Enhancing the role of insurance in cyber risk management

OECD

2018

The cyber insurance market: Responding to a risk with few boundaries

On the occasion of the OECD Conference on Unleashing the Potential of the Cyber Insurance Market in Paris on 22-23 February 2018, the OECD's Bill Below and Leigh Wolfrom look at some of the challenges to insuring cyber risk.

With the growth of cybercrime, and intensive media coverage of privacy breaches and ransomware attacks over the last year, could complacency about cyber risks soon be a thing of the past? While consumers remain dismally bad at protecting themselves (e.g. the low uptake of Two-Factor Authentication), boardrooms are increasingly hungry for protection, with larger companies taking the lead.

The numbers alone should motivate any firm, large or small, to rev up its cybersecurity game: by 2019, cybercrime is expected to cost businesses over USD 2 trillion, up from USD 500 million in 2015 (Juniper Research, 2015). Companies are investing more in cybersecurity technology and services, registering a 7% increase in spending from 2016 to 2017. The global expenditure for these technologies and services (other than insurance) for 2018 is estimated to reach USD 93 billion. These head-spinning numbers are big, almost to the point of abstraction. As it stands, the most potent wake-up call motivating investment in cyber risk management seems to be having one's own company attacked—a dangerous strategy, to say the least.

Common types of cyber incidents		Potential losses
 **Data confidentiality breach** (3rd party data)	e.g. unauthorised disclosure of third party personally identifiable information	Incident response costs Breach of privacy compensation Reputational damage Regulatory and legal defense costs Fines and penalties Directors and officers liability
 **Data confidentiality breach** (own data)	e.g. theft of trade secrets	Intellectual property theft Directors and officers liability
 **Operational technology malfunction**	e.g. manipulation of a control system	Business interruption Fines and penalties Physical asset damage Bodily injury and death Directors and officers liability
 **Network communication malfunction**	e.g. denial-of-service attack on a server leading to the unavailability of a company website	Business interruption Reputational damage Directors and officers liability
 **Inadvertent disruption of 3rd-party system**	e.g. transmission of malware to 3rd party system	Network security failure liability Regulatory and legal defense costs
 **Disruption at external service provider**	e.g. disruption to software application provided by cloud service	Contingent business interruption
 **Deletion or corruption of data**	e.g. malware that leads to the deletion of data on connected computers	Data and software loss Regulatory and legal defense costs Products liability Directors and officers liability
 **Encryption of data**	e.g. ransomware that impedes access to data or a network until a ransom is paid	Cyber ransom and extortion Directors and officers liability
 **Cyber fraud/theft**	e.g. illegitimate financial transfer is made as a result of a network intrusion or social engineering	Financial theft and/or fraud Directors and officers liability

Growth in the cyber insurance market is a sure sign of firms' increasing awareness of cyber risk and appetite to transfer exposure. But buying the right policies can be challenging, particularly for companies whose understanding of their own vulnerabilities may be sketchy. A lack of similar terminology and different approaches to offering coverage, along with the complexity of the policies themselves, add to the frustration and dampen buyer demand.

The challenge of understanding exposure

Even large firms who are 'on it' can underestimate their exposure and the coverage needed. Equifax's cyber risk coverage was estimated between USD 100 million and USD 150 million, yet total losses will be significantly higher than that (Bloomberg, 2017). Beyond this potentially expensive gap, the Equifax case offers a chilling demonstration of the impacts of a large-scale data breach. In the five trading days following the Equifax breach, the company lost USD 3.5 billion in market value, its share price bottoming out with a 30% drop (share prices have since clawed back about 20% as of this writing). Damage to its brand, disruption caused by post-breach management changes, regulatory scrutiny and impending fines, the cost of offering a year of free credit monitoring services to 143 million affected customers and at least 24 proposed class-action lawsuits add to the challenges facing the company. Settling those suits alone is expected to cost the company some USD 200 million (Pettersson, 2017). The latest available quarterly results showed profits down 27% (Bloomberg, 2017).

If big firms can fall victim to cyberattacks, smaller firms are particularly vulnerable. While the penetration level for stand-alone cyber insurance is above 50% or more among large companies in most countries, take-up by SMEs is in the single digits.

A lack of historical cyber incident data (and direct experience) is a big problem, preventing insurers from developing the predictive models they depend on to set accurate premiums and exposure models. This, in turn, reduces the willingness of insurance companies (and reinsurers) to extend significant amounts of coverage. It also leads to exclusions and sub-limits that customers may find unappealing. What data is collected primarily exists in the isolated repositories of diverse entities without ready access or the harmonisation required for comparison.

A risk with few boundaries

The evolving nature of cybercrime means risk models may have to look beyond historical data. With new forms of malware and other technologies targeting ubiquitous operating systems, common applications, cloud services and hardware platforms, a single criminal act can potentially scale to global dimensions. Last year's WannaCry ransomware attack may be a harbinger of things to come. Propagating through legacy Windows systems, Wannacry infected over 200,000 computers in 150 countries. Indeed, the potential for accumulation risks may discourage some insurers and reinsurers from entering the cyber insurance market at all. The bottom line: uncertainty and correlated risks lead to higher prices and limited coverage levels.

Remediating the lack of sharable, harmonised data on cyberattack incidents is critical if the insurance industry is to leverage its risk management expertise to help countries address the risks inherent in the transition to a digital economy. The policy and legal environment can provide information which can diminish the level of uncertainty. Particularly in countries with limited notification or disclosure requirements, governments should consider the contribution such requirements could make to improving the availability of data on cyber incidents. On another level, a number or actors in the insurance sector are examining the value of different protection technology and practices with the aim of improving their ability to assess risk at companies. While assessing the effectiveness of cyber security technologies is challenging, there may be scope for governments to encourage certification and standards for the management of cyber risk.

Enabling the cyber insurance industry

With the Equifax breach and the WannaCry ransomware attacks, 2017 may have been a tipping point in organisational awareness of cyber risks. Right on its heels, the discovery of Meltdown and Spectre, two security weaknesses built into the microprocessors of virtually all the world's computers, was the first bad news of 2018, and could spell trouble for years to come. Let's ensure that policies are in place to enable the cyber insurance industry to become a driving force supporting national cyber risk mitigation and resiliency.

Links and data sources

Bloomberg (2017), Equifax's Insurance Is Likely Inadequate for Breach, www.bloomberg.com/news/articles/2017-09-09/equifax-s-insurance-said-likely-to-be-inadequate-against-breach

Juniper Research (2015), Cybercrime will cost businesses over $2 trillion by 2019 www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

OECD (2018), OECD Conference on Unleashing the Potential of the Cyber Insurance Market, www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, www.oecd.org/daf/fin/insurance/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm

Pettersson, E. (2017), "Legal Experts See Room for Deal in Equifax Data Breach Lawsuits", Insurance Journal, 25 September, www.insurancejournal.com/news/national/2017/09/25/465299.htm

www.oecd.org/insurance

This article contributes to the OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.