ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES
www.oecd.org
BETTER POLICIES FOR BETTER LIVES DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

OECD PROJECT ON CYBER RISK INSURANCE

April 2016

Introduction

1. Cyber risks pose a real threat to society and the economy, the recognition of which has been given increasingly wide media coverage in recent years. Cyber insurance is one of the risk transfer mechanisms to address the financial costs that arise from cyber attacks, assisting in the recovery of those affected. In addition, cyber insurance can support risk reduction by promoting mitigation and prevention measures.

2. Since 2013, major corporations and retailers like Target, Home Depot, Sony, JP Morgan and Anthem Health have fallen victim to massive cyber-attacks on their databases. Consequential losses and disruptions impact not only the affected corporate. They can also affect persons whose data, identities and privacy may have been exposed or identities stolen, and beyond, with the whole ecosystem of corporations and networks at risk. The prevalence of cyber attacks has led managers to admit that not all cyber attacks can be prevented.

3. Cyber risk is high on many corporations' and governments' security agenda. The recently published National Security Strategy of the United Kingdom places cyber attack (including by other states, organised crime and terrorists) as one of the four highest priority risks for the United Kingdom over the next five years. On 13 February 2015, the White House Summit on Cybersecurity and Consumer Protection proposed several initiatives to make cybersecurity a national priority, with President Obama urging companies and governments to take stronger action to protect businesses and consumers from attacks and protect individuals' privacy. Meanwhile, the legal and regulatory environment is being strengthened in many countries in order to protect consumers and incentivise companies to adopt a more proactive protection strategy.

4. These factors have driven the growth of the market for cyber protection, including through privacy and security products and services. They also explain the emergence of a specialised insurance market for cyber risks. While cyber insurance is offered to some extent in the United States and other markets, it remains limited relative to the magnitude of risks and market potential. Cyber risk insurance involves fast evolving and correlated risks which could be difficult to insure, accompanied by limited modelling capability and awareness of coverage and exclusions. Further, cyber risk can be compounded by the aggregation and correlation of risks. These barriers may be impeding the provision of this financial protection, leaving wide gaps in coverage and raising questions on how to better protect the privacy of businesses, individuals, and the intellectual property and databases of corporations and how to appropriately assign responsibility for damages after a breach.

5. The importance of cyber insurance is increasing, but there has yet to be an in depth analysis of policy issues surrounding the development of a sound cyber insurance market with market conduct safeguards.

6. This project proposes to look at various facets of the market and the issues that may arise as the market evolves and develops. The OECD's Insurance and Private Pensions Committee (IPPC) can draw on its expertise in the areas of disaster and terrorism risks management to support the analysis of this market given the similarity of some of the issues (e.g. challenges to insurability of risks, widespread underinsurance, etc.), as well as draw on relevant work on financial consumer protection.

7. The project will consist of three reports which will be carried out over the next 18 to 24 months. The outcome of the project can be amalgamated and discussed in an event on the topic in 2017.

Project on cyber risk insurance

8. The project on cyber risk insurance would aim to better understand cyber risk and insurance, and how cyber security and financial protection against losses from cyber attacks could be improved as the market develops. Such a policy discussion would require a better understanding of the market, and how the improvements in awareness of risks and potential mitigation options expected to result from further penetration of cyber insurance might enhance the level of cyber security more generally. The project is thus focussed on areas with possible regulatory and policy implications, as well as areas in which greater understanding of policies might benefit the industry. This project does not aim to standardise market practices *per se*, but provide a basis to enable greater transparency of cyber insurance contracts and subsequent improved risk awareness by policyholders.

9. This project will contain three reports (which could constitute chapters in a final publication):

- Cyber risk insurance: the market and nature of available insurance coverage;
- Awareness of cyber risks and the role of insurance in risk measurement, mitigation and prevention; and
- Regulatory and policy issues relevant to the development cyber insurance markets.

10. In particular, the project will try and focus to some extent on how consumer protection can be enhanced with cyber insurance, in particular in relation to third party liability, and what elements support or hamper this. In addition, the policy discussion could lead to insight into public policy measures and considerations that could affect the provision of cyber insurance, including possible areas of international cooperation going forward.

