Cyber Insurance Incentive Model

By Denny Wan and Petra Wildemann

This whitepaper extends the concept of Pro-active Cyber Insurance Pricing Model[1] leveraging cyber risk control metrics in order to encourage insureds to improve their cyber security posture. In the previous white paper "Pro-active cyber insurance pricing model" (by the same authors), a simple set of cyber risk control metrics, based on readiness indicators such as availability of current data inventory and effective execution of incident response plan, was translated into dynamic adjustment of the claim excess amount as an incentive for insureds.

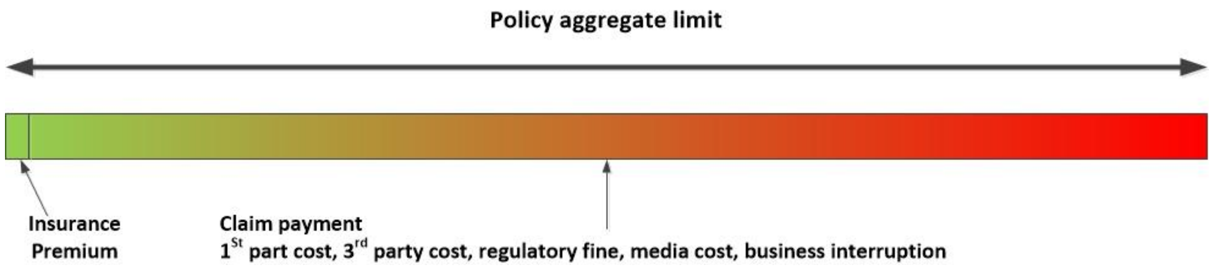
> This "Pro-active cyber insurance pricing" model does not impose any upfront costs on the insurer or insured, but rather provides an incentive to the insured to investigate and implement pro-active measures to improve their cyber security posture. Given the absence of upfront costs and the paucity of historical claim data, it becomes clear that a robust incentive model is essential.

The design is based on "no cost" or "low cost" incentives. At first glance, reduction in claim excess would result in increased costs to the insurer. On the other hand, as asserted in our model, reduction in the claim excess amount is likely to be offset by material reduction in the total claim amount. The reduction is expected to be attributed to containment of business impact from the cyberattacks and minimisation in recovery effort. But in the larger scheme of things, the proposed incentive from potential reduction in claim excess might not be sufficient to incentivise the insureds to materially change their behaviour. This whitepaper explores the underpinning incentive model for cyber insurance policy and its potential to elevate and amplify the incentive effort.

The Insurance Incentive model

Insurance is a risk transfer model whereby the insurers promise to compensate the insureds financially when the insured risk events materialise. The insurers maintain their right to adjust the payable claim amount based on their assessment of the actual financial damages suffered by the insureds attributable to the insured risk events. The maximum payable claim amount is known as the "policy aggregate limit" in the policy. From the insureds' perspective, the aggregate limit is a continuum in funding available to mitigate their financial risk exposure to the insured risk events.

The continuum is depicted in the diagram below:


Policy aggregate limit
Insurance Premium
Claim payment
1st part cost, 3rd party cost, regulatory fine, media cost, business interruption

[1] https://www.cyber-risk-insurance.com/Publications
https://www.securityexpress.com.au/research-into-cyber-insurance/

The default risk mitigation option is “self-insured”. When the insurance premium is comparable to the aggregate limit, such an approach could be financially attractive e.g. why bother with insurance?

The table below compares the ratio between the aggregate limit and policy premium for sample automotive and cyber insurance covers based on sample online quotes from local Australian insurers.

Example of Aggregate Limits versus Policy premium for Automotive and Cyber, showing the ratio for a cyber attack of 0.2% in case of a cyber claim versus 12% in case of an automotive claim. This is exactly why there are a lot of uninsured or under-insured vehicles on the road particularly for older vehicles. On the other hand, the demand for cyber insurance is sky rocketing because it is prudent to acquire such protection for the business for a relatively small outlay in premium. The decision is almost trivial after experiencing or witnessing the devastating impact from ransomware or phishing email attacks.

Policy type	Aggregate limit	Policy premium	Cover/premium
Automotive	$29,000	$3,500	12%
Cyber	$1,000,000	$1,900	0.2%

Current cyber insurance pricing does seem quite low. This might suggest that insurers believe cyber-attack is extremely unlikely compared to automotive accidents. However, it is probably more likely that the price is being kept artificially low to attract more business. Insureds who elect to take out a policy cover are likely to value the financial protection represented by the aggregate limit.

Our previous whitepaper (“Pro-active cyber insurance pricing model”) asserted that cyber insurance might, in fact, encourage cyber criminals to monetise cybercrime. This can result in a vicious circle of accelerated cyberattack incentivised by insurance payout placing unsustainable financial pressure on insurers.

The recent case of significant reduction in the final claim payout to the National Bank of Blacksburg[2] in Virginia USA is a timely reminder of such hypothesis. The loss was attributed to two separate attacks in 2016 and 2017 resulting in a total loss of US$2.4M.

