briefing note 405 Nov 2019

Australia's 2020 Cyber Security Strategy

Tahiry Rabehaja[1], Denny Wan[2] and Ryan Springall[1]

The Australian Government, through the Department of Home Affairs, has called for views regarding the cyber security strategy that Australia should adopt from 2020. This strategy will be the successor to the 2016 initiative which the Government accompanied with an investment of $230 million in cyber security. The call for views consists of a series of 26 questions ranging from technical solutions to legislative discussion. Few questions in the call for views were directly related to regulation and cyber insurance. In the response that Risk Frontiers submitted to the call, we stressed that Cyber Security is a risk and thus should be managed as such. This means that whilst mitigation and deterrence are important components in risk management, insurance has a role to play as a mechanism for risk transfer and for reinforcing robust cyber security practices through pricing and policy signals. Here is a summary of the top five questions that Risk Frontiers addressed.

4. What role should the government play in addressing the most serious threats to institutions and businesses located in Australia?

To accurately price risk, insurers require a robust quantitative understanding of frequency (how often) and severity (how much financial loss). These data are often obtained through years of claims data and experience dealing with natural catastrophes, for example. In the case of cyber-risk, this understanding is currently lacking. Overcoming this deficiency will require strong and pragmatic leadership from the government to ensure a cyber-risk resilient Australian economy.

The USA is amongst the countries with well-developed cyber security laws and regulations. In addition, the US government actively encourages US businesses to implement robust cyber risk management and, in particular, promotes the incorporation of cyber insurance into their Enterprise Risk Management strategy. According to a 2018 Aon report[i], the current global cyber insurance market premium is estimated to be between 4 and 5 billion US dollars with the US accounting for more than 80% of this market. Figure 1 shows the breakout of global cyber insurance premiums. The US market is considered to be maturing while the rest of the world is developing and expected to grow. In 2018, the Australian cyber insurance market premium was approximately $60 million US dollars, which was about 2% of the global market by premium volume.

[1] Risk Frontiers

[2] Security Express

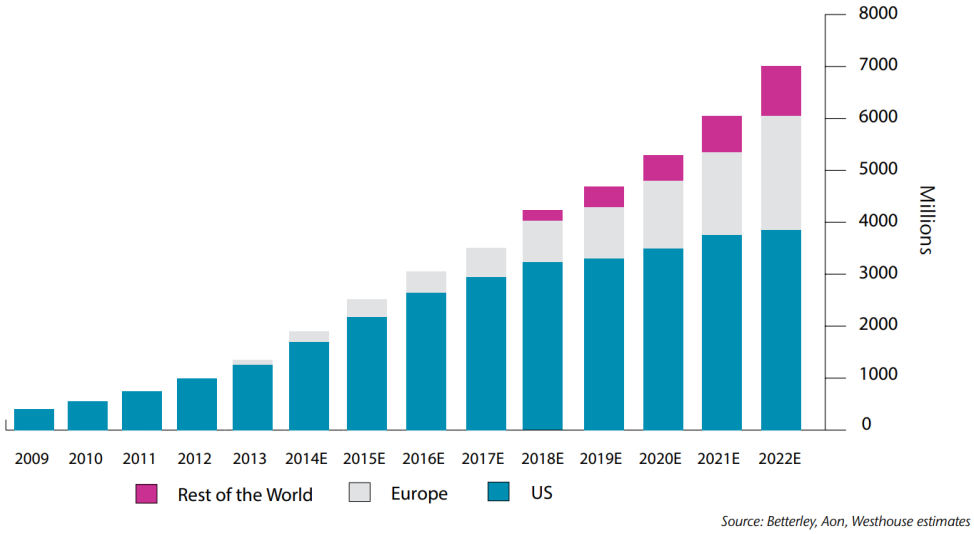

Figure 1: Measured and estimated written premiums (source: Aon Cyber Insurance Market Insights 2018).

In Australia, the recent enforcement of the Notifiable Data Breach (NDB) scheme as well as the introduction of APRA's CPS 234 regulation are positive steps towards improving the resilience of Australian businesses to cyber threats. However, more information on breach frequency and severity needs to be shared with the insurance industry to assist in understanding frequency/ severity relationships underpinning risk transfer policies and to educate businesses and the community on the value of taking up cyber insurance.

Such governmental regulations have already proven effective for other countries and regions. In the case of the US, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Federal Information Security Management Act (FISMA) form the three pillars for digital security compliance for businesses and governmental institutions.

Corresponding regulations for Australia are framed through the Privacy Act 1988 and subsequent amendments such as the NDB in 2017. However, compliance alone does not ensure resilience as shown by high profile cases such as the Target breach. At the end of 2013, hackers exfiltrated more than 100 million records containing credit card details and other Personally Identifiable Information (PII) from Target's internal network. Target was PCI compliant and deployed state-of-the-art security systems but the breach still occurred due to a third party weak link, poor network segmentation and other system misconfigurations[ii]. Target did have cyber insurance that proved useful in offsetting some of the financial losses incurred during the post-breach response period. A well-planned response is an equally important defence strategy and cyber insurance will go a long way to providing a better incident response and business continuity.

