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

