OECD
INSURANCE POLICY INSIGHTS

BUILDING A SUSTAINABLE CYBER INSURANCE MARKET

The Role of Public Policy and Regulation

Leigh Wolfrom

In an era of increasing reliance on digital technologies – and the growing exposure to cyber risks that accompany that reliance – cyber risk insurance can make an important contribution to providing financial protection and helping policyholders prevent and respond to cyber incidents. This summary shares some of the findings from two examinations on the role of public policy and regulation in supporting the development of a sustainable cyber insurance market.

In recent years, an insurance market for cyber risks has emerged to provide financial protection (mostly to businesses) for some of the digital security and privacy risks that have accompanied the growing use of data and digital technologies. While growing quickly – with some estimates suggesting that the market will double or triple in size in the next few years – the market remains small relative to other lines of commercial insurance business. A lack of understanding of cyber exposure, limited data on past incidents, misunderstandings about when cyber risk is covered in a given insurance policy and what types of exclusions might apply along with a significant (and difficult to quantify) exposure to accumulation risk have all contributed to caution among insurance companies in extending coverage and reluctance among policyholders to acquire this coverage.

The OECD has been examining impediments to the development of a sustainable cyber insurance market since early 2017. In February 2018, the OECD organised a conference with the aim of building some consensus around the role of different stakeholders in addressing the impediments to the market's development. In these two reports, the OECD examines the role that public policy and regulation could play in helping address some of these challenges.

Enhancing the availability of data for cyber insurance underwriting

For insurance and reinsurance companies, data on past incidents is a critical input into estimating the likely frequency and magnitude of losses and for calibrating the models that are often used for premium pricing and capital allocation. Limited claims experience as well as the evolving nature of both cyber risk and the public policy and regulatory frameworks that drive many types of cyber losses create challenges for cyber insurance underwriting - and ultimately impede policyholders' understanding of their insurance coverage needs and insurance companies' willingness to extend significant coverage.

Within the insurance sector – and among many regulators and supervisors – there is increasing support for the establishment of a repository of incident and claims data that could leverage the claims experience of multiple (re)insurers (potentially from multiple countries) to address the gap in historical claims experience and potentially provide a sounder basis for underwriting cyber insurance coverage. More data on claims and

incidents could also help in identifying emerging loss trends more quickly. It could also support competition by facilitating market entry in a market that is characterised by a few large insurers with significant market share.

Data sharing has a long history in the insurance sector to support underwriting, detect fraud and even improve risk management in some countries. Competition authorities in many jurisdictions have recognised the benefits of data sharing within the insurance sector, leading them to provide exceptions for this form of industry cooperation subject to conditions on the form and use of data and access arrangements. The types of data that would need to be shared for cyber insurance underwriting – which is focused on business policyholders –would also remove the concerns related the sharing of protected personal information.

Claims and incident data sharing initiatives for other perils have generally been led by the industry, whether through dedicated service providers or on the initiative of insurance associations. The insurance sector is now taking steps to do the same for cyber incidents. Insurance regulators and supervisors should support these efforts by eliminating any regulatory barriers to the sharing of relevant insurance policy information and potentially encouraging insurance companies to participate in these initiatives (particularly the large cyber underwriters for whom the benefits of data sharing may not be as clear). Ultimately, greater knowledge of cyber incidents and impacts will contribute to the development of the cyber insurance market and support risk management.

Encouraging clarity in cyber insurance coverage

Digital security risks are a relatively new and evolving source of losses for the insurance sector which has led to adjustments in coverage offered across a number of lines of business and the emergence of specific products and endorsements to provide coverage for these risks. These adjustments in insurance coverage have led to some confusion among policyholders about whether they need to acquire specific coverage for cyber risk and the types of incidents and losses that their insurance will cover.

One of the most important areas of policyholder misunderstanding has been related to whether the property, liability, crime/fidelity and kidnap and ransom insurance policies that many businesses have acquired will also provide coverage for losses caused by cyber incidents. These types of policies were developed before digital security risks were a significant concern and many of the policy wordings used do not provide any explicit reference to these risks as either a covered peril or exclusion. Uncertainty about whether cyber risk is covered in these lines of business – and overlaps between what is covered in these lines of business and dedicated cyber insurance – will remain for some time. However, there is an emerging consensus in the insurance sector on the need to either provide cyber coverage on an explicit (affirmative) basis or exclude it – driven partly by supervisory guidance on this issue in the United Kingdom. Insurance regulators and supervisors in other countries should also encourage this effort to provide greater clarity.

The source of a cyber-attack – and specifically whether the perpetrator is a state-sponsored or terrorist group – can also have implications on whether the losses from an incident are covered by a property, liability or cyber insurance policy. For now, many stand-alone cyber insurance policies will reimburse losses resulting from attacks attributed to these groups for losses that are otherwise covered under the policy – although this is changing. Property and liability policies often exclude war and/or terrorism or provide coverage for terrorism backed by a terrorism (re)insurance programme although not all of these programmes have adapted their coverage to address the possibility of cyber-terrorism attacks. As the insurance market moves to comprehensively exclude losses resulting from destructive politically-motivated cyber attacks, governments will need to ensure that no important gaps in coverage emerge. At the invitation of the Australian Reinsurance Pool Corporation (ARPC), the OECD recently completed a report examining the potential coverage gaps that might arise in Australia and internationally for cyber-terrorism and other politically-motivated and destructive cyber attacks.

The other important source of policyholder (and insurer) misunderstanding relates to the impact of public policy and regulation on the types of cyber-related losses that can be legally insured. Two types of losses in particular – administrative or civil fines and penalties imposed for privacy or cyber security violations and the ransoms paid to cyber-extortionists – are not legally insurable in some jurisdictions. This is often based on the argument that insurance coverage for these losses would be counter to public order. The cost to companies of fines and penalties for violating privacy protection and cyber security regulations is clearly reduced if these losses are reimbursed by an insurance policy – while the payment of ransoms is likely to improve the profitability of this form of (criminal) business. . However, there is uncertainty around when fines, penalties and ransoms can be insured – which might only come to light in the event of litigation – and ways for policyholders and insurers to find coverage even where restrictions are relatively clear. Insurance regulators and supervisors should provide a clear statement on the insurability of fines, penalties and ransoms which should be based on a careful consideration of the costs and benefits to society of allowing reimbursement for these types of losses.

References

OECD (2020), Enhancing the Availability of Data for Cyber Insurance Underwriting

OECD (2020), Encouraging Clarity in Cyber Insurance Coverage

OECD (2020), Insurance Coverage for Cyber-Terrorism in Australia

OECD work on insurance policy issues:www.oecd.org/pensions/insurance

For more information about the OECD's Insurance Policy Insights series, please contact Mamiko.Yokoi-Arai@oecd.org.

www.oecd.org/pensions/insurance