent such attacks) (Risk Management Solutions, 2014).

The development of these models has benefitted greatly from several external sources of data and analysis, including: (i) decades of trusted data on the occurrence of natural hazard events and their physical characteristics from government meteorological, geological and hydrological institutions and on terrorism events (and unsuccessful plots) from specialised tracking institutes; (ii) for natural hazards, a real-time monitoring infrastructure for many types of natural perils, such as weather stations, satellite imagery, seismographs and river gauges); (iii) extensive databases on buildings and infrastructure (and landmark buildings and infrastructure); (iv) engineering studies on the impact of physical parameters such as wind speed, water height or explosions on structures; (v) years of (often harmonised) claims data, including through claims data aggregators, to support the calibration and verification of models; and (vi) extensive scientific analysis of natural hazard and terrorism risks and their evolution which allows model developers to leverage scientific advancement in understanding these risks (one of the main advantages of models is that they make use of both historical experience and expert understanding of the nature of the peril to develop estimates (Marsh & MacLennan, 2016)).

While these models cannot provide perfectly accurate estimates of the probability of a given event or the precise impact of an event with specific characteristics, regular advancements have led to a level of convergence across different commercial models (suggesting reduced uncertainty) and increasing confidence in the estimates that they generate (Swiss Re, 2017; Hancock, 2017).

Currently, modelling of cyber risk is mostly scenario-based - providing a framework for deterministic estimates of losses - although without providing a basis for estimating the probability that the given scenario might occur (Swiss Re, 2017). As existing scenario-based models have been focused on extreme incidents (including incidents involving a high potential for correlated losses), they are mostly being used for managing accumulation risk rather than for pricing. Two of the major commercial modelling firms (AIR Worldwide and Risk Management Solutions (RMS)), for example, have developed extensive data sets that allow for calculations of potential losses at different companies under a diverse range of scenarios (Swiss Re, 2017). Similarly, Lloyd's has developed a

Realistic Disaster Scenario for a major data security breach based on a common system or software vulnerability and has committed to developing ten more scenarios to assist syndicates' analysis of potential losses from various types of incidents (Lloyd's, 2016a; Lloyd's 2016b). However, the (fortunate) scarcity of extreme incidents limits the ability to attach frequency estimates to these scenarios (or even to most less-extreme scenarios) (Swiss Re, 2017). Some probabilistic models have been developed for higher-frequency incident types[1] such as third party (personal) data confidentiality breaches given the greater availability of data. There are also a number of new entrants that are developing different approaches to adding a probability component to existing models, including through the use of cyber value-at-risk models (Swiss Re, 2017).

The following sections will examine initiatives that could help address the dearth of data on incidents, accumulation risk and the effectiveness of protection measures which, if overcome, could support the development of probabilistic models of cyber exposure over time (although it took many generations of catastrophe models before the necessary level of precision for building wider trust and acceptance was achieved (Fitch Ratings, 2017)).

Incident data sharing initiatives

A critical requirement for developing probabilistic models is availability of sufficient data to predict with some confidence the probability distribution of incidents of varying severity (i.e. not just the impacts of specific scenarios but the probability that such an event could occur within a given return period). As noted in Box 5.2, natural hazard models achieve this through analyses of (extensive) historical data as well as from the findings of scientific research into the nature of the perils (including any potential for changes in frequency and severity) – none of which is readily available in the case of cyber risk.

There are a number of sources of information on cyber incidents in government and in the private sector:

- *Government sources of information on cyber incidents*: Within governments, the main sources of information on cyber incidents are computer security incident response teams (CSIRTs, also known as computer emergency response teams or CERTs), privacy enforcement authorities and sectoral regulators. Governments (e.g. responsible line ministries or national statistical offices) may also collect information through business surveys, either regularly or periodically (see OECD, forthcoming). CSIRTs have been established in a number of countries in order to "prevent, handle and mitigate computer security incidents" (OECD, 2013). CSIRTs collect technical data on incidents that they handle and many use that data to generate (and often publish) statistics on trends in the types of cyber incidents (OECD, 2013) (although with a potential for bias based on the type of incidents that are reported to CSIRTs).

  Privacy enforcement authorities collect data on data confidentiality breaches involving personal information that are reported to them based on applicable notification requirements. Many of these authorities will publish annual statistics on the number of breaches and the number of records exposed (among other indicators). As noted above, the volume of incidents that will be reported to privacy enforcement authorities is expected to increase as a result of the spread of reporting and notification requirements around the world, which means that these authorities are likely to have a more comprehensive picture of these types of incidents in the future (see Box 2.2). For example, national supervisory

authorities responsible for the implementation of the GDPR in the EU will be required to prepare annual reports which may include information on the types of incidents that led to privacy infringements.

Sectoral regulators, such as financial or energy sector regulators, may require the companies that they regulate to notify them of any (or any material) cyber incidents. For example, almost all responses to the OECD questionnaire from insurance regulators indicated an expectation that insurance companies would notify their supervisors of an incident and some had specific requirements for notifying supervisors of material incidents. In some cases, the relevant regulator will publish aggregated information on the incidents reported to them although this occurs much less frequently than in the case of CSIRTs or privacy enforcement authorities. In addition, regulators (whether sectoral or functional) could also impose requirements for the disclosure of cyber incidents (e.g. the US SEC disclosure requirements).

Finally, many insurance regulators (or statistical agencies) collect and publish data on premiums written and claims paid for different business lines by the insurance companies that they oversee. However, at the time of writing, only the US National Association of Insurance Commissioners indicated that they collected regular data on stand-alone cyber insurance premiums and claims (many others collect such data only as needed). Such information would provide statistics on the aggregate value of the insurance payments made, although not specific information on the types of incidents or their individual impacts.

Data and statistics provided by government agencies is rarely harmonised across countries (or even across agencies, given the different drivers behind the data collection). In 2013, the OECD (2013) developed guidance for improving the comparability of statistics provided by CSIRTs. The OECD has also recently begun an assessment of the comparability across countries of personal data breach notification reporting which could lead to greater consistency in terms of the resulting statistics. There is little known information sharing on incidents across sectoral regulators (or efforts to harmonise approaches). The G7 has established a Cyber Expert Group to share information and practices related to cyber security among financial sector regulators although no work on harmonising incident reporting is being planned by this group. The European Union Agency for Network and Information Security (ENISA) intends to examine how mandatory incident reporting schemes within the European Union (e.g. GDPR and NIS directives) could be harnessed as a source of useful incident data for insurance companies.

- *Private sector sources of information on cyber incidents*: Individual insurance companies collect information on incidents affecting their policyholders (where a claim is made) although this information is usually not publicly available (outside of the initiatives described below). In addition, there are a number of private sector companies and organisations that collect data on incidents as a service (or as input into a service) provided to the insurance industry. One US-based company (Advisen) has reportedly collected information from public sources (media reports, legal analyses, freedom of information requests) on more than 35 000 data confidentiality breaches, data integrity/availability incidents, system malfunctions and malicious activities (Advisen, 2017). There are also at least three major databases that provide information on operational risk incidents,

including cyber incidents. One dataset (SAS OpRisk Global Data) is based on publicly available data and reportedly includes over 25 000 operational incidents since 1995, including cyber incidents (Eling and Wirfs, 2016). The ORX database includes an anonymised set of incidents reported by its financial sector members from around the world (although this data is not publicly available). ORIC, a membership-based organisation for insurance and asset management companies, also provides a platform for sharing information on operational risk incidents. Commercial modelling companies, such as RMS and AIR Worldwide, also collect extensive information (including from third-party commercial sources) on cyber incidents in order to calibrate their models.

There are a number of efforts to harmonise claims and incident data in the insurance sector. Lloyd's has established common coding for reporting data on cyber insurance coverage provided by Lloyd's syndicates, including a code for cyber security data and privacy breach (CY)[2] and a code for cyber security property damage (CZ)[3] (Lloyd's, 2015). Two of the major modelling firms (AIR Worldwide and RMS) have released data categorisation schemas in order to encourage the collection of harmonised data on company characteristics, risk management practices, incidents and loss types. The two modelling companies and Lloyd's have also agreed on a set of common core data requirements (Lloyd's, 2016c) (see Table 5.1).

There is also at least one initiative aimed at collecting a harmonised set of incident data. Since January 2017, the ORX database is receiving cyber incident reports from insurance companies on a pilot basis using the CRO Forum data categorisation (which is also used in this report) (Bishop, 2017). The pilot exercise involves reporting by members on incidents that have affected their own systems only (not those affecting their policyholders). There are also a few initiatives aimed at collecting claims information on a harmonised basis. One organisation, NetDiligence, has been publishing cost of claims studies for a number of years. It's most recent study (NetDiligence, 2016) included claims data from 17 insurance companies operating in the US market, including a number of the largest providers, and appears to cover a significant (50% to 70%) share of claims paid in the US market.[4] One of the two main aggregators of insurance claims data for natural catastrophe events,[5] the Insurance Services Officer (ISO), undertook a cyber insurance data call to collect premium and loss data for cyber liability and first-party coverages written between 2010 and 2014 (based on the AIR Worldwide categorisation) and has also launched a platform for aggregating losses related to large cyber incidents (see Box 5.5).

