Pro-active cyber insurance pricing model

By Denny Wan and Petra Wildemann

The lack of historical claim data on cyber-attacks and the rapid evolution in cyber-attack methods have been cited[1] as key barriers to developing a structured approach in cyber insurance pricing. In order to overcome this constraint, newer research[2][3] has attempted to use stochastic processes (Markov and non-Markov) to describe the dynamics of attacks and use the copula approach to model the dependencies among risks. While these research models will somewhat ease the constraints from the lack of historical claim data, they cannot cope with the rapidly evolving nature of cyber-attack methods. Some research recognizes that cyber-attack differs from other form of risks in that it is primarily man-made in nature, resulting in a mis-match[4] between the insured risk and policy coverage.

A break through will require us to recognize that historical claim data for cyber incidents, even when available, will not be sufficient to inform the premium pricing strategy without corresponding cyber risk control metrics. Cyber risks are a kind of "modern risk", and they are man-made. Therefore, it is unsurprising that historical data are not available with a long-term view, such as for many catastrophic risks.

As Petra Wildemann wrote in her article "Pricing insurance in the age of cyber-risk":

> "Therein lies the dilemma: a cyber risk is priced as a man-made risk, and yet has many of the features of natural disasters with high impact and large-scale damages. This will become even more important as sovereign combatants and terrorists increasingly target their attacks on the industrial control systems of critical infrastructure, such as water authorities, energy and power generation and distribution systems, where detection can be very difficult and damage consequences existential."

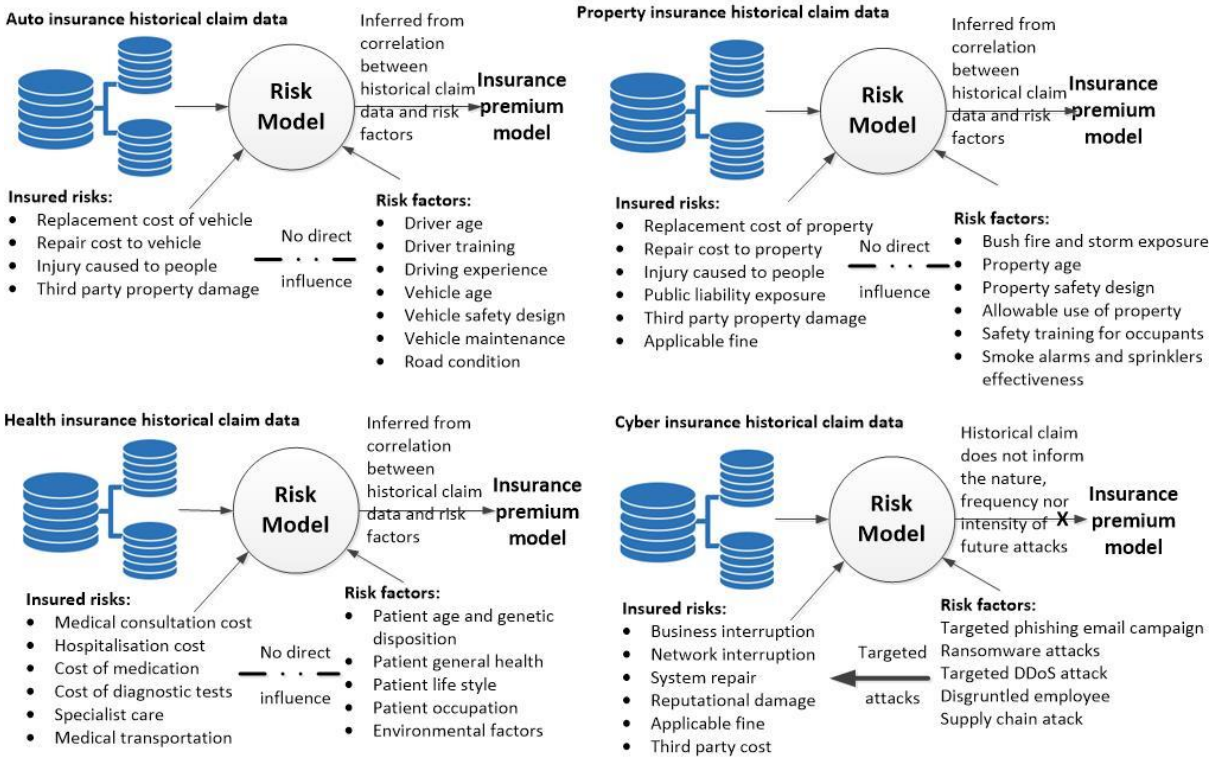
For automotive insurance, the corresponding risk metrics are the year/model of the vehicle and age/gender of the driver. For property insurance, the risk metrics may include bush fire and flood rating. In other words, the premium pricing takes into consideration special attributes of the insured risks. For these classes of insurance products, there are plenty of historical claim data which can be used to inform the pricing model using actuarial techniques.