Outlook to an attack at the “National Bank” (USA)

The attack against the National Bank in Virginia, USA was sophisticated and highly targeted. It is understood that the bank implemented additional security controls after the initial attack in 2016, but they were insufficient to prevent the second attack.

The feature of this cyber incident which drew such public attention was not the size of the loss suffered or the sophistication of the attack, but rather the fact that the final claim payout was a mere US$50,000, notwithstanding the aggregate policy limit of US$8M. The insurer asserted their right to adjust the loss based on exclusion clauses and partially overlapping insured event definitions in the policy. Naturally the bank was not satisfied with the position and took action against the insurer for breach of contract. Unfortunately for the bank, the court upheld the insurer’s position.

[2] https://slate.com/technology/2018/07/cyberinsurance-company-refuses-to-pay-out-full-amount-to-bank-after-hacking.html

It is not the focus of this whitepaper to analyse the claims, counter-claims, technicality or fairness in the loss adjustment process. The following observations were drawn from the analysis:

1. The National Bank of Blacksburg chose a policy aggregate limit of $8M. This sum would have been more than sufficient to cover their losses validating their internal risk assessment process.
2. The National Bank of Blacksburg clearly understood and correctly set the business value of their cyber insurance policy. It would be reasonable to expect their full co-operation with the insurer to improve their cyber security exposure. In fact, they implemented additional security controls after the initial attack in 2016 before receiving any claim payout to fund the investment and associated remediation activities.
3. The unilateral assertion of the contractual right by the insurer could result in a distortion of the credibility and value of cyber insurance policy even for sophisticated and pro-active customers like the National Bank of Blacksburg.

One of the premises in our previous whitepaper is the potential collapse of the cyber insurance industry projected from the above observations if nothing is done to change the current culture and practice in cyber insurance pricing strategies. It is in the interest of the insurer and insureds to work collaboratively to manage the cyber risk exposure to the community. A structured approach to risk transfer within the broader economy is a healthy and necessary economic process. Dumping of risk is not.

Moreover, in this case, given that the bank did attempt to react appropriately to the first attack, it must be admitted that even a more Pro-active Cyber Insurance Policy approach based on specific cyber risk control metrics might not have worked in this case. However, for most small and medium businesses with less sophisticated operations or high value information asset, willingness on the part of the insureds to protect their aggregate limit can be highly effective and offers great leverage to the insurers to manage the cyber security posture of the insureds. This appeal to the self-interest of the insureds is a far more powerful form of incentive than the offer of slightly cheaper premiums. The confidence in a fair and equitable loss adjustment process based on agreed and measurable cyber risk control metrics would be very attractive to insureds.

There appear to be other examples, such as the case where the Indian Bank was hit by $13.5 Cyber attack after the FBI had sent warning about imminent ATM cash out schemes set to unfold across the globe.[3]

The attack actually materialised. But what is most interesting is the comment from Matthew Heiman in this recent cyber law podcast[4] which alerted to the possibility of insurers splitting the cyber insurance market by jacking up prices for a social engineering attack.

If this market split were to materialise, it would present a very good opportunity for our proposed Pro-active Cyber Insurance Model, because the insurers would earn higher premiums at the risk of higher exposure to a much more concentrated insureds demographics with similar risk profiles (banks, financial institutions, etc). So, they do need a different approach to manage such risks. The opportunities are not in insuring banks which already have large resources, such as the National Bank or this Indian Bank. The opportunities are in the small-to-medium business markets, such as

[3] https://krebsonsecurity.com/2018/08/indian-bank-hit-in-13-5m-cyberheist-after-fbi-atm-cashout-warning/

[4] https://www.steptoecyberblog.com/2018/07/30/episode-228-best-idea-yet-for-derailing-the-kavanaugh-nomination/

small loan brokers and lawyers. They will need pro-Active cyber insurance to help manage their cyber risks.

Our assertion is that by lifting the cyber security readiness of the business community in general, the total loss exposure of the economy to cybercrime will be greatly reduced. We might draw an analogy to the simple health message of washing your hands. While this measure does not cure any infectious disease, it is very effective in combating the spread of infectious disease across the community and saves lives.

In this discussion of the pro-active cyber insurance pricing model, we have compared the risk models for cyber to automotive insurance. Comparing Cyber incentive models to more complicated business lines will require a great deal of careful analysis.

Historical claim-data-driven risk models are not suitable for forecasting future risks, and measurement and modelling approaches that have been developed for other risks (such as natural catastrophes) cannot easily be transferred to cyber risk. Our approach is genuinely unique and has material value, and we are in the process of clarifying a solid path for execution, e.g. by identifying sources of incentives.

About the Authors

Denny Wan and Petra Wildemann are co-authors of the White Paper “Pro-active cyber insurance pricing model” from 29 July 2018, which has been published on Social Media, Cyber-risk-insurance and *Security Express.*

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 modelling 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).*

Links to the White Paper: “Pro-active cyber insurance pricing model”

https://www.cyber-risk-insurance.com/Publications

https://www.securityexpress.com.au/research-into-cyber-insurance/