A number of information sharing initiatives have been established by - or between - governments and the private sector, although most are focused on sharing operational threat information rather than incident reports (see Box 5.2). In the United States, the Department of Homeland Security has established a Cyber Incident Data and Analysis Working Group which is working on the development of a Cyber Incident Data and Analysis Repository. The objective of the repository is to provide standardised data on past incidents that would allow for the risk analysis necessary to support "better cyber risk assessments, enhanced cyber incident modelling and prediction, and more cost-effective and dynamic cybersecurity programs" (Department of Homeland Security, 2015). An initial set of potential data categories were published for consultation in September 2015 and included categories for company characteristics, type and severity of incident, risk management approaches and impacts and costs (among others) (see Table 5.1).

Box 5.2. **Public-private threat information sharing initiatives: selected examples**

A number of countries have established mechanisms for sharing information on operational threats between the public and private sectors:

- In the United States, a number of Information Sharing and Analysis Centers (ISACs) have been established for critical infrastructure sectors as trusted environments for sharing threat information (supported by specific legislation to protect against liability and other risks of data sharing). While the ISACs have been established to address multiple risks, some of the sectoral ISACs (such as the Financial Services ISAC (FS-ISAC)) focus extensively on sharing operational and technical information related to cyber threats, including both information identified by private sector members as well as by government. Some, such as FS-ISAC, also operate internationally.
- In the United Kingdom, a Cyber Security Information Sharing Partnership has been established to exchange cyber threat information, including threat analysis provided by a "fusion cell" analytical team comprised of government and industry experts, as well as alerts and threat advisories, weekly and monthly summaries and a malware and phishing email analysis service. The service is free and open to both businesses and individuals.
- In Switzerland, the "Reporting and Analysis Centre for Information Assurance" (MELANI, its acronym in German) provides threat and mitigation information to both individuals and businesses. It also provides a more comprehensive service for operators of critical infrastructure, bringing together the intelligence available through law enforcement, security and intelligence agencies as well as computer emergency response teams.
- In Canada, the Canadian Cyber Threat Exchange has been established as a not-for-profit organisation to share information on cyber threats and vulnerabilities among businesses, government agencies and research institutes. It provides various levels of services to its members, ranging from direct access to its analysts and access to closed information sharing platforms to advice available to the general public on how to protect against identity theft and fraud.
- In France, "Action against cyber crime" (ACYMA, its acronym in French) was established in 2015 as a national platform with three objectives: (i) providing victims (businesses, individuals and local governments) with access to expert advice; (ii) organising awareness and prevention campaigns; and (iii) creating an observatory of digital risks that will support predictive analysis of threats.

These initiatives have generally been established with the aim of preventing cyber incidents and therefore do not provide a platform for sharing information on incidents that have occurred. However, the information that is collected on threats could potentially prove useful for understanding the evolution of cyber incidents. It could also provide a source of data on attempted attacks and success rates - which might both prove useful for probabilistic modelling of cyber risk (as is the case for modelling terrorism risk).

Table 5.1 provides an overview of the types of incident data that are collected (or recommended for collection), as well as the specific data categories (where available) across a few of the major data aggregation initiatives (US Cyber Incident Data and Analysis Working Group, Advisen, CRO Forum, AIR Worldwide and Cambridge Centre for Risk Studies). Four of the five initiatives include a specific categorisation of cyber incidents, although there is currently no harmonisation in terms of incident categories across initiatives[6] with a wide variety of different categories used as well as differences in terms of the scope of incidents covered.[7] All of the initiatives include a categorisation of impacts, including non-financial indicators of impact in the case of two initiatives (US Cyber Incident Data and Analysis Working Group and Advisen). The CRO Forum and Cambridge Centre for Risk Studies' classifications of financial impacts (types of losses) are closely harmonised and can be mapped to the AIR cyber exposure data standard. The

US Cyber Incident Data and Analysis Working Group classification plans to include a much more granular classification of some types of impacts (e.g. incident response costs) and a much less granular classification of others (e.g. liability). The US Cyber Incident Data and Analysis Working Group also intends to collect data on a variety of incident attributes (detection time, attacker motivation, specific control failures, etc.) not collected in the other initiatives.

While a lack of harmonisation across these initiatives limits the availability of comparable data for use in developing probabilistic models of cyber risk, there are also a number of factors that limit the amount of data shared by participants within these initiatives. Sharing of incident data within the insurance industry and between the public and private sectors could be limited by concerns related to: (i) the robustness of the "anonymisation" process, which requires that an appropriate balance be found between providing a sufficient level of detail on incidents without allowing for the identification of the affected organisations; (ii) strength of the security controls protecting the repository, including ensuring sufficient security amongst those able to access the repository; and (iii) confidence in the neutrality and independence of the organisation responsible for the repository, given the need to ensure that data is managed, processed and used appropriately.

From the perspective of insurance companies, there may also be more significant obstacles to disclosing information on incidents that affected their policyholders (relative to incidents that affected the insurance companies themselves (American Insurance Association, 2016)) - notably the potential for liability or for disclosing information that may be subject to future litigation. Insurance companies that have built-up significant claims experience may also be reluctant to share that experience with other companies for competitive reasons (as claims experience can provide a competitive advantage in terms of underwriting). However, one recent global survey found a relatively high-level of acceptance (68% of respondents) that data and information sharing on cyber risk will increase. Close to half of all respondents across most industries indicated that they were prepared to collaborate more strongly in terms of information sharing on an industry-wide basis and with insurance companies (particularly in the hotel, industrial products, consumer products and chemical and petroleum sectors although the media, healthcare and transportations sectors indicated less willingness to collaborate) (Swiss Re, 2016; Swiss Re, 2017).

Access to threat information from government might also provide an incentive for joining information sharing initiatives more generally (Marsh & McLennan Companies, 2016), as could encouragement from regulators. For example, the US National Association of Insurance Commissioners indicated that it encourages the insurers it regulates to share information on incidents in order to improve the collective knowledge of cyber threats.

The establishment of information sharing initiatives also faces practical obstacles that must be overcome, such as what type of organisation is best-placed to host an incident repository. Some of the threat information sharing initiatives (e.g. US Information Sharing and Analysis Centers, Canadian Cyber Threat Exchange) have been established as membership-based not-for-profit organisations while others (e.g. Melani, ACYMA) are government or government-sponsored agencies. The US Cyber Incident Data and Analysis Working Group has not identified a host organisation for the proposed incident repository (although it is not recommending that the repository be hosted by the government). Some insurance industry initiatives (ORX and ORIC International) are

membership-based organisations established for the specific purpose of providing data and analysis to contributing members. Others, including NetDiligence, Advisen and the Insurance Services Office, are independent, for-profit service providers that have been established to specifically offer services to other companies (cyber security assessment services in the case of NetDiligence and a range of insurance-related services in the case of Advisen and ISO). The for-profit organisations could be driven by competitive pressures to develop broader and better data coverage, although competition between them could lead to the development of proprietary arrangements and other practices that would prevent the establishment of a comprehensive repository.

Data on the effectiveness of risk management approaches

As noted above, the quantification of cyber risk exposure also requires an assessment of the relative effectiveness of risk management processes and technologies in both reducing the probability of an incident and the impact of incidents that do occur. While not only a challenge in the case of cyber risk (for example, see OECD (2016) for a discussion on the challenges in measuring and recognising the effectiveness of flood protection measures), the wide variety of available cyber security technologies makes this particularly challenging in underwriting coverage for cyber risk. One estimate has suggested that there are more than 600 products on the market for protecting digital assets and that some large organisations might use more than 100 of these products in their cyber risk management (Harrington, 2017). This requires a significant investment by underwriters in understanding the level of protection provided through the wide variety of protection technologies available (which is particularly important since some have suggested that one third of all cyber vulnerabilities result from the use of security software (Harrington, 2017)). Meanwhile, ever evolving (and increasingly sophisticated) attack methods may make some protection technologies quickly obsolete while some attacks are so sophisticated that it does not matter how much a company has invested in cyber security (Marsh & McLennan Companies, 2016). Further, a comprehensive picture of the level of resilience against cyber risk also requires an assessment of risk management, business continuity planning and information technology policies and processes. Many incidents occur as a result of human error or even a failure to respond to warnings provided by protection technologies - not a technical failure in the protective technology itself (Marsh & McLennan Companies, 2016).

A number of the insurance sector respondents to the OECD questionnaire indicated that they are examining the value of different protection technologies and security practices with the aim of improving their ability to assess risk at different companies, sometimes in partnership with cyber security service providers. Management consulting firms (e.g. McKinsey) and cyber security companies are also providing cyber security assessments services, and in some cases (e.g. Symantec), are offering standardised application forms to support cyber insurance underwriting. There are some models that specifically assess the level of risk at a company with a given set of protective technologies, security procedures and policies (e.g. Cyence) - with some reported success in terms of differentiating risk across different security postures (Marsh & McLennan Companies, 2016; Insurance Journal, 2017).