11. For its part, the International Association of Insurance Supervisors (IAIS)'s Financial Crime Task Force will be looking at "understanding developments in the cyber insurance market," and will be developing an Issues Paper which explores the area of cyber-crime risks to the insurance sector. The Issues Paper will focus on the protection of the private information of insurance customers and the mitigation of fraud committed through cyber-attacks and will identify areas for further work in providing guidance for supervisors. This project will be structured to compliment the work that is expected by the IAIS.

12. For the purpose of the project, a short questionnaire will be sent to delegates to collect information on the relevant initiatives on cyber security and cyber insurance. In addition and more broadly, a questionnaire will be sent to insurers to collect information on their gross written premiums, scope of protection and exclusion, risk assessment methods, pricing, level of claims paid out, and challenges moving forward.

I. Cyber risk insurance: the market and nature of insurance coverage available

13. The first part of the project would provide an overview of the cyber insurance market as it stands, market segments which may not benefit from coverage as well as the insurance policies being offered, in particular the scope of coverage and exclusion included in those policies. The intention would not be to look into the trend of cyber attacks, which are discussed extensively by other expert groups, but to look at the level of financial protection being offered. The market is at its nascent stage and currently mainly focussed on corporate policyholders. However, as it develops, and as the frequency and severity of attacks change, policies being offered are likely to evolve, which may have implications that require careful consideration.

14. The types of policyholders taking up the cyber risk option will be analysed, feeding into the discussion in the second part of the project on consumer protection aspects. Although cyber insurance is a relatively new product and policy language is yet to be standardised, the report does not intend to standardise policies, but look into ways in which protection is being offered on the market, and the elements that are being incorporated into policies. By identifying elements typical in core cover and more specific optional cover, the direction in which the market is developing can be analysed as well as how transparency of coverage may be improved. Ambiguities in the definition of cyber risk, the scope of insurance cover, and triggers activating payment may create uncertainties on the exact perimeter of events insured, and can lead to gaps in coverage and a general lack of understanding of cyber insurance coverage and benefits.

15. The report will in particular try to look at some sample policies in detail, to understand the extent of their coverage and premium levels. The level of coverage and premium levels would also provide an indication of the types of cyber insurance policyholders. Practices in the market which would improve the definition of cyber risks and the extent of insurance coverage, in terms of transparency and comparability of contracts, could also be discussed. In particular, whether smaller firms, which lack technical expertise to conduct in-depth audits of their cyber vulnerabilities, are able to understand the extent of their cyber insurance coverage and whether adequate protection is being offered will be considered.

16. An additional facet will be to understand any barriers to the provision of cyber insurance. While some markets, in particular the US, are more developed, other markets have not developed in tandem with the potential risk exposure of the market. Understanding the background to this lack of development may assist in understanding the market conditions required to providing cyber insurance.

17. The report will analyse the extent to which terrorism risk insurance would cover cyber terrorism. While terrorism risk insurance may not, by default, cover cyber risks, some of the policies may have the possibility of covering a large extent of cyber attacks attributed to terrorism.

18. The report will therefore include the following sections:

- Overview of the market size and penetration levels: market capacity, take-up rates, characteristics of policyholders
- Trends in cyber insurance policies: extent of cover (events/financial limits) and exclusions, pricing
- Sample policies for cyber risk: protection and premium levels
- Cover of cyber terrorism losses by terrorism risk insurance

II. Risk awareness of cyber risks and the role of insurance in risk measurement, mitigation and prevention

19. This part of the project will look into how cyber insurance could contribute to risk measurement, mitigation and prevention, and consider some consumer protection issues. Cyber insurance provides an opportunity for preventative measures to be encouraged through the use of risk-based premiums and provision of advice on risk mitigation. Insurers could also contribute to the measuring of cyber risk. The possibility of security audits to determine premium levels has been discussed during the Committee meeting, and could lead to better privacy and security of information technology systems.

20. Cyber insurance can provide an incentive to enhance cyber security. A better understanding of the current practices of risk assessment and mitigation, what is being taken into account for premiums and the possible correlated risks could lead to better preparation towards cyber attacks by potential policyholders. The possibility of insurers carrying out in-depth cyber security audits to assess their client's security tools and practices across all activities – i.e., as part of underwriting and exposure monitoring, policyholders could be required to undertake audits – could amplify the risk reduction benefits of insurance. Insurers can incentivise prevention and mitigation by reduced premiums and extensions on coverage. Insurers can also contribute to the measurement of risk through modelling efforts and better data collection.