For historical data on health insurance, the WHO data sets and many other statistical data sets are available either at internal databases within the insurance industry or externally with Universities and Research organizations'. Examples of the existence of data are given for pandemic and epidemic risks "Zoonotic Diseases: Heightened Risks to Industry and Government"[5] and "Assessing Global Risks: Pandemics and Cyber Risks" on page 14, issue 16, March 2018 The European Actuary of the AAE[6].

The most important point is that these actuarial models are designed specially to reflect on these commonly understood risk metrics.

[1] https://www.linkedin.com/pulse/cyber-risk-insurance-challenges-modelling-risks-data-age-wildemann/
[2] https://www.soa.org/Files/Research/Projects/cybersecurity-insurance-report.pdf
[3] https://www.econinfosec.org/archive/weis2007/papers/24.pdf
[4] https://www.linkedin.com/pulse/pricing-insurance-age-cyber-risk-petra-wildemann/
[5] https://www.soa.org/Library/Newsletters/Risk-Management-Newsletter/2017/december/rm-2017-iss-40-wildemann-ayscue.aspx
[6] http://theeuropeanactuary.org/downloads/TEA%2016-MRT2018-FINAL.pdf

This is highlighted in the diagram below:



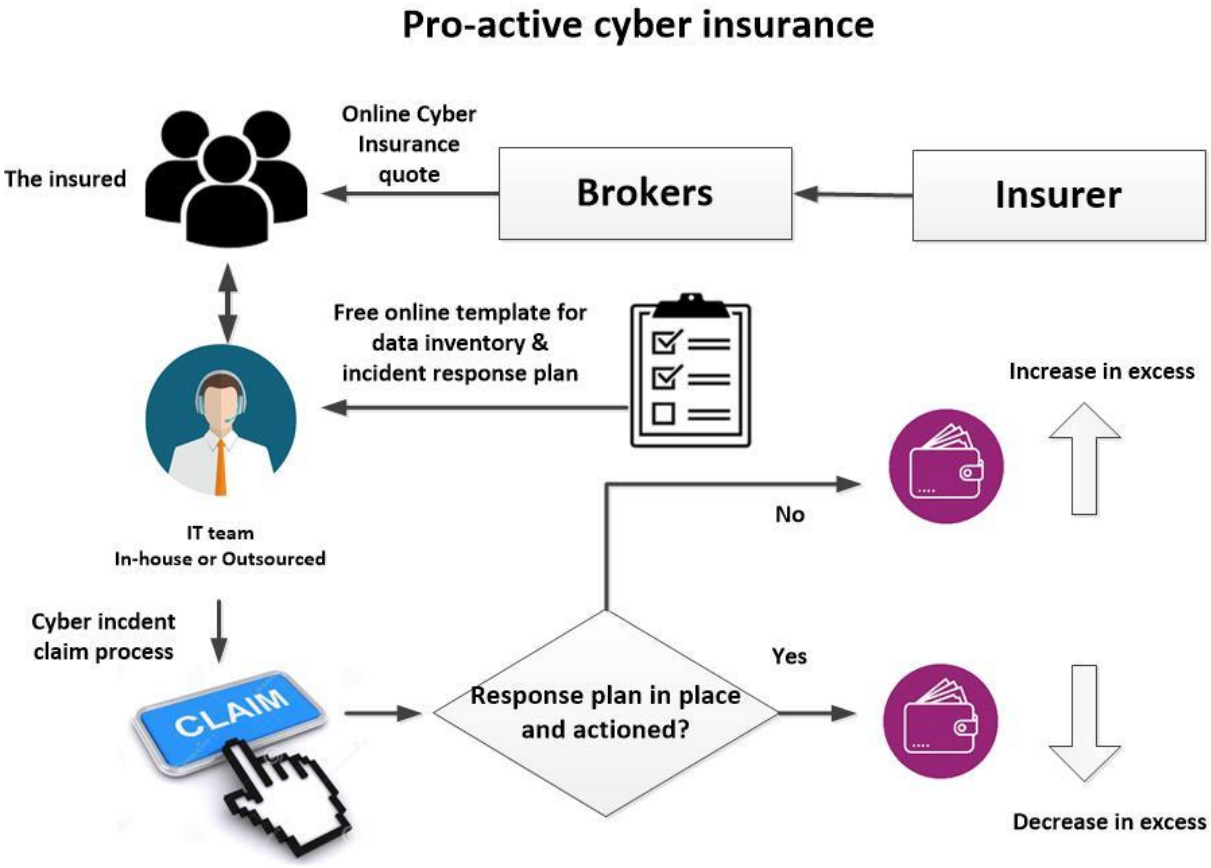
For most forms of insurance (auto, property, health etc), the risk factors evolve over a long period of time with identifiable patterns such as climate and economic changes. Most importantly, risk factors are generally not influenced by the selection of the insured risks. For example, the bush fire and storm exposure risk rating of a property is not influenced by whether the property is insured for complement replacement or only for public liability exposure. The fire and storm are still going to hit when they hit. On the other hand, cyber criminals purposely target victims whom they expect are more likely to be able and willing to pay thanks to their cyber insurance cover. Such differences in risk characteristics are highlighted by the arrows in the diagram above.