As the importance of cyber risk has increased, a number of private sector companies have started to develop cyber security ratings that can be used by underwriters (e.g. BitSight ratings, FICO Enterprise Security Scores, Security Effectiveness Scores (PGP Corporation and Ponemon Institute), etc.) based on assessments of cyber security practices as well as observable data on cyber attacks. Providers of these ratings have

claimed some success in identifying a correlation between their ratings and cyber-related losses, although there may be some risk in overreliance on these ratings (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). As a result of the increasing use of these types of security ratings, a number of US companies (including many of the security rating organisations) released a set of shared principles for the development and reporting of security ratings, leveraging some good practices that have been put in place by credit rating agencies (U.S. Chamber of Commerce, 2017).

Governments can play a role in facilitating the assessment of risk management technologies and processes by promoting the establishment and adoption of cyber security standards and methodologies for assessing compliance against these standards (or by encouraging adoption of existing international standards such as ISO/IEC 27001). Examples of such standards include the US National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* and the UK *Cyber Essentials*. Companies often perceive government information and advice as more impartial (relative to cyber security vendors interested in selling protection technologies) and some have suggested a government role in certifying the effectiveness of specific protection technologies. In some countries, government certification schemes do exist for some cyber security related services. For example, in the United Kingdom, the public National Technical Authority for Information Assurance (CESG) provides certification of cyber security consultancies and incident response companies (Department for Media, Culture & Sports, 2016). In the United States, the Department of Homeland Security is offering to undertake cyber security assessments and technology reviews for certain companies (a service advertised as a policyholder benefit by at least one insurance company) (Carrier Management, 2016). In Europe, the European Commission recently announced the establishment of a European cybersecurity certification framework for products and services that are important for the functioning of the Digital Single Market (European Commission, 2017).

Sectoral regulators could also contribute to the assessment of cyber risk management practices by establishing guidance for the companies they regulate on their expectations for cyber resilience (which may provide some assurance to underwriters about the level of cyber resilience in regulated companies). Financial sector regulators normally include cyber risk within the scope of their supervisory activities and a number have established specific guidance on cyber security practices for regulated entities. For example, the Office of the Superintendent of Financial Institutions Canada (2013) has published "Cyber Security Self-Assessment Guidance" which sets out desirable cyber security practices. The G7 Finance Ministers and Central Bank Governors have established the "G7 Fundamental Elements of Cyber Security for the Financial Sector" which provides a framework to ensure financial institutions are properly managing cyber risks. Governments might even consider minimum cyber security standards which all companies must achieve (Eling and Wirfs, 2016).

So far, there is no convergence across the insurance sector in terms of an approach to rating the effectiveness of different technologies or processes/policies. As outlined in Table 5.1, four of the five main data aggregation/harmonisation initiatives collect some information on company attributes and practices although there is little harmonisation, except at the level of basic company data (employees, revenue, sector, etc.).[8] The two data schemes involving the catastrophe modelling sector include similar "company risk attributes" (such as number and type of confidential records and measures of business interruption potential) although apply very different approaches to collecting information on company risk management practices (the Cambridge Centre Risk Studies uses a single

user-generated rating of cyber security practices rather than a set of criteria related to the use of different risk management practices). The AIR Worldwide and US Cyber Incident and Data Analysis Working Group include data on some similar risk management practices (although more detail is sought under the AIR Worldwide framework).

Table 5.1. **Data collected (or planned for collection) by different data aggregation/harmonisation initiatives**

	US Cyber Incident Data and Analysis Working Group	Advisen	CRO Forum	AIR Worldwide Cyber Exposure Data Standard	Cambridge Centre for Risk Studies
Basic company data	Sector (list)	Sector[2]		Sector (NAICS code) [2]	Sector[2]
	Number of employees[2]	Number of employees[2]		Number of employees[2]	Number of employees[2]
	--	Annual revenue[2]		Annual revenue[2]	Annual revenue[2]
	--	Location and geographical footprint		Location and geographical footprint	Location and geographical footprint
Company risk attributes				Registered domain names	--
				IP addresses	--
				Cloud service providers[2]	--
				Internet-based revenue	Internet-based revenue
				--	Revenue dependent on cloud services
				Number and types of confidential records[2]	Number and types of confidential records (PII, PCI, PHI) [2]
				Business interruption cost	Business interruption from internet failure[2]
					Business interruption from cloud service failure
					Business interruption and financial losses from payment system service failure
				Breach history (5-year)	--
Risk management practices	Officer responsible for cyber/information security			Chief Information Security Officer, Chief Privacy Officer, Chief Digital Officer	Cyber security score (user generated)
	Risk management framework, best practice or standard used, standard certification			Standards: (ISO 27001, NIST 800-53, Cyber Essentials, PCI data security standards, etc),	
	Length of time that resources have been dedicated to cyber security Are risk management practices formalised as a policy Is cyber security integrated into enterprise risk management Are policies and procedures risk-informed			Qualitative score – IT maturity	
	--			Qualitative score –	

	US Cyber Incident Data and Analysis Working Group	Advisen	CRO Forum	AIR Worldwide Cyber Exposure Data Standard	Cambridge Centre for Risk Studies
				business recovery	
	--			Qualitative score – network intrusion recovery	
	--			Qualitative score – privacy policy	
	Are dependencies understood			Qualitative score – vendor security	
	Level of knowledge of personnel			Qualitative score – security policy	
	--			External or internal cyber security management	
	--			Segmentation of networks into sub-networks	
	--			Asset types (e.g. database, computer, server, laptop, etc.)	
	--			Remote access policy	
	--			Qualitative security scores (firewall, antivirus, encryption, update and backup frequency)	
Incident type	Data theft (PII, financial data, health records, other)	Privacy – unauthorised contact or disclosure	Third party data confidentiality breach		Cyber security data and privacy breach (Lloyd's CY)[2]
	Data theft - intellectual property	Data (unintentional disclosure, physically lost or stolen, malicious breach)	First party data confidentiality breach		
	Industrial espionage				
	System failure	--	Own system malfunction		Cyber security property damage (Lloyd's code CZ)[2] or Cyber security data and privacy breach (Lloyd's CY)[2]
	SCADA or Industrial Control System	Industrial controls & operations			
	Configuration error	IT – configuration/ implementation errors			
	Web page defacement	--			--
	Outage	--			Cyber security data and privacy breach (Lloyd's CY)[2]
	Malware	--	Own system affected by malware		
	Zero-Day malware attack				
	Destructive WORM				
	Distributed Denial of Service	Network/website disruption	Network communication malfunction		
	--	--	Inadvertent disruption of third party system		
	Third-party event	--	Disruption of external digital infrastructure		
	Storage/back-up failure	IT – processing errors	Deletion or corruption of own or third party data		
		Cyber extortion	Encryption of own or		

	US Cyber Incident Data and Analysis Working Group	Advisen	CRO Forum	AIR Worldwide Cyber Exposure Data Standard	Cambridge Centre for Risk Studies
	Ransomware/extortion		third party data		
	--	--	Misuse of system for defamatory systems		
	Phishing	Phishing, spoofing, social engineering	Cyber fraud/cyber theft		
	--	Skimming, physical tampering	--		--
		Identity – fraudulent use/account access			--
	--	Privacy - unauthorised data collection	--		--
	Natural or man-made (physical) peril	--	--		--
	Physical sabotage	--	--		--
	Categories for incident causes (network intrusion, insider attack, lost device accident/human error) that cover multiple categories	--	--		Cyber terrorism
	--	Privacy - unauthorised data collection;	--		--
Impact	Non-financial indicators of impact (severity, affected assets, type of impact, outcome of incident, duration of interruption/ outage, security response to incident, number of records compromised and level of sensitivity)	Non-financial indicators of impact (affected count, source of loss, type of loss)			
	Credit monitoring[2]	Loss amount	Breach of privacy [compensation] [2]	Security breach expense limit[2]	Breach of privacy event[1,2]
	Legal costs		Regulatory and defence (excluding fines and penalties)	Fines limit[2]	Regulatory and defence[2]
	PCI fines and assessments		Fines and penalties[2]		
	Investigation/forensics		Incident response costs	Public relations limit	Incident response costs
	Victim notification				Breach of privacy event
	Public relations/reputation		Reputational damage (excluding legal protection)		Reputational damage
	Theft		Cyber ransom and extortion[2]	Extortion limit[2]	Cyber extortion[2]
			Financial theft and/or fraud		Financial theft and fraud
	Liability[2]		--	Publishing liability limit[2]	--
			Communication and media [liability] [2]	Media liability limit[2]	Multi-media liabilities (defamation and disparagement) [2]
			Network security/security failure [liability] [2]	Security breach liability limit[2]	Network security failure [liability] [2]
			Directors and officers	--	Liability - directors and

