amsterdam2016.eurofi.net

The role of insurance in cybersecurity and how policymakers can help

By John Scott
Zurich Global Corporate , Chief Risk Office Global Corporate Business

As society's reliance on technology increases, so cybersecurity is becoming ever more important. Innovations such as the Internet of Things and Self Driving Vehicles are exciting opportunities, but they bring risks, as consequences from cyber-attacks move beyond data breaches towards physical and bodily damage. With cyber-attacks already cost global business over $300bn per year, cybersecurity is key to harnessing the full potential of cyber technology, preventing the rising cost of cyber-attacks becoming a disincentive to invest by outweighing benefits. It is vital we get this right: a 2015 study by Zurich and the Atlantic Council estimated a $120 trillion difference to global GDP between creating an open and secure internet and an insecure, poorly regulated one in next 15 years.

Insurance has an important social and economic role in cyber security. Firstly, risk transfer provides an important part of decision making around cyber investments. Current market coverage includes third party liability costs from attacks and internal actions, as well as first party costs including business interruption and privacy breaches. Second, insurers advise on risk management and resilience measures which help to limit cyber risks. Such measures can also help to protect more intangible and less insurable assets like reputation.

However, there are a number of hurdles to the insurers fully realizing its value. This includes a lack of information on cyber risks – technical data used to price and underwrite risks is scarce and inconsistent, whilst businesses are reluctant to disclose information on attacks due to concerns over liability and reputation. Equally, whilst maximum losses would likely exceed the private market, the exact potential losses for insurers from cyber-attacks are largely unknown. This uncertainty over "accumulation risk" is a major barrier to the expansion of the cyber insurance market. Lastly, a knowledge gap exists both within the insurance industry, which requires more cyber risk management expertise and similarly through a general lack of awareness on cyber risks amongst customers, particularly SMEs.

EU policymakers have an important role in helping insurers to overcome some of these hurdles. Action falls into two broad objectives: promoting a thriving insurance market and promoting an effective global risk management framework. A thriving cyber insurance market requires a focus on raising standards, improving data, de-risking information exchange and promoting "cyber education". An effective risk management framework, allowing businesses to effectively manage their exposure to cyber risks, requires global cooperation. However, this is currently hindered by geopolitical tension. Policymakers must respond by strengthening global governance institutions

whilst insulating them from tensions. Meanwhile, the systemic nature of cyber risk should also be addressed through greater oversight and response measures.

The insurance industry can play an increasingly important role in achieving cyber security and looks forward to working with EU policymakers to realize this potential.