Debate on managing risk in cyber insurance 11th Jan 2019

I am Petra Wildemann (PW), the Chair and Founder of the Swiss Cyber Think Tank and an expert on Risk with over 25 years of experience in the Actuarial world.

My guests today are:

Denny Wan (DW) and Steve Wilson (SW)

Denny is a cybersecurity expert with over 20 years experience and a researcher into cyber insurance pricing models. He is the chair of the Australian Cyber Insurance Think Tank and the Open Group FAIR Sydney Chapter.

Steve is a general insurance veteran with experience spanning many product lines, markets and disciplines. He recently co-authored a paper on the management of cyber accumulation risk – a key concern for the development of this market.

PW> Your paper "Advancing Accumulation Risk Management in Cyber Insurance - Prerequisites for the development of a sustainable cyber risk insurance market"[1] tabled some concrete and positive steps being taken by the cyber insurance market to manage accumulation risk. But clearly, this is a material concern to the industry and could potentially present an existential threat to the industry if not handled properly. Am I reading too much into your analysis? Could you please elaborate on this point to set the scene for this debate?

SW> There is indeed a view that a major event perhaps from a widespread virus or other wide-ranging attack could be a very significant issue – not just for the cyber insurance market but such an event could have very significant economic ramifications or could even cause major physical damage and loss of life. So, we cannot dismiss the potential of an extreme event but I think the insurance markets are doing a good job in managing the accumulation risk today whilst learning to understand it better so the market can continue to expand.

For example, the specialist model providers are increasingly using advanced techniques to understand the quantum of a major event. Furthermore, the risk carriers – insurers and reinsurers - are undoubtedly taking care to manage their exposures. It's worth saying that the major players in the cyber insurance market are the top international insurers who are well recognised for underwriting discipline. As long as the market overall remains disciplined in it's underwriting, I would be confident that it continues to develop.

DW> Steve. Thanks for the clarification. It certainly makes it much clearer for me. My research with Petra also focuses on countering the global and man-made nature of cyber-attacks amplified by interconnectivity between systems. Our research paper titled "Pro-active cyber insurance pricing model"[2] contrasted cyber insurance with auto/property/health insurance from this perspective. It seems to me that your analysis went further. Can you summarise your insight for the benefit of our readers?

SW> Yes, our study found that there is a number of characteristics that make cyber risk unique amongst risk types. The levels of interconnectivity in particular make understanding the risk

[1] https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf
[2] https://www.securityexpress.com.au/wp-content/uploads/2018/08/Pro-active-cyber-insurance-pricing-model.pdf

especially difficult. Whereas conventional risks – such as property, auto and even liability – are easily conceptualised, with cyber it is difficult to even define the underlying exposure. Assets exposed are diverse: microchips, software packages, processing systems, databases etc; the threats to these assets are wide and constantly evolving; and the potential damages that could arise to these assets are equally diverse and difficult to quantify. Add to that the ever-increasing links between systems and the indirect linkages arising from the often widespread dispersion of common software, and it becomes clear that new approaches to understanding exposures and measuring exposures are needed.

By way of example, look at the cloud. There is a rapid increase in businesses – and individuals - outsourcing to the cloud, so there is potential for risk concentrating around Cloud Service Providers' operations. Equally, many industries use common software packages and some software, such as for accounting, runs across industries, so these create wide-spread exposure to malware attacks. That said, insurers have a lot of experience with other risks where there is the potential for contagion and/or interconnectivity. The so-called Financial Lines – that is Directors' and Officers' liability and other professional liability classes – are a case in point. These classes were exposed to multiple linked events in the financial crisis of 2008, so there are historical references from which insurers can, and are, learning.

PW> Your comparison between D&O and cyber insurance modelling is an interesting angle. Isn't it more like property with the potential for a major catastrophe?

SW> Well, cyber risk has characteristics like both. The potential for a cyber cat[astrophe] has been described in several papers, with scenarios including a major attack on a city infrastructure, a cloud service operation failing and a widespread malware attack. So, in some respects, you can draw parallels with nat cats such as windstorms, floods and wildfires as well as man-made cats such as explosions or terrorist bombings.

But also, cyber underwriters are leveraging expertise from the liability and speciality lines areas. This is encouraging since these underwriters are very skilled in managing their risk acceptance – and so cyber risk exposure can be managed using deductibles, waiting periods and policy limits. This is good for the industry and bodes well for the sustainability of the cyber insurance market, but there are some views that it contributes to the protection gap and that this gap needs to reduce over time.

DW> Steve. You raised a very interesting and potentially controversial point around the use of deductibles, waiting periods and policy limits by insurers to manage their risk acceptance. In my research with Petra, we noted a trend of insurers rejecting claims resulting in current court cases. We explored some of these cases in our research paper "Cyber Insurance Incentive model"[3]. Some of these disputes are attributed to the interpretation of exclusion clauses in the insurance policy. What are your thoughts?