10. Is the regulatory environment for cyber security appropriate? Why or why not?

Regulatory frameworks such as the NDB primarily focus on protection of privacy. In contrast, other regulation such as the CPS 234 is more balanced due to its focus on broader information security challenges beyond the protection of PII. While only currently enforced on APRA regulated entities, CPS 234 is applicable to other organisations and presents an encouraging point of departure to lift cyber security standards in the Australian economy. The standard is principle based and non-prescriptive, offering regulated entities scope to leverage their current investment in Information Security Management Systems (ISMS) to achieve compliance.

The 2019 update of CPG 234 (guidance for implementation of CPS 234) includes some concrete best practices such as information to be presented to the business board tabled in Appendix H. Implementation of the standard can be assisted by taking advantage of a standard cyber risk quantification framework such as Factor Analysis of Information Risk (FAIR).

The FAIR methodology is a quantitative approach that provides estimates on the frequency and severity of loss events using historical data, heuristics and expert opinions. FAIR is a comprehensive methodology that provides a framework for analysing tail losses through quantitative metrics such as Value at Risk. The quantification process provides a structured approach to prioritise risk and remediate efforts based on expected reduction in potential financial loss, enabling a prudent investment culture in cyber security based on established financial management principles.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can these be addressed?

In the insurance industry, cyber-risk is broadly categorised either as affirmative (named as a risk) or as silent (covered without explicit recognition of the risk as it is not excluded). Increasingly, traditional commercial general liability and property insurance policies exclude cyber risk[iii] with insurers looking to provide explicit policies that are accompanied by robust risk management processes. However, there remains significant ambiguity, especially when it comes to attribution of a cyber-attack[ivv]. This means that cyber insurance is emerging as a stand-alone coverage and insurance companies with "silent cyber" built into their products are exploring ways to isolate that component. Current cyber insurance policies are covering a relatively wide range of costs depending on the level of coverage. A comprehensive cover will typically include direct costs associated with a post-breach response. Figure 2 shows the classification of costs due to cyber-attacks[vivii]. Blue costs are direct first- or third-party losses and are usually explicitly attributed to the cyber event. Grey costs are less tangible and hard to measure. Costs with purple outlines are currently covered by various branded cyber insurance products. For instance, asset destruction is generally covered under silent cyber.

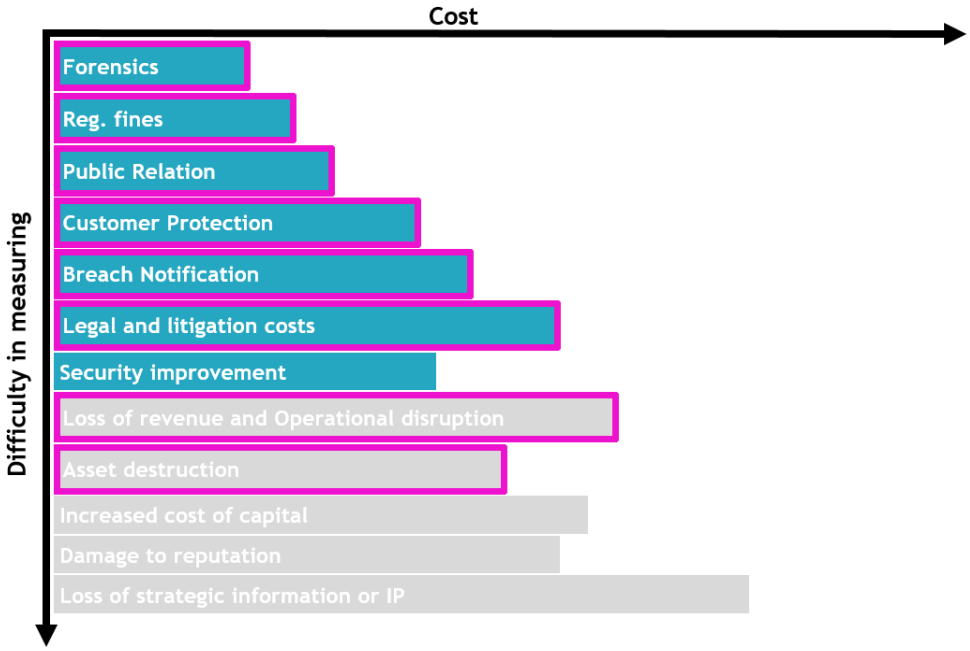

Figure 2: Costs of a cybersecurity breach (source: Risk Frontiers in-house analysis).

The first obvious observation here is that current coverage is generally restricted to direct costs and excludes intangible losses or long-term impacts such as reputational damage. One example is the 2017 Equifax data breach where losses in market share prices and subsequent security improvements were not covered by their insurance policy.