Therefore, cyber insurance policies might even encourage cyber criminals to monetize cybercrime instead of encouraging the insured to strengthen their cyber security posture. This is because insurance policies, by design, are reactive in nature, targeting the recovery process. There is limited scope in the insurance funding model to encourage and support the insured to invest in preventive cyber protection measures. In other forms of insurance policies such as property, automotive and healthcare, investment in preventive measure is often compelled through community expectations and applicable regulatory frameworks. However, there is very limited incentive for implementing preventive cyber security measures, except under executive orders[7] for protecting critical infrastructure[8][9].

[7] https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
[8] https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure
[9] https://www.dhs.gov/using-cybersecurity-framework

In fact, the "targeted attack" nature of cyber risk has discouraged insurers from exposing details of the exact coverage in their cyber insurance policies. This is akin to "silent cyber" where the covered events are not explicitly defined. On the other hand, a more explicit cyber insurance pricing model (depicted in the diagram below) characterized by well-defined security metrics can potentially provide the necessary incentive to the insured to improve their cyber security posture as a sustainable response to worsening cyber threats. The premise of such a model recognizes that there is a fundamental disconnect between the insured and the insurer for the risk being covered.

The draft ISO Standard 27102[10] is designed to close this knowledge gap. The diagram below depicts a simplified implementation of this concept. The goal is to empower the insured and their IT teams with increased awareness of and readiness for preventive cyber security practices. Such guidance can be developed and published for free under the ISO 27102 framework. The insureds who take advantage of such tools can be rewarded with a reduction in claims excess. Similarly, those insureds who refuse to take advantage of such tools or who do not implement such advice can be penalized through an increase in claims excess.



This design of the model "Pro-active cyber insurance pricing" does not impose an upfront cost on the insurer or insured but rather provides an incentive to the insured to investigate and implement pro-active measures to improve their cyber security posture. The selection of dynamic adjustment of claims excess level in the diagram above is designed to illustrate the concept with a simple example. More sophisticated incentives and enforcement scheme can be conceived with more effectiveness in targeting specific cyber risk behaviors while minimizing enforcement cost.

[10] https://www.iso.org/standard/72436.html

Petra Wildemann mentioned in her article on pricing mechanism that the insurance market recognizes the need to find a solution to the challenge posed by cyber-risk. And yet, with this emerging sector relying largely on highly hypothetical scenarios, the key question remains: Can cyber-risk be measured with sufficient reliability to enable companies to effectively and reliably insure it? The answer to this is still not clear.

About the Authors

Denny Wan *is the principal consultant of Security Express (https://www.securityexpress.com.au/), a Sydney Australia based cyber security consulting practice. His specialisation includes security policy development, IT security audit, GRC risk management, virtualisation and hybrid cloud security architecture. He is the chair of the Open Group FAIR Sydney Chapter (https://link.fairinstitute.org/group/19-sydney-chapter) and currently undertaking postgraduate research into Cyber Insurance Pricing Strategy at Macquarie University (https://www.mq.edu.au/) under an Australian Government Commonwealth Scholarship.*

Petra Wildemann *is the Chair and Founder of the Swiss Cyber Think Tank (https://www.risk-cyber-insurance.com), a business network for Cyber Risk & Insurability, providing an industry-wide networking platform for insurers, technology and security firms. As a qualified actuary for Life Insurance and Property & Casualty Insurance in Switzerland (SAV), Germany (DAV) and UK (IFoA Affiliate), her specialisation includes risk management on a variety of local and global risks. Of late, she has expanded her focus to also include the challenges of modeling the risks in the age of cyber risk (https://www.linkedin.com/pulse/cyber-risk-insurance-challenges-modelling-risks-data-age-wildemann/) and the mismatch between measurement and pricing of cyber-risk insurance policies (http://images.info.fticonsulting.com/Web/FTIConsultingInc/%7B36264fa2-8735-4956-9a87-f69201c1253a%7D_FTI_Consulting_Article_Pricing_Cyber-Risk.pdf).*