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" 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). 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 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 attack in the previous 12 months (Hiscox, 2017).

Figure 1.2. Perceptions of the level of cyber risk

![Perceptions of the level of cyber risk](image)

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

Figure 1.3 Increasing frequency of cyber incidents

![Increasing frequency of cyber incidents](image)

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. 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
1. GROWING CYBER RISK AND THE CONTRIBUTION OF INSURANCE TO CYBER RISK MANAGEMENT

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 Quarterly (May), McKinsey & Company,
www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rising-
strategic-risks-of-cyberattacks.

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-

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).


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

PwC (2014), Managing cyber risks in an interconnected world: Key findings from The
Global State of Information Security® Survey 2015, PwC,

PwC (2015), Turnaround and transformation in cybersecurity: Key findings from The
Global State of Information Security® Survey 2016, PwC,

