A Closer Look at the Chinese Cyber Risk Insurance Industry

Zhan Hao, Sharif Hendry

Recent "ransomware" attacks worldwide, including greater China, have once again brought to the fore the nascent yet potent threat "cyber risks" present as an all-encompassing enterprise risk management challenge to corporations worldwide. Concordantly, the raft of operational consequences that can potentially cascade from an attack, including the liability of directors and officers for errors and omissions, reputational and market valuation knock-on effects, and regulatory compliance issues[1], present an ever burgeoning opportunity for insurers to expand further into this potentially lucrative new line of business.

Tantamount to successful expansion of the cyber security insurance market will be insurers' ability to address the fears of market incumbents with sufficient clarity and certainty in respect of coverage, in order to exponentially develop the larger scale market. China in particular seems to present an obvious, but as yet largely untapped cyber insurance market that is at a relatively early stage of growth compared with other major jurisdictions, alongside the wider Asian economy in general. For now, its participants are mainly confined to international insurance companies providing coverage to larger businesses operating in the region. Part of the reason for this is that cyber risk related losses are relatively harder to quantify in the absence of publicly available data and an increasing proliferation of attacks, and are therefore more suitable for experienced underwriters with the ability to withstand the potential for a sequence of high loss events[2]. In addition, potential losses beyond repairing systems relating to reputational and brand damage, and the claims of multiple stakeholders, are relatively harder to quantify and call for proper controls to avoid over exposure[3]. In China, AIG has recently led the way with an 87% jump in cyber insurance policy enquiries for China (including Hong Kong) in May as compared with April[4]. This followed in the wake of the self-replicating WannaCry ransomware attack that affected over 200,000 computers globally. Despite the apparent spuriousness of such attacks, major contagion can result from the damage they can cause, extending beyond simple IT terms to affect major integrated data and

[1] http://deloitte.wsj.com/cfo/2017/07/05/cyber-insurance-understand-the-potential-trapdoors/

[2] https://www.pwccn.com/en/insurance/insurance-2020-sep2015.pdf

[3] https://www.pwccn.com/en/insurance/insurance-2020-sep2015.pdf

[4] https://www.reuters.com/article/us-aig-china-cyber-idUSKBN1AP12E

operating systems, loss or leaking of personal and sensitive information, and in some cases, affect sensitive industries such as airports and hospitals. The potential for widespread systematic disruption entails liability risks that may be inadequately covered by existing property and casualty terms with respect to D&O, professional liability and business interruption insurance, for instance. This is especially so where such terms are silent and/or untested on their application to cyber security events[5].

The widespread contagions that may accompany these events make cyber insurance particularly pertinent to China. Following an unprecedented infrastructure boom the country is now shifting towards increasing digitization and automation in various high-tech industries for which data and system integrity are paramount, and of national significance in terms of security and stability. This has been accompanied by a rise in estimated cyber-crime related losses to around USD 60 billion annually[6], second only to the US. To this end Chinese regulators have since July 2015 been introducing a series of laws and draft laws on internet controls and state access to private data, including those regulating data management in the insurance sector. The new Cyber Security Law that came into effect in June 1, 2017 is an important step in bringing cyber security norms and practices in line with global standards, particularly since compared with the US and Europe, cyber security and data management were less comprehensive overall[7]. We may have to wait further for government-led policies relating to cyber insurance, since these remain in the works for now. However, since a higher proportion of SMEs within China are leading the way in various high-tech endeavors, and may not consider cyber insurance a priority on their restricted budgets, it may be regulation that finally brings impetus to the market.

[5] http://deloitte.wsj.com/cfo/2017/07/05/cyber-insurance-understand-the-potential-trapdoors/
[6] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

[7] http://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/