SW> I wouldn't consider the way cyber insurance policies are structured or worded to be controversial – the terms and conditions are just like those in other classes and so I don't think there's anything unusual. I would also observe that the risk is evolving so you'd expect terms and conditions likewise to evolve. Overtime insurers will increase the levels of coverage as the risk becomes better understood and can be better quantified and priced. Also, as data and models become more credible, insurers will be able to transfer more aggregate risk to either reinsurers or other providers of risk transfer – such as Insurance Linked Securities or Industry Loss Warranties. This will all help the cyber insurance market to continue to grow – and, by the way, it is already growing rapidly.

[3] https://www.securityexpress.com.au/wp-content/uploads/2018/10/Cyber-Insurance-Incentive-model.pdf

However, there's a danger of placing too much focus on the dynamics of the insurance market as this may miss the point that insurance is not the whole answer. Really, what's needed is to manage the risk at its origin. This is the case with all types of risk – whether its homeowners locking their doors and windows or major corporations employing advanced risk management teams. Cyber risk is no different, and so risk management and mitigation needs to be developed and this too requires a better understanding.

PW> We completely agree. Insurance should only be part of the answer. It is a necessary enabler for the growth of the data-driven economy. We also believe that it is essential for insurers to work with policyholders "pro-actively" to manage their cyber risks. This is akin to encouraging homeowners to lock their doors and windows – basic and cost-effective measures that only take a bit of effort from the homeowners to apply their protection. The challenge with cyber risk management is that it is not as intuitive as door or windows locks. The prevailing approach is for insurers to subsidise cyber risk management services for the policyholders.

This trend was discussed in a research paper published by the Geneva Association titled "Cyber Insurance as a Risk Mitigation Strategy"[4]. While this is a useful service for large enterprise where the insurance premium is sufficient to support such subsidy, it is not a commercially viable approach for small and medium business where the premium is much lower. The Pro-active model "dynamic excess" discussed in our research paper solved this scalability and sustainability challenge because there is no upfront cost to the insurer with a high likelihood of a net reduction to their claim exposure. Do you have views on this topic?

SW> Again, I think we can draw some parallels with other lines. It is always the case that managing the risk at its point of origin is the first step with insurance as a subsequent transfer mechanism. For larger commercial entities, the size and complexity of risks can make it economically viable to invest in risk management services or even to have in-house risk departments, but this is mostly not the case for SMEs. Additionally, for "traditional" risk classes the risk management is more intuitive and so the business owner or manager often has a good knowledge of what he/she needs to do. But for cyber, the underlying risks are less familiar and so this makes it more difficult for the business owner to implement adequate mitigation processes.

DW> Steve. That is an excellent and insightful summary. We are extending our research in the Pro-active model by integrating telematics to inform the policy dynamically. It has some similarity to parametric insurance where policies can be paid when pre-defined parameters such as rainfall levels have reached the agreed threshold. In our model, these parameters are security metrics such as backup quality. One particular use case we have modelled is to monitor the RPO (Recovery Point Objective) to limit the claim exposure attributed to Business Interruption. Many of our readers might not be familiar with RPO. Simply put, a ransomware policy might be priced on the protection of backup limited to four hours of business interruption. When our system detected the quality of backup has deteriorated, the policy will limit the claim exposure to four hours if the policyholder failed to rectify the backup quality issue after an agreed period (such as 24 hours) upon warning by the insurer. Do you think this is a practical approach to improving the resilience of the policyholder?

SW> This sounds very promising and shows how technological tools can be used to manage technology risks in ways. I think we will see more of technological innovations for risk management so your ideas is part of a wider trend. In fact, your model is in line with my view that it is of primary importance to facilitate cyber resilience at the source of risk. I also like the dynamic nature and I

[4] https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf

think leveraging “real time” information will become a growing trend in many classes of insurance. However, we need to recognise that SMEs generally do not have the inhouse risk management capabilities. So is it a realistic expectation for businesses (even larger firms, not just SMEs) to understand RPO (using your example) and be in a position to respond to notification of deterioration in the way you have described?

DW> Thanks for the question and challenge. This is indeed a significant commercial and technical challenge today. Technical terms such as RPO, while well understood by IT professionals and backup solution providers, is not necessarily a suitable business language to use used in a cyber insurance policy. In our approach, we convert these measurements into “security metrics” to enable simpler decision making processes. A parallel trend is in the rise in Usage Based Insurance[5] (UBI) products for cars. UBI is based on data collected by the black boxes installed into vehicles. Insurers do not disclose exactly what telemetry data is being collected nor do the policyholders care too much about it. Policyholders just expect “good drivers to be rewarded with lower premiums”.