	US Cyber Incident Data and Analysis Working Group	Advisen	CRO Forum	AIR Worldwide Cyber Exposure Data Standard	Cambridge Centre for Risk Studies
			[liability][2]		officers[2]
			Products [liability] [2]	--	Liability – Product and Operations[2]
			Professional services errors and omissions/professional indemnity [liability] [2]	--	Liability – professional services errors and omissions[2]
			Technology errors and omissions [liability] [2]	Programming errors & omissions limit[2]	Liability - technology errors & omissions[2]
	Staff overtime		Business interruption/ interruption of operations[2]	Business interruption limit[2]	Business interruption[2]
	Production delays				
	Business interruption[2]				
	Lost wages and profits				
	--		Contingent business interruption for non-physical damage	--	Contingent business interruption
	System/software installation[2]		Data and software loss[2]	Replacement of data limit[2]	Data and software loss[2]
	Back-up restore[2]				
	--		Intellectual property theft		Intellectual property theft
	Equipment replacement		Physical asset damage[2]	Physical limit[2]	Physical asset damage [2]
	Hardware replacement and new investment				
	--		Bodily injury and death[2]	Bodily injury limit[2]	Death and bodily injury[2]
	--		Legal protection – lawyer fees	--	--
	--		Assistance coverage – psychological support	--	--
	--		Environmental damage	--	Environmental damage

1. The Cambridge Centre for Risk Studies includes notification costs as part of the breach of privacy event loss type (the CRO Forum includes notification costs as incident response costs).
2. Included in Lloyd's (2016c) Cyber Core Data Requirements (also agreed by AIR Worldwide and RMS)

Source: AIR Worldwide (2016a); Cambridge Centre for Risk Studies (2016); Advisen (2017); Department of Homeland Security (2015).

Data for managing accumulation risk

A third critical element in quantifying cyber risk exposure is assessing the potential for correlation (accumulation) risk. In the case of natural catastrophe or terrorism modelling, this can mostly be accomplished by understanding the geographical location of buildings and infrastructure exposed to damage as most natural catastrophes and terrorism attacks will only affect a limited geographical area.[9] Cyber risk, on the other hand, could be correlated on a global basis given the dependence of companies around the world on common technologies and service providers.

As noted above, modelling firms and other insurance sector organisations are developing a broad range of scenarios to help insurance companies understand their exposure to incidents that could lead to correlated losses. For example, RMS has recently released new data exfiltration, financial theft, cyber extortion, denial of service attack and cloud service provider failure scenarios involving widespread impacts across a broad range of companies (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). RMS has also developed several scenarios related to physical damage (e.g. cyber induced fires in commercial office buildings or industrial plants, explosions on

oil rigs, cargo theft and regional power outages) (Carrier Management, 2017). AIR Worldwide's modelling software provides capacities to model data theft, vulnerable or unsupported software, denial-of-service attacks, cloud service provider failure, payment processor failure, domain name server provider failure, cyber extortion, blackouts, internet service provider failure and a compromise of public key infrastructure (e.g. encryption keys, certificate authentication, etc.) (AIR Worldwide, 2016b). JLT Re has developed a number of scenarios based on various types of information technology outages (JLT Re, 2017). As noted above, Lloyd's has committed to developing 8-10 accumulation scenarios to help its syndicates manage accumulation risk (Lloyd's, 2016a).

Equally important is the collection of data to allow for the mapping of potential accumulation risk. Several respondents to the OECD questionnaire indicated that they are collecting such information through the underwriting process (e.g. the type of software that is being used). As outlined in Table 5.1, the AIR Worldwide and Cambridge Centre for Risk Studies data schemes recommend collection of various data points that could support the assessment of accumulation risk, including data related to the identification of cloud service providers, IP addresses and registered domain names, as well as various indicators of the business interruption impact of a failure of a company's internet service provider, cloud service provider or payment system service provider.

Addressing the challenges to understanding cyber insurance coverage

As noted in Chapter 4, misunderstanding about the need for - and utility of - cyber insurance coverage is likely to be an important impediment to demand for such coverage.[10] The misunderstanding results from both the difficulty in determining where there may be gaps in terms of the coverage provided by traditional policies, as well as the complexity (and wide diversity) of stand-alone cyber insurance coverage terms and conditions. There are a number of potential approaches to addressing these issues (and a few examples of efforts to do so) ranging from building awareness about coverage offered in the market to market and regulatory initiatives aimed at promoting (and/or ensuring) harmonisation/standardisation of coverage terms and conditions.

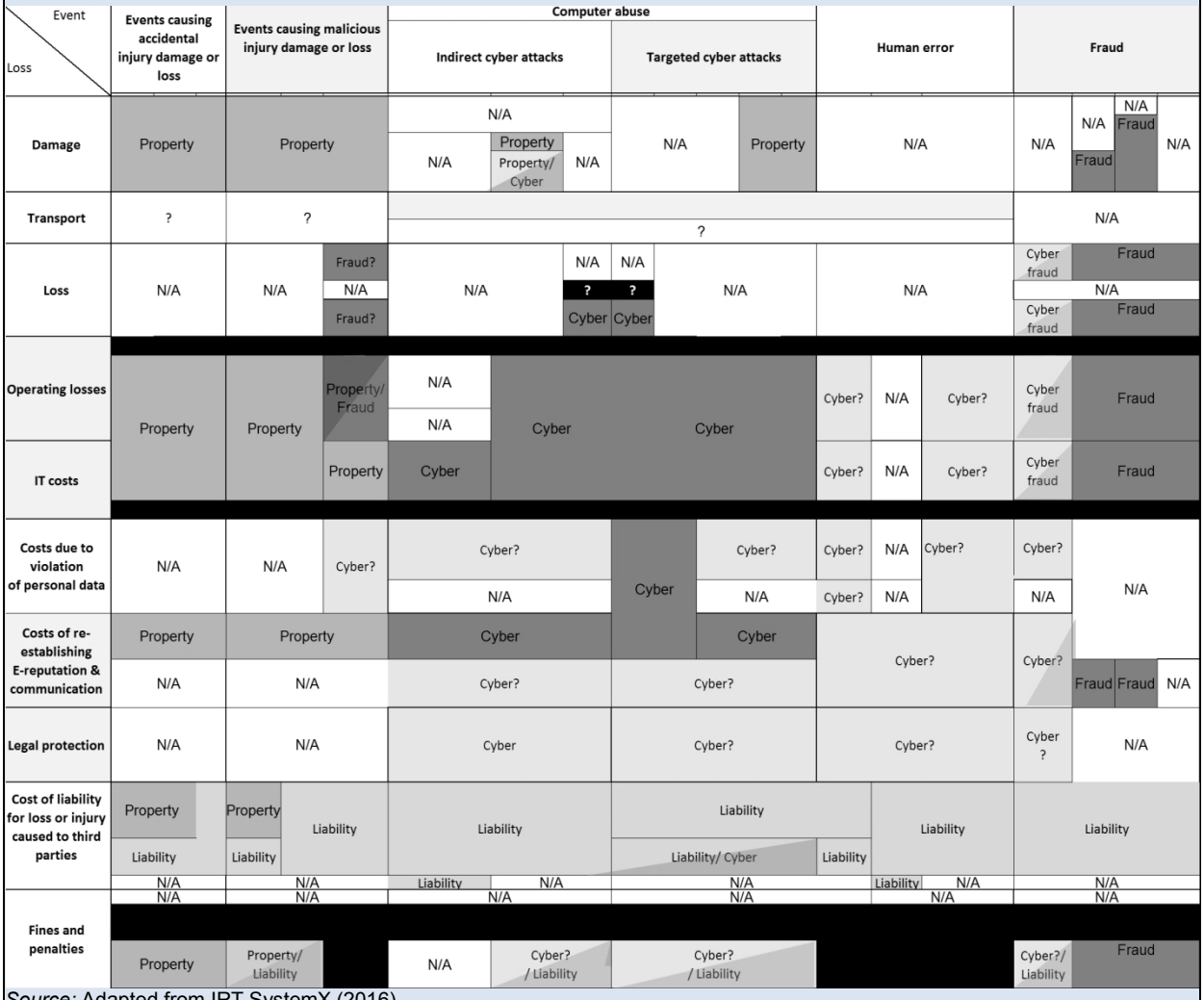
Insurance brokers play a critical role in helping companies identify the coverage needed and the form of coverage best suited to their needs. The brokers and broker associations that responded to the OECD questionnaire identified various methods to raise awareness of cyber risks and coverage options among their clients, including conferences and seminars, publications and customer surveys. One brokerage specifically mandates all of its brokers to discuss cyber coverage upon renewal of their policies and offer an indication of the premium they may expect. This is consistent with other surveys that found that the vast majority of brokers (close to 90%) play an active role in educating their clients about cyber risks (Council of Insurance Agents and Brokers, 2016). Similarly, comments from insurance underwriters highlighted the role of brokers in educating clients and their efforts to ensure that brokers had sufficient knowledge of the cyber insurance products available in the market. Many insurance associations have also developed educational materials for business on protecting against cyber risks and available insurance options, including in France ("*Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise: TPE, PME, vous êtes concernées!*"), the United Kingdom ("Making Sense of Cyber Insurance: A Guide for SMEs"), Canada ("Cyber Liability" website) and the United States ("Cybersecurity and identity theft coverage: The state of the industry") (Fédération française de l'assurance, 2017; Association of British Insurers, 2016; Insurance Bureau of Canada, n.d.; Insurance Information Institute, n.d.).