Another barrier for the growth of cyber insurance in Australia, and globally, is that cyber risk is not well understood. Brokers and underwriters lack the training and tools to quantify this emerging risk efficiently as the tools to assessing cyber risk (and hence pricing and policy construction) are different from traditional property and casualty insurance. In fact, current approaches to assessing cyber security risk rely heavily on manual assessments that greatly impede the scalability and application to small and medium enterprises. Unlike other mature risks such as those arising from natural catastrophes, cyber security risk is extremely hard to quantify due to its dynamic nature, the scale, the lack of physical boundaries upon which accumulations are analysed and the aggregate expertise required to produce a good model of the risk. This gap in cyber risk modelling has a major impact on pricing where premium prices becomes unsound or unaffordable for SMEs.

Another issue with current cyber insurance is regarding policy terms, which drives the lack of certainty in successful claims. Since cyber-insurance products are still young compared to P&C insurance, the policy terms are constantly being tested in court and usually contain explicit exclusion clauses for cases such as "act of war"[viii]. A recent example of a more subtle exclusion occurred in the court case confronting National Bank of Blacksburg to its insurer Everest National Insurance Company[ix].

The above issues and challenges can be addressed (at least partly) through:

a. Governmental initiatives including the development of a compelling regulatory framework for cyber security risk as well as the promotion of the cyber risk management with particular emphasis on cyber insurance.
b. The government should encourage and support collaboration between academia and the industry into paving the way towards better understanding and modelling of the cyber-security risk landscape as it pertains to Australian businesses. Without a proper understanding of the risk, there is only a small degree of price differentiation across different firms.
c. The government also needs to work with insurers to assist in the "attribution" process (which is important for certain policy exclusions) and potentially consider establishing a cyber reinsurance pool.
d. Finally, the government should increase awareness and provide platforms for SMEs to explore their alternatives in terms of cyber risk transfer.

16. How can high-volume, low sophistication malicious activity targeting Australia be reduced?

The first and foremost protection against high-volume and low sophistication threats is the adoption of good cyber hygiene. Credential management (password usage, multi-factor authentication for example), regular patching and employee training (resilience against phishing and frauds) are amongst the top low-cost but high return strategies to prevent attacks in this category. These types of attacks are most prevalent for lower-tier enterprises, which should be encouraged and made aware of the impact of good cyber hygiene. This cyber security strategy mirrors the public health management strategy in encouraging hand sanitation to minimise the spread of the common cold and flu viruses that help to prevent flu pandemics. Through insurance engagement, the insurance industry can provide the services as part of a broader product offering to increase cyber hygiene.

20. What funding models should Government explore for any additional protections provided to the community?

A cyber reinsurance pool is one form of funding that the Government should explore to improve confidence in the cyber insurance market, increase the resilience of the economy and community to cyber-attacks and, more generally, as a signal to build market confidence. For instance, in the UK, Pool Re was established by the insurance industry and the government as a reinsurance pool to protect insurance companies against large claims originating from terrorist incidents. Since 2018, Pool Re also covers cyber-terrorism[14]. Thus, similar extension or more innovative approaches, such as Hiscox's cyber Insurance-Linked Securities[x], can be explored through the ARPC to cover cyber-attacks on critical infrastructures. Risk Frontiers can provide more detail on these schemes if required.

briefing note 405 Nov 2019

About Risk Frontiers

Risk Frontiers specialises in the assessment and management of risk across the Asia-Pacific region. We help organisations ranging from the global insurance industry and infrastructure operators to government departments and emergency services.

Our research and expertise cover major hazards affecting the region including floods, tropical cyclones, storms, bushfires, heatwaves, coastal erosion and earthquakes. We also continue the development of a cyber risk model in partnership with the Optus Macquarie University Cyber Security Hub.

Our work with government encompasses a diversity of projects including understanding community risk perception, evaluation of resilience and recovery programs, research into catastrophic disasters and the development of resilience frameworks.

As a partner of the Australian Research Council Centre of Excellence for Climate Extremes, Risk Frontiers is well positioned to deliver the latest in climate change solutions to enhance our clients' decision making.

Rigorous, independent and data-driven, Risk Frontiers is one of Asia- Pacific's leading providers of risk management and catastrophe modelling solutions.

---

[i] Aon. Cyber Insurance Market Insights, 2018.

[ii] Xiaokui Shu et al. Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, 2017

[iii] Sasha Romanosky et al. Content analysis of cyber insurance policies: how do carriers price cyber risk?, 2019

[iv] Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.

[v] Milton Mueller et al. Cyber Attribution: Can a New Institution Achieve Transnational Credibility?, 2019

[vi] The Council of Economic Advisers. The cost of Malicious Cyber Activity to the U.S. Economy, 2018

[vii] Deloitte. Beneath the surface of a cyberattack, 2016

[viii] Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.

[ix] https://krebsonsecurity.com/wp-content/uploads/2018/07/1-main.pdf

[x] Insurance Day. Hiscox plans dedicated cyber ILS fund, 2019