21. The OECD's Working Party on Security and Privacy in the Digital Economy is likely to also look into issues relevant to cyber insurance, being the expert group on security and privacy, and a possible collaboration on this topic could lead to a better informed discussion in this area. The Committee may wish to have a horizontal approach in this part of the project, possibly working with the Working Party on Security and Privacy in the Digital Economy on security measures which could support risk mitigation and underwriting.

22. While corporates, in particular large ones, may have the institutional and financial capacity to develop appropriate security measures towards cyber risk, in addition to purchasing cyber insurance, smaller corporates and individuals remain exposed to cyber risks both directly and indirectly, with the potential of correlated risks. They would be exposed directly through possible cyber attacks on their information technology system, and indirectly through privacy breaches of systems with their personal details. Also, cloud technology, which many businesses and individuals widely use, is exposed to cyber risks, although improved security at the cloud level may increase overall security. While policyholders of cyber insurance are, at least in the current market, mainly companies, those affected are often consumers/clients who are dependent on the security measures taken by the company to whom they provide their personal details. It would be beneficial for the Committee to consider policy issues arising from breaches of privacy and how cyber insurance provides coverages. For example, from understanding how cyber insurance policies cover liability arising from cyber breaches towards individuals, to how damages could be reasonably covered, current practices could be reviewed to better understand good practices going forward. In particular, the types of security measures which would address risk mitigation and prevention, and support underwriting of the risks, could be discussed.

23. The report will include the following sections:

- The risk mitigation and prevention measures incorporated into cyber policies and how risk-based premiums are being determined: security audits and governance arrangements
- What efforts are being made to better measure cyber risk including correlated accumulation risk
- First and third party liability of cyber insurance: protection being offered and its adequacy

- Consideration of how security and consumer protection could be enhanced through cyber insurance

- Awareness of cyber insurance and consumer protection: how awareness can be raised for better protection

III. Regulatory and policy issues related to the development cyber insurance markets

24. While cyber insurance is a relatively new market, the number of cyber attacks and breaches of personal data has led to increased interest in policy measures related to protecting against cyber attacks. While measures taken specifically to address cyber insurance have been limited, there have been a number of policy discussions relevant to cyber insurance.

25. This part of the project will look into relevant regulatory and policy issues related to the development of cyber insurance markets. Discussions that took place in the first two parts of the project will be reflected upon to consider areas in which further discussion and policy measures may be necessary.

26. The US and UK have been actively engaging in policy discussions on how to address the ascent of cyber insurance, in particular for attacks on critical infrastructure with possible national security implications. How the government wishes to support improved security and address financial losses as a result of cyber attacks will have an important implication on the development of cyber insurance. Relevant regulatory measures, or market best practices being promoted to improve cyber security and risk transfer of cyber risk, will be discussed, including the nomination of a chief (information) security officer, introduction of mandatory cyber insurance in limited cases and possible tax incentives. The role of data protection legislation and notification requirements will also be analysed.

27. The absence of relevant data series on past losses, the limited actuarial information available on the frequency and magnitude of actual and potential cyber security incidents, and the ever-changing form of cyber threats are major challenges to cyber risk insurability. How transparency and monitoring of the market could be improved could be reviewed.

28. Some general observations on how the solvency of insurers might be affected by the provision of cyber insurance and whether there could be a sector wide impact will be analysed. While both solvency and stability impact of cyber insurance are not an immediate policy concern, the lack of data, risk modelling capability and expertise could create barriers to appropriately monitor the market. An analysis of how a large and/or multiple attacks might implicate insurers could also be considered. As the IAIS will be considering possible supervisory guidance in regard to cyber attacks, this report will observe how cyber risk-related claim payouts could impact insurers' solvency.

29. The report will include the following sections:

- Regulatory discussions and measures taken in relation to cyber insurance, including notification requirements in case of a breach

- Monitoring approaches that could improve transparency and monitoring of the cyber insurance market

- Possible insurer solvency and stability considerations

- Possible policy recommendations and/or issues for the future

For interest and contact:

Mamiko Yokoi-Arai (tel: +33-1 45 24 75 26 | mamiko.yokoi-arai@oecd.org)
www.oecd.org/daf/fin/insurance/cyber-risk-insurance.htm