In some countries, different stakeholders have come together to provide greater clarity on the insurance coverage of cyber risk. In France, for example, representatives of the business community, brokers, insurance companies, reinsurance companies, legal firms and government collaborated on a research project aimed at providing clarity on types of cyber risks, where these risks are covered by different insurance policies and any gaps that might exist (see Box 5.3).

Box 5.3. **Building awareness on the insurance coverage for cyber risk: France**

In France, a research group involving business, re/insurance companies, researchers and government agencies was established by a public research institute (IRT System X) to examine how companies can better measure and manage their exposure to cyber risk, including through risk transfer to re/insurance markets. One outcome of the project was the development of a matrix outlining the types of potential losses that companies could face as a result of cyber incidents and the types of insurance policies that would normally provide coverage for those losses based on practices in the French insurance market (a simplified version of that matrix is provided in Figure 5.1). The research led to the identification of important gaps in coverage in the market in areas such as reputational losses, ransoms, and fines and penalties (similar to other markets). It also to the establishment of a larger working group that aims to make specific recommendations on how to improve cyber resilience and risk coverage.

Figure 5.1. **Insurance coverage for cyber risks in France**



Source: Adapted from IRT SystemX (2016).

A number of insurance sector respondents to the OECD questionnaire identified the need for further harmonisation (or standardisation) of cyber insurance coverage. The Geneva Association (2016), a research institution funded by large insurance companies, has also indicated that it might be "important to establish standards with regard to definitions, coverages and pre-coverage risk assessment" as a means to address challenges to the development of the cyber insurance market (particularly as new companies enter the market). Some have also suggested that more harmonisation in terms and conditions could facilitate market entry (and therefore capacity and competition) as new entrants could build policies based on standard language and reduce the potential for claims disputes (Deloitte, 2017). However, other respondents highlighted the risks of any regulatory intervention aimed at achieving standard terms and conditions for cyber insurance, noting that such an intervention could impede innovation and choice in the market and also risks becoming quickly irrelevant (or in need of update) as a result of the fast-evolving nature of cyber risk.

As noted in Chapter 3, there are some indications that market development has led to increased harmonisation across policies (although significant variation is still the norm). There have been suggestions that an increasingly competitive market will continue this trend towards uniform terms and conditions (The Geneva Association, 2016). Some market practices, including product development/packaging by brokers, reinsurance companies, the Insurance Services Office and even modelling firms, could encourage greater harmonisation. Automation of product sales through websites could also play a role in increasing harmonisation (at least one company has launched a comparison engine for cyber policies in the United States (Sclafane, 2016)). Some insurance associations are also supporting greater harmonisation of policy language. For example, the German Insurance Association (GDV) has released a set of non-binding model conditions for use by insurance companies offering cyber insurance coverage to SMEs (Gesamtverband der Deutschen Versicherungswirtschaft, 2017). A similar effort is also underway in Austria (Insurance Europe, n.d.).

Another potential means of reducing uncertainty would be to mandate that cyber risks be covered in traditional policies (i.e. eliminate the need for stand-alone cyber insurance products and therefore any confusion on where cyber risks would be covered).[11] As noted in Chapter 3, some insurance companies are moving in this direction by explicitly providing coverage for cyber risks in traditional policies. Companies might prefer this approach as many would consider cyber risk to be a peril like any other peril normally covered in traditional policies. However, there are a number of advantages to covering cyber risks under a stand-alone policy including the specific expertise that is being developed in understanding and quantifying cyber risks, helping companies protect against those risks and supporting their response to cyber incidents (which might not occur if cyber risk were treated as a peril in multi-peril policies). Despite the complexity noted above, stand-alone policies might also provide greater clarity on coverage of cyber risks than the general language included in traditional policies (JLT Re, 2017). There are precedents in terms of other emerging risks that were carved out of traditional policies into stand-alone specialty lines as claims experience (and loss potential) grew, such as in the case of directors and officers liability policies (Fitch Ratings, 2017).

Another approach would be to seek greater transparency at the level of individual policies on the exact scope of coverage for cyber risks. The UK Prudential Regulation Authority (2017) published a supervisory statement in July 2017 setting out its expectations for the management of cyber insurance underwriting risk which should encourage (re)insurance companies to provide greater clarity on the coverage that they

are providing for cyber risks in traditional policies (and also encourage more robust management of "non-affirmative" or "silent" coverage) (see Box 5.4).

Box 5.4. **Prudential Regulation Authority supervisory statement on cyber insurance underwriting risk**

In July 2017, the Bank of England Prudential Regulation Authority (PRA) issued a supervisory statement outlining its expectations with respect to the management of cyber insurance underwriting risk. The statement applies to all UK non-life insurance and reinsurance groups (including the Society of Lloyd's and managing agents) and includes cyber insurance underwriting risk related to both affirmative (explicit) and non-affirmative (implicit or "silent") coverage of cyber risks.

The supervisory statement sets out the PRA's expectation that companies are able to identify, quantify and manage both types of cyber exposure and will have clear Board-level strategies and risk appetite statements for these risks (such as strategies for managing non-affirmative cyber risk, rules related to the overall amount of coverage provided and/or limits for specific industries). It sets out that, at a minimum, companies should be able to provide management with clear articulations of their risk appetite, exposure metrics for both affirmative and non-affirmative exposure and stress testing approaches for potential loss aggregation at a return period of up to 1 in 200 years).

It also sets out specific expectations for the management of non-affirmative cyber risk (defined as "insurance policies that do not explicitly include or exclude coverage for cyber risk") aimed at reducing unintended exposure to cyber risk, suggesting that companies should: (i) offer explicit cover and adjustthe premium accordingly; (ii) introduce robust wording exclusions; or (iii) attach specific limits to the coverage provided. Companies are able to offer coverage for cyber risk in traditional lines of business without a corresponding premium increase although the PRA would expect a comprehensive assessment of the implications of offering such coverage and suggests that the coverage be made explicit in policy wordings.

Source: Prudential Regulation Authority (2017)

Other approaches to supporting greater market capacity

While improving capacity to quantify cyber risks and addressing the challenges to understanding cyber coverage are likely to be the most important means to improving insurance market capacity, other approaches have also been suggested. These include various types of tax incentives to: (i) encourage insurance purchase; (ii) support the accumulation of reserves by insurers to cover peak risks; or (iii) support transfer of cyber risks to capital markets (Swiss Re, 2017; Eling and Wirfs, 2016). In the United States, a *Data Breach Insurance Act (H.R. 6032)* has been introduced in Congress to provide tax credits equal to 15% of the cost of cyber insurance premiums (subject to the adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity) (Council of Insurance Agents and Brokers, 2016). Some have also suggested that mandatory purchase requirements may be necessary for cyber risks, particularly for liability risks (Swiss Re, 2017) which, if effectively enforced, would ensure a sufficient pool of insureds (and thereby support insurability).

Several analyses have noted the potential benefits of an insurance pool for addressing market capacity issues (Swiss Re, 2017; Eling and Wirfs, 2016; Carbone and Ryan, 2016), such as:

- *Increased market capacity:* Pooling of risks creates diversification benefits that would allow the pool to carry a higher level of risk than the sum of risk that can

be covered by its members individually (Eling and Wirfs, 2016). A pooling mechanism might also facilitate the entry of smaller firms that wish to gain experience in the market while limiting their liability (Swiss Re, 2017). The diversification benefits and reduced uncertainty inherent in a large pool might also lead to lower prices for coverage (Eling and Wirfs, 2016).

- *Harmonisation of coverage:* Pooling mechanisms would normally only pool the risks from similar (if not identical) coverage offerings, as the sharing of risk would otherwise be too complicated. As a result, a pooling mechanism would normally lead to greater standardisation of products (Carbone and Ryan, 2016; Eling and Wirfs, 2016).
- *Sharing of information about threats and incidents:* A pool would have access to the claims experience of its members and therefore could make a contribution to reducing the gap in data availability for underwriting and modelling cyber risk. Pool members could also share information on threats and vulnerabilities (Carbone and Ryan, 2016) and potentially the effectiveness of different security practices. A pooling mechanism that covers a large share (or all) of the market should also reduce the incentive for companies to gain market share by reducing underwriting standards (and thereby increase the contribution of insurance to the overall level of cyber security) (Carbone and Ryan, 2016).
- *Facilitating the transfer of cyber risk to reinsurance and capital markets:* By establishing a pool of similar risks, a pooling mechanism can make it easier (and less expensive) to transfer risk to international reinsurance and capital markets (see Box 5.5) (Carbone and Ryan, 2016). If deemed necessary, a pooling mechanism could also establish a structure for providing a government back-stop for cyber risk (a number of analyses have suggested that a government backstop may be necessary to: (i) cover the most extreme events which may be otherwise uninsurable (Swiss Re, 2017); (ii) cover cyber terrorism and cyber warfare (JLT Re, 2017); or (iii) as a means of reducing the overall level of uncertainty in the market (BNY Mellon, 2016)).