The value of the UBI program is in offering insurers the means to identify risky driving behaviours. Armed with such information, insurers can manage driver behaviour through deductibles, waiting periods and policy limits, some of the tools you mentioned before. In a fleet situation, the fleet program can be used to effect driver behaviour management as a reverse risk transfer program back to the policyholders. This is an effective way to improve “resilience at the source of risk”.

In a similar way, these “security metrics” are designed to empower insurers to manage IT security management practices with policyholders without getting bogged down by technical details. By monitoring and alerting on breaches of the RPO metric, policyholders will be empowered to take remediation action without the need to understand the technical details of RPO.

Under this approach, insurers will issue technical instructions to the policyholders on how to send RPO telemetry data from their backup infrastructure and what remediation actions to take when notified of a breach of RPO metric. This is akin to the practice of mobile phone operators sending SMS based configuration instructions to automatically configure their mobile phone when subscribers join their network. The subscribers do not need to understand how to configure a particular mobile phone. They just need to accept the SMS instructions.

SW> Denny, that clarification is extremely helpful. Motor insurance black boxes had come to mind, but your wider point about how the customer needn’t know all the technical details so long as it is clear what they need to manage is key. In other areas, such as the apps on smartphones and tablets, the user interface is really simple – technology is not restricted by jargon and technicalities any more. If the cyber insurance providers embrace this type of thinking then they will be able to open up the market further.

PW> Steve. Your paper expressed confidence and noted advancement in accumulation risk modelling. Can you share some specific examples or references to these modelling efforts for the benefit of our listeners?

SW> We should start by recognising the need for a strong foundation to the any modelling efforts- and that means having well-defined data and, from there, build models and scenarios. For example, Cambridge Centre for Risk Studies and Risk Management Solutions (RMI) published a paper titled

[5] https://www.insurancebusinessmag.com/au/features/opinion/ubi-and-telematics-79774.aspx

"MANAGING CYBER INSURANCE ACCUMULATION RISK"[6] which explored the accumulation risk of five specific scenarios. The paper made reference to the risk codes published by Lloyds of London (2015)[7] and the Cyber Insurance Exposure Data Schema.[8] Such effort to standardise insurance codes offer a solid foundation to advance such research. I think we will see the language of cyber risk develop further to help define and measure the exposures given the unique characteristics of cyber. For example, the term "confinement zone" has been used to describe the fact the impact of certain cyber events may be bounded - although the "boundary" might be difficult to define, let alone measure with accuracy.

DW> Steve. These are definitely solid steps. We discussed earlier about the man-made nature of cyber risk. But some of these risks are the result of un-intentional actions such as coding errors, e.g. non-targeted attacks. What are your views on this?

SW> I think it's important to differentiate between the type of attack – and also the type of perpetrator. Particularly for the major adverse scenarios it is most likely that there will be a sophisticated perpetrator. That said, I'm not sure if "targeted" and "non-targeted" are the right terms. The nature of an attack is related to the motive. If it is perpetrated by organised crime there will be a financial motive and so it will be very targeted. However, a nation state or terrorist organisation might look to create more random disruption. A malware that is designed to evolve like a mutating virus could spread widely and so impact multiple different software systems. This would be very disruptive but not targeted. When you consider today the speed of machine learning this is daunting threat.

DW> Steve. Thanks for the fascinating discussions and your insights. I think we are drawing to the close of our debate. Perhaps the last area I want to seek your opinion is on the role of cyber insurance in supply chain risk management. A key difference, as I see it, is that the beneficiaries of the cyber insurance policy in a supply chain context such as Open Banking are generally not the policyholders. Such model shares some similarity with mandatory Third-Party Automotive insurance as part of the vehicle registration requirements in some countries. Dimensioning of the insurance requirements is often mandated by the authorities.
I believe the governments have similar fiduciary duties to specify cyber insurance requirements in the supply chain context.
An added complexity is that some of this information might be specifically protected by data privacy legislation such as the EU GDPR (General Data Protection Regulations) and subjected to heavy fines. This is particularly problematic for intermediaries such as information brokers or mortgage franchisees who have limited control on the collation, dissimilation and consumption of the information. But they are exposed to the full force of these regulatory frameworks. Dimensioning of cyber insurance for such use cases requires a new risk language. This is the focus of my current post graduate research in Macquarie University in Australia.

What is your experience in conceptualising cyber insurance requirements in this context?

SW> I think the primary issue here is that the data driven economy has a structure that is very new and so unfamiliar and not transparent to most people. Using again the example of the cloud, many users will not know how and where their data is stored or transported. Further, many services are

[6] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf
[7] https://www.lloyds.com/~/media/files/the-market/operating-at-lloyds/resources/risk-codes/2015/risk-code-guidance-notes-apr-2015.pdf
[8] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-data-schema-v1.0.pdf

now coming directly from the cloud and so it's not just data but wider technological capabilities that migrