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
EXECUTIVE SUMMARY

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.**