Insuring Cyber Risk

Concerns about Risk

By Susie Amos and Alina Pettifer Posted on: July 7, 2016

Insurers will need to work through their concerns about cyber to remain relevant in the future, write Susie Amos and Alina Pettifer in the final instalment of this Two Part series on cyber risk.

How do we underwrite and price?

We are bombarded with cyber statistics every day. However, the available statistics are rarely directly relevant or usable in traditional insurance pricing approaches. In addition, the evolving nature of cyber risk increases the difficulty of underwriting and pricing, even when historical data is available.

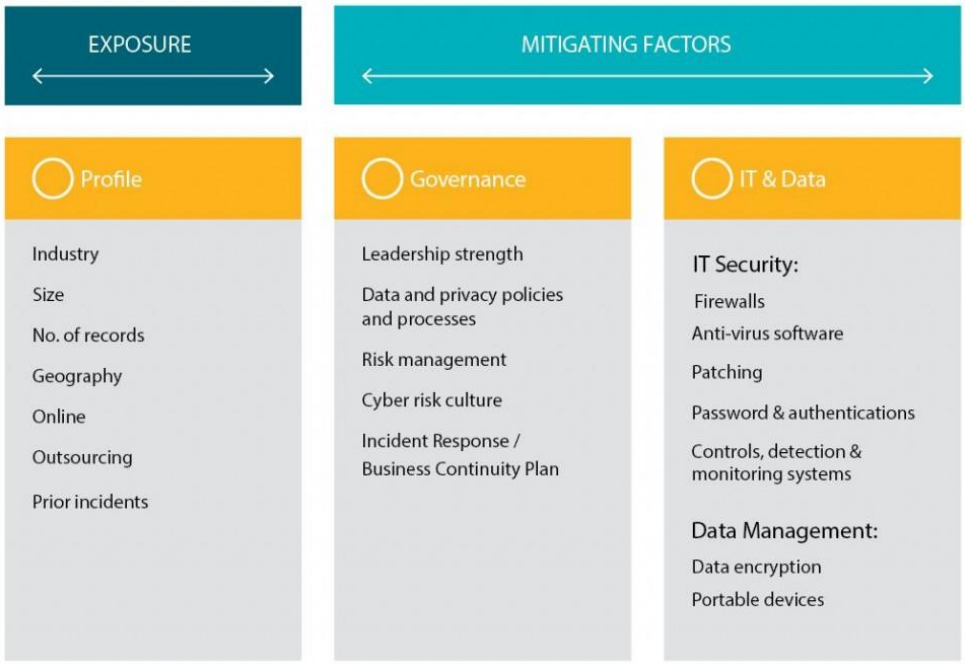
Given the immaturity of the Australian cyber insurance market, there is little claims experience. This lack of data should be a short term problem as the market matures. However, in the meantime, we need to look at ways of pricing and underwriting without perfect data.

There are currently diverse approaches to underwriting and pricing in the Australian market. We have seen up to 50 underwriting questions being asked by a single insurer, and over 200 different questions across the market. Some questions are qualitative, and can be difficult to translate into quantitative terms for pricing.

In this context it is perhaps not surprising that premium rates offered for the same risk can vary significantly – by up to a factor of four. As the market matures, we expect to see convergence in underwriting questions and in pricing.

Pricing and evaluating risk with limited data is not new to the insurance world. Products such as D&O, Political risk, Kidnap and Ransom, as well as many products written in the Lloyd's market, are priced with very limited data. A more judgement-based approach is needed, and this can be refined as experience emerges.

Do we need a new approach to evaluating risk? We think an approach which goes back to the insurance fundamentals of assessing the risk potential and mitigation can be used. The suggested key measures of exposure, and mitigating factors to be considered are shown in the diagram below.



There is data available (albeit limited) on a number of the exposure measures and mitigating factors outlined in the figure, and this can be used as a starting point to differentiate risk. The effectiveness of a business's IT security is probably the most difficult element for an underwriter to assess and translate into a price. Insurers may be able to source expertise from IT security companies – to help develop a quantified and consistent 'security vulnerability' measure to feed into underwriting.

As mentioned, it is difficult to translate the drivers of cyber risk into a price. The diagram below outlines a proposed approach. The assumptions adopted in this approach can and should be refined as experience emerges and the environment evolves.

We believe that it will be useful to set separate **likelihood** (frequency) assumptions for incidents of different types – system errors, crimeware, misuse, physical loss, web attack – as this will allow for emerging trends in any area to be reflected quickly. In a similar vein, adopting individual **severity** assumptions by incident type and type of loss (notification, legal, investigation, loss of business) will enable different expectations – and eventually, experience – to be reflected.

There is more data on the likelihood of cyber incidents, and experience is reasonably consistent across countries. Severity statistics are harder to come by, and vary significantly across jurisdictions, being dependent on local laws and regulations.

How will aggregation be dealt with?

Cyber risk poses an aggregation risk for insurers that is difficult to quantify, and this creates significant uncertainty for underwriting cyber insurance. Some cyber events can result in losses across multiple policies, products, industries and geographies – for example, power grid outage, hacking of a major investment firm or common service provider, software vulnerability, denial-of-service scams.

This potential aggregation is new to insurers and cyber catastrophe models are now being developed to assist insurers and reinsurers understand this risk. A scenario-based approach can help in understanding the potential aggregations for a given portfolio. Some realistic disaster scenarios have been specified by Lloyd's, and these could be used as a starting point.

An insurer can limit its aggregation by managing portfolio exposures and by purchasing catastrophe reinsurance. At the moment, reinsurance capacity appears to be available, but this may not continue.

How do we assess claims?

Claims management for this new product is different from the 'usual'. It requires a combination of claim specialties – including cyber forensics, cyber and privacy law, business interruption and property adjusting.

A number of the big law and audit firms have developed cyber risk specialties, and their expertise can be tapped into for assessing claims. Some of the claims assessors have similar skills to assessors of property, business interruption and liability claims.

How will risk change over time?

In the evolving digital world, insurers will need to be quick to respond to the emerging experience. This will involve monitoring trends, understanding their impacts, and responding via underwriting terms, limits and deductibles and/or price.

We see the following main drivers of change in cyber risk in the short to medium term:

Conclusion

The insurance industry is well placed to support businesses operating in the digital age, but some aspects of cyber insurance are new and are creating concerns for insurers. However, the digital age is here to stay and commercial insurers will need to work through these concerns to remain relevant into the future.

There is currently limited data available for underwriting, pricing and assessment of aggregation, but judgement-based techniques can be used (alongside the data) to evaluate levels of cyber risk. Ongoing monitoring and product responsiveness will be required as this product evolves.

Some insurers have seen the opportunities and launched into the cyber insurance space. Offerings and pricing are currently diverse, but we expect to see convergence over time.

We look forward to seeing the cyber insurance market continue to evolve and help businesses navigate the digital age.

Find out more in Part One: 'Concerns about Coverage' (http://www.actuaries.digital/2016/06/29/insuring-cyber-risk-concerns-about-coverage/) of this article series by Alina and Susie.

(http://creativecommons.org/licenses/by-nc-nd/3.0/au/)
This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivatives CC BY-NC-ND Version 3.0 (CC Australia ported licence) (http://creativecommons.org/licenses/by-nc-nd/3.0/au/).

CPD Actuaries Institute Members can claim two CPD points for every hour of reading articles on Actuaries Digital.