Pooling mechanisms have been created in a number of countries to address market capacity for covering various perils, including aviation, nuclear, terrorism, earthquake, wind and flood (or a range of natural perils). Pools have also been established for particular business lines such as accident and health in the United States in the 1970s (Carbone and Ryan, 2016), environmental liability in Italy and directors and officers liability coverage in Germany (Eling and Wirfs, 2016). Some pools have been established on a temporary (or renewable) basis and have been abolished as the market developed (e.g. the US accident and health reinsurance pools (Carbone and Ryan, 2016)). However, most have become quasi-permanent organisations leading many to suggest that an exit strategy would be difficult to implement. Pools can also limit market competition and innovation (Carbone and Ryan, 2016) and many pools operate with premiums that are not differentiated by level of risk.

Given the significance of liability in cyber losses, another approach to increasing market capacity might be to restrict (or otherwise reduce) the potential liability that companies might face as a result of a cyber incident (and therefore reduce the potential maximum losses that insurers could face). In the United States, for example, the *SAFETY Act* adopted after the September 11th terrorist attacks limited the legal damages that firms

providing anti-terrorism technologies could face (where those technologies had been approved by the Department of Homeland Security) (Swiss Re, 2017). Changes to the framework for establishing liability could also reduce the potential liability that companies face, for example, by limiting the amount of compensation that can be provided where no damages have been identified, requiring that defendant's legal fees are paid by plaintiffs when lawsuits are not successful or limiting the role of litigation funding - although these kinds of interventions may have other unintended consequences.

Box 5.5. **Insurance-linked securities covering cyber risk: challenges**

Insurance-linked securities (ILS), such as catastrophe bonds, sidecars, industry-loss warranties and other instruments, were developed in the 1990s and have played an increasing role in providing coverage for peak losses (given the much larger potential for capital markets to absorb losses) (an assessment of their use in the context of other catastrophe perils is provided in OECD (2011)). ILS have mostly been issued to cover property catastrophe risks although products have also been issued for other business lines, including life, accident and health, casualty lines and even operational risks in one recent case (Swiss Re, 2017). The development of the ILS market has benefitted from increasing confidence in the models and industry loss estimates that underpin many ILS issuances as well as from the availability of high-quality meteorological, hydrological and geological data that can also be used as a trigger for payouts.

The potential for issuing ILS to cover cyber losses faces a number of challenges, not least the lack of available data and modelling (let alone confidence in that modelling) (Swiss Re, 2017; Amaral, 2016) and the lack of standard definitions (Morris, 2017). Long-tail, unpredictable liability risks, which are often the most substantial part of cyber losses, tend to be less attractive to capital markets investors (Amaral, 2016). There is also a higher potential for the triggering event to have an impact on bond and equity markets, reducing the diversification benefits that have attracted investors to ILS covering property catastrophe risks. There have also been few options for a viable parametric or index-based trigger, which normally must be easily understandable and observable (from the investors' perspective) while sufficiently correlated with actual losses (from the issuers' perspective). Recently, however, PCS, a provider of industry loss estimates for other perils that are often used in the ILS market, has announced its intention to develop industry loss estimates for significant cyber incidents ("PCS Global Cyber") that will seek to aggregate claims data from the insurance industry for incidents with potential industry-wide losses above USD 20 million (Verisk, 2017). The data confidentiality breach at Equifax has reportedly been designated by PCS as the first such event for which an industry loss estimate will be calculated (Artemis, 2017).

A pooling mechanism could potentially facilitate the structuring of an ILS issuance for cyber risk by providing the possibility of triggering the ILS on an industry-loss basis or even on a proportional basis based on losses suffered by the pool. The one successful issuance of an ILS linked to operational risks (Credit Suisse's "operational risk bond")[1] involved the issuance of an insurance policy for operational risks (which defines the terms and conditions of coverage) with the operational risk bond providing a layer of coverage above the insurance policy, triggered when annual aggregate losses covered by the insurance policy exceed a certain threshold (Artemis, 2016).

1. An ILS transaction involving both cyber and terrorism risk was reported in September 2017 although the specific details of that transaction have not been publicly disclosed (Insurance Day, 2017).

Finally, insurance regulators and credit rating agencies can have an important impact on the amount of coverage the market is willing to provide. The level of uncertainty related to cyber risks - and the dearth of available data and models - have led some insurance regulators and rating agencies to take a cautious approach in their oversight of cyber risk underwriting (Carbone and Ryan, 2016). Fitch Ratings (2017), for example, has taken the view that a downward trend in pricing for cyber insurance would be a ratings concern due to the more limited availability of actuarial data relative to mature lines of business. While this caution is reasonable given the level of uncertainty, an abundance of caution could reduce the willingness of insurance companies to underwrite cyber risk.

Notes

1. For example, Marsh Cyber IDEAL is a predictive frequency and severity model for data confidentiality breaches based on past incidents (e.g. an estimate of return period for suffering from a given loss based on number and types of records held) (Marsh & McLennan Companies, 2016). Cyence has developed an economic modelling platform for predicting the frequency and severity of cyber incidents based on various company characteristics, which is reportedly being used for both underwriting and accumulation management (Marsh & McLennan Companies, 2016). JLT has developed a model for companies to measure their exposure based on various company characteristics, such as sector, number of records and security practices for data breach, loss of data, network interruption and cyber extortion incidents which, while targeted at companies (policyholders), may also be useful for insurers (JLT Re, 2017). There is also some academic work on calculating incident rates by sector (Romanosky, 2016). Commercial modelling firms are also working on the developing probabilistic models, particularly for the incident types for which there is better data (Hancock, 2017c).

2. Defined as "coverage in respect of first or third party costs, expenses or damages due to a breach (or threatened breach) of cyber security and/or privacy of data, that does not include damage to physical property."

3. Defined as "coverage in respect of first or third party costs, expenses or damages due to a breach of cyber security that includes damage to physical property."

4. The 2016 claims data report included submissions from ACE, AIG, Acent Underwriting, Aspen Insurance, Beazley CFC Underwriting, CUNA Mutual Group, Endurance Insurance, Hylant, One Beacon Technology Insurance, Philadelphia Insurance Companies, Safehold Special Risk, Travelers, United States Liability Insurance, Wells Fargo Insurance Services, XL Group and Zurich NA.

5. ISO and Perils collect data from insurance companies upon the occurrence of a natural catastrophe that meets a certain threshold, anonymises the data and then publishes industry-wide loss estimates. These estimates are often used as a trigger for capital market risk transfer instruments.

6. The AIR Worldwide (2016a) cyber exposure data standard does not include a specific categorisation related to incident type although AIR Worldwide, RMS and Lloyd's have agreed to use common peril codes in their data standards. The incident categorisation in Cambridge Centre for Risk Studies (2016), which was developed with RMS and Lloyd's, includes the common peril codes.

7. For example, the US Cyber Incident Data and Analysis Working Group includes nearly 20 incident types (and sub-types) relative to approximately 11 used by the CRO Forum and 3 used by the Cambridge Centre for Risk Studies. In addition, some incident types (e.g. physical peril, unauthorised data collection) are only included in one of the five data aggregation initiatives.

8. The Cyber Core Data Requirements developed by AIR Worldwide, RMS and Lloyd's includes a few common data points related to company attributes, including sector, number of employees, annual revenue, number and types of confidential records, internet business interruption potential and identification of cloud service providers. These are reflected to some extent (although not completely) in the current AIR Worldwide and Cambridge Centre for Risk Studies data schemes.

9. For the purposes of managing contingent business interruption exposures, some models are beginning to assess risks related to disruptions in global supply chains which could have implications far beyond a particular geographic region.

10. Chapter 4 also discussed challenges in terms of cyber risk awareness and particularly the need for companies to invest in quantifying their exposure to cyber risk. There are several examples of ways to address these challenges, from awareness campaigns to the efforts of brokers to help companies quantify their exposures, including through the use of models (which also related to the data challenges outlined in the previous section). A comprehensive discussion of these issues was deemed to be outside the scope of this report.

11. The opposite is also possible - i.e. mandate that all cyber risks be excluded from traditional policies.

References

Advisen (2017), *Advisen's Cyber Dataset (January)*, Advisen Ltd., www.advisenltd.com/wp-content/uploads/2017/01/201701_Advisen-Cyber-Dataset.pdf.

AIR Worldwide (2016a), *Cyber Exposure Data Standard and Preparer's Guide*, AIR Worldwide, www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/index.htm.

AIR Worldwide (2016b), *AIR Cyber Risk Solutions*, AIR Worldwide.

Amaral, R. (2016), "Cyber Risks and ILS", *Risk & Insurance*, 15 October, http://riskandinsurance.com/cyber-risks-ils/.

American Insurance Association (2016), *Re: National Protection and Programs Directorates' Cyber Incident Data Repository White Paper (24 May)*.

Artemis (2017), "PCS designates Equifax hack as first Global Cyber Index event", *Artemis news articles*, 13 September, www.artemis.bm/blog/2017/09/13/pcs-designates-equifax-hack-as-first-global-cyber-index-event/.

Artemis (2016), "Operational Re, Credit Suisse's op-risk cat bond, settles at CHF220m", *Artemis news articles*, 26 May, www.artemis.bm/blog/2016/05/26/operational-re-credit-suisses-op-risk-cat-bond-settles-at-chf220m/.

Association of British Insurers (2016), *Making Sense of Cyber Insurance: A Guide for SMEs*, Association of British Insurers, London, www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/cyber-insurance/making-sense-of-cyber-insurance-a-guide-for-smes.pdf.

Bishop, S. (2017), "Cyber Incident Data Capture & Sharing in Practice", Presented at OECD Expert Workshop on Improving the measurement of digital security incidents and risk management, 12-13 May, Zurich, www.oecd.org/sti/ieconomy/Bishop%20ORX_OECD%20Presentation_Final_110517.pdf.

BNY Mellon (2016), *Insurance Linked Securities - Cyber Risk, Insurers and the Capital Markets*, Bank of New York Mellon.

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

Carbone, W. and T. Ryan (2016), "Cyber liability insurance: As the market heats up, is it time to cool off in a pool?", *Milliman Insight*, 23 May, http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/.

Carrier Management (2017), "The Latest Launches From Chubb, Liberty Mutual and RMS", *Carrier Management*, 6 April, www.carriermanagement.com/news/2017/04/06/165942.htm.

Carrier Management (2016), "Ironshore Adds U.S. Homeland Security Assessment to Cyber Policy", *Carrier Management*, 24 February, www.carriermanagement.com/news/2016/02/24/151398.htm.

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

Deloitte (2017), *Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market*, Deloitte University Press.

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.

Department for Culture, Media and Sport (2016), *Cyber Security Breaches Survey 2016*, Department for Culture, Media and Sport, London.

Eling, M. and J.H. Wirfs (2016), *Cyber Risk: Too Big to Insure?*, Institute of Insurance Economics, University of St. Gallen.

European Commission (2017), "State of the Union 2017: The Commission scales up its response to cyber-attacks", *European Commission - Fact Sheet*, 19 September, http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm.

Fédération française de l'assurance (2017), *Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise : TPE, PME, vous êtes concernées!*, Fédération française de l'assurance, Paris, www.ffa-assurance.fr/content/anticiper-et-minimiser-impact-un-cyber-risque-sur-votre-entreprise-tpe-pme-vous-etes-0?parent=79&lastChecked=384.

Gesamtverband der Deutschen Versicherungswirtschaft (2017), *GDV stellt Musterbedingungen für Cyberversicherung vor*, Gesamtverband der Deutschen Versicherungswirtschaft, Berlin, www.gdv.de/2017/04/gdv-stellt-musterbedingungen-fuer-cyber-versicherung-vor/.

Hancock, R. (2017), "Cyber risk modellers look to next generation probabilistic models", *Insurance Day*, 11 May, www.insuranceday.com/ece_incoming/cyber-risk-modellers-look-to-next-generation-probabilistic-models.htm.

Harrington, J. (2017), "Cyber Insurance: Many Choices Now That There Is No Choice", *MyNewMarkets.com*, 27 April, www.mynewmarkets.com/articles/182994/cyber-insurance-many-choices-now-no-choice.

Insurance Bureau of Canada (n.d.), *Cyber liability (website)*, www.ibc.ca/ns/business/risk-management/cyber-liability, accessed 13 October 2017.

Insurance Day (2017), "Hiscox Re transfers cyber risk to ILS investors", *Insurance Day*, 14 September.

Insurance Europe (n.d.), *Cyber insurance (website)*, www.insuranceeurope.eu/cyber-insurance, accessed 13 October 2017.

Insurance Information Institute (n.d.), *Cybersecurity and identity theft coverage: The state of the industry*, www.iii.org/article/cybersecurity-and-identity-theft-coverage-the-state-of-the-industry, accessed 13 October 2017.

Insurance Journal (2017), "Allianz Partners with Cyence to Expand Capabilities in Cyber Risk Analysis", *Insurance Journal*, 27 September, www.insurancejournal.com/news/international/2017/09/27/465584.htm.

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).

JLT Re (2017), *Unlocking the potential of the cyber market: JLT Re Viewpoint*, JLT Re, London.

Lloyd's (2016a), *Lloyd's Cyber-Attack Strategy*, Lloyd's, London.

Lloyd's (2016b), *Realistic Disaster Scenarios: Scenario Specification (January 2016)*, Lloyd's, London.

Lloyd's (2016c), "Cyber Core Data Requirements", *Lloyd's Risk Insight*, Lloyd's, London, www.lloyds.com/news-and-insight/risk-insight/emerging-risks-team/cyber-core-data-requirements.

Lloyd's (2015), *Lloyd's Risk Codes: Guidance and Mappings (April)*, Lloyd's, London.

Marsh & McLennan Companies (2016), *MMC Cyber Handbook 2016: Increasing resilience in the digital economy*, Marsh & McLennan Companies.

Morris, I. (2017), "Insurance-linked securities and cyber risk", *Property Casualty 360°*, 29 September, www.propertycasualty360.com/2017/09/29/insurance-linked-securities-and-cyber-risk.

NetDiligence (2016), *2016 Cyber Claims Study*, NetDiligence.

OECD (forthcoming), *Review of surveys on digital security risk management practices in businesses*.

OECD (2016), "Enabling the Next Production Revolution; The Future of Manufacturing and Services", Interim Report, Meeting of the OECD Council at Ministerial Level, 1-2 June 2016, Paris, www.oecd.org/mcm/documents/Enabling-the-next-production-revolution-the-future-of-manufacturing-andservices-interim-report.pdf.

OECD (2013), *Guidance for improving the comparability of statistics produced by Computer Security Incident Response Teams (CSIRTs)*, OECD Working Party on Security and Privacy in the Digital Economy, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en.

OECD (2011), *Risk Awareness, Capital Markets and Catastrophic Risks*, Policy Issues in Insurance, No. 14, OECD Publishing, http://dx.doi.org/10.1787/9789264046603-en.

Office of the Superintendent of Financial Institutions Canada (2013), *Cyber Security Self-Assessment Guidance*, 28 October, www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx.

Prudential Regulation Authority (2017), *Cyber insurance underwriting risk: Supervisory Statement SS4/17 (July)*, Bank of England, London, www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss417.pdf.

Risk Management Solutions (2014), *Terrorism Modelling 101*, Risk Management Solutions, Inc., www.rms.com/blog/2014/12/17/terrorism-modeling-101/.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2017), *2017 Cyber Risk Landscape*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol 2 (2), pp. 121-135.

Sclafane, S. (2016), "How to Sell Cyber Insurance Online; CyberPolicy.com Set to Launch in July", *Carrier Management*, 30 May, www.carriermanagement.com/news/2016/05/30/154818.htm.

Swiss Re (2016), *Cyber: in search of resilience in an interconnected world*, Swiss Re, Zurich.

Swiss Re (2017), "Cyber: getting to grips with a complex risk", *sigma*, No. 1/2017, Swiss Re, Zurich.

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

US Chamber of Commerce (2017), *Principles for Fair and Accurate Security Ratings*, 20 June, www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

Verisk (2017), *PCS Global Cyber (website)*, www.verisk.com/insurance/products/property-claim-services/global-cyber/, accessed 13 October 2017.

Chapter 6

Supporting the cyber insurance market through better policies and regulation

This chapter provides a set of recommendations on policy and regulatory measures that could be implemented to improve the development of the cyber insurance market. Governments could contribute to the availability of data on past cyber incidents, forward-looking analyses on the changing nature of the risk and on the effectiveness of security practices, including through the development or promotion of cyber security standards. Governments should also closely monitor the market developments and consider if there is a need to intervene to encourage greater clarity on coverage or to support the management of accumulation risk.

The insurance market for cyber risks is developing rapidly although there are a number of signs of continued market immaturity, including the relatively small market size and low levels of penetration as well as the limited (and highly-variable) coverage that is offered at higher prices than other insurance lines. This is the result of a high-level of uncertainty among both policyholders and insurance companies about the future evolution of cyber risk. The insurance sector, including insurance companies, reinsurers, brokers and their associations, are investing significant efforts into reducing this level of uncertainty, including through partnerships with cyber security firms and public sector organisations, although further coordination and information sharing could improve the functioning of the market.

The public sector could make several contributions to reducing the uncertainty that impedes the development of the cyber insurance market. This includes both supporting the availability of the historical data and the forward-looking analysis necessary to improve the understanding of cyber risk as well as encouraging greater clarity for policyholders about the level of coverage provided for cyber risk in insurance policies. **Given the potential contribution that insurance can make to cyber risk management, governments should consider the development of the cyber insurance markets as a component of their strategies and policies for digital security risk management.**

Governments could support the availability of the incident reporting data, threat analysis and risk management expertise necessary to reduce uncertainty about cyber risk exposure and allow for the development of probabilistic pricing and exposure management models:

- ***Incident reporting*:** The characteristics of the policy, legal and regulatory framework can have important implications for the level of disclosure of cyber incidents. The legal and regulatory framework for **privacy protection**, and particularly the existence of notification requirements for privacy violations, has important implications for the availability of information on data confidentiality breach incidents. The much longer experience with notification requirements in the United States, for example, has provided the time-series data necessary for the development of probabilistic and advance pricing models in support of underwriting and exposure management.

  Securities legislation and regulation, particularly **disclosure requirements** for public companies, can play a role in increasing data availability for a broader set of past incidents (i.e. beyond data confidentiality breaches) although experience in the United States suggests that robust guidance and enforcement may need to accompany regulatory requirements. **Sectoral regulators and supervisors** could also make a potential contribution to the availability of data on past incidents, where: (i) incidents are reported to supervisors; (ii) they do not face legal impediments to sharing incident information; and (iii) where there is a volume of incidents that is sufficient to provide anonymity. Governments should examine whether regulatory agencies could make a material contribution to data availability and whether any impediments to data sharing exist.

  Incident repositories are being developed, or have been established on a pilot basis and could make an important contribution to improving the availability of data on incidents. However, there are a number of obstacles to information sharing that need to be overcome, including identification of an **appropriate data controller** and establishment of **security standards** that have the confidence of repository participants. In some countries, specific **legal protections** might also be a necessary condition for sharing incident information. A particular challenge for insurance companies relates to sharing information on policyholder incidents, which, if it can be overcome, could provide a significant (and increasing) source of data as the penetration of cyber insurance coverage continues to grow. The insurance sector experience in **claims data aggregation** could potentially be useful in this regard.

  Finally, the full benefits of improved notification, disclosure and information sharing will only be maximised if there is sufficient **harmonisation across categories and definitions** of cyber incidents (or at least a means to map across the different sources of information). While some insurance companies have collaborated on the development of a common taxonomy, use of this taxonomy is far from universal. The OECD has recently launched an initiative to bring together representatives from the various government providers of data on cyber incidents and the insurance sector, as part of its mandate to improve the evidence base for information security and privacy policies following the 2016 Cancun Ministerial on the Digital Economy. A first ***Expert Workshop on improving the measurement of digital security incidents and risk management*** was organised in May 2017 to begin addressing data collection and sharing challenges across the public and private sectors. (More information on the expert workshop is available at: www.oecd.org/sti/ieconomy/improving-the-measurement-of-digital-security-incidents-and-risk-management.htm.)

- ***Threat analysis*:** The ever-changing nature of cyber risk places limits on the usefulness of past incident data for predicting future losses. A significant level of uncertainty about cyber exposure is likely to remain for the foreseeable future as operations and processes continue to be digitalised - highlighting the need to ensure a robust understanding of how threats are evolving. Governments have significant access to information on operational threats, through information sharing exchanges established with the private sector and as a result of the activities of dedicated computer security incident response teams. Specific operational threat information may have limited value for insurance companies (other than for the purposes of protecting their own networks) although analyses of **trends in tactics** could be useful in helping insurance companies understand the evolution of cyber risk.

- ***Risk management expertise*:** A key challenge to understanding exposure to cyber risk is the complexity involved in measuring the **effectiveness of different security technologies and practices**. Governments can contribute to reducing this complexity in two main ways: (i) by contributing to - or encouraging - **certification, testing or rating of security technologies or providers**; and (ii) by establishing and/or encouraging adherence to **standards for the management of cyber risk**, either generally applicable or targeted to specific sectors, supported by guidance to facilitate implementation. Consistent with the ***OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity*** (2015), governments should foster active participation among relevant stakeholders in initiatives aimed at sharing knowledge and expertise on risk management practices. While a number of considerations govern the setting of risk-based premiums, insurers can encourage adherence to standards by providing premium reductions where implementation of such standards has a meaningful impact on risk reduction.

As outlined in Chapter 4, the complexity of cyber policies along with the misunderstanding about whether cyber risk is covered in traditional policies is likely to be a significant barrier to demand for cyber insurance. The potential for "silent" coverage to be found in traditional policies could also be impeding the willingness of insurance companies to expand the coverage they provide for cyber risk. Different companies are taking different approaches to providing coverage for cyber risks, with some "expanding" the boundaries of traditional policies to include cyber risks while others are expanding the scope of stand-alone cyber insurance policies beyond the data confidentiality breaches that most stand-alone policies were developed to respond to. Both approaches have benefits for policyholders. Inclusion of cyber risk in traditional policies may be preferred by corporate risk managers who might be concerned about the coverage gaps created by the broad use of cyber exclusions (while preferring the higher limits that traditional policies usually offer). However, the development of stand-alone policies creates clearer incentives for cyber risk quantification and management, and has leveraged the expertise of external service providers, which might not occur if cyber risk were treated as one of many perils in a traditional policy. While divergence in approaches to coverage provides significant choice in the market, it also exacerbates the confusion for policyholders on where to seek coverage for cyber risks.

At a minimum, governments need to **closely monitor the development of the cyber insurance market** to ensure that policyholders are provided with as much clarity as possible on available coverage and that no significant gaps in coverage emerge as a result

of market practices. The Prudential Regulation Authority's recent Supervisory Statement on cyber insurance underwriting risk should have a positive impact on **reducing the level of non-affirmative or silent coverage of cyber risks in traditional policies** offered by UK (re)insurers and therefore providing greater clarity on when cyber is, or is not, covered. The insurance market, including through insurance associations, should also encourage greater clarity about coverage through the **development of common definitions and terminology on the risks and losses** that may or may not be covered in cyber insurance policies, while allowing for different approaches in terms of which risks and losses are covered in individual policies. Insurance regulators should ensure that efforts to improve clarity and consistent terminology are being implemented by the market and can support that effort by reviewing policy language for unclear or misleading terms and conditions. They can also reduce the uncertainty that is created by different approaches to the **insurability of fines and penalties and ransoms** in different jurisdictions by working towards a common approach to these issues. The insurance sector can also improve the relevance of cyber insurance for policyholders by addressing demand for coverage for **reputational losses** and **first party intellectual property losses**.

Providing the necessary data for modelling and reducing the complexity of coverage terms and conditions will not be sufficient to encourage the development of the cyber insurance market if policyholders do not improve their capacity to measure and understand their exposure to cyber risk. Oversight of cyber risk at board-level could ensure that sufficient resources are devoted to **quantifying cyber exposure**. Governments can encourage **corporate governance practices** that ensure appropriate board oversight of cyber risk.

While the financial impacts of cyber incidents that have thus far occurred have been generally manageable (both by the insurance sector and affected companies), there is significant concern about the potential for **significant accumulation losses**. These concerns impede the expansion of insurance coverage by insurance companies that wish to avoid both the possibility of large accumulation losses as well as the negative repercussions of taking on too much exposure from a ratings and/or supervisory perspective. Governments should **examine options for managing cyber accumulation risk**, including the potential role of risk pooling. When designed properly, risk pools can contribute to **enhancing private market capacity** by limiting each company's exposure and taking advantage of the diversification benefits and reduced uncertainty inherent in a large pool. A forward-looking examination of this issue could help avoid the kinds of market disruptions that occurred after Hurricane Andrew in 1992 and the September 11th terrorist attacks in 2001.

References

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD, Paris, www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

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.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(21 2017 06 1 P) ISBN 978-92-64-28213-1 – 2017

Enhancing the Role of Insurance in Cyber Risk Management

The digital transformation of economic activities is creating significant opportunities for innovation, convenience and efficiency. However, recent major incidents have highlighted the digital security and privacy protection risks that come with an increased reliance on digital technologies. While not a substitute for investing in cyber security and risk management, insurance coverage for cyber risk can make a significant contribution to the management of cyber risk by promoting awareness about exposure to cyber losses, sharing expertise on risk management, encouraging investment in risk reduction and facilitating the response to cyber incidents. This report provides an overview of the financial impact of cyber incidents, the coverage of cyber risk available in the insurance market, the challenges to market development and initiatives to address those challenges. It includes a number of policy recommendations which support the development of the cyber insurance market and contribute to improving the management of cyber risk.

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264282148-en***.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases.
Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

THE LONDON BOOK FAIR WINNER
INTERNATIONAL EXCELLENCE Awards 2017
IN PARTNERSHIP WITH THE PUBLISHERS ASSOCIATION

ISBN 978-92-64-28213-1
21 2017 06 1 P

9 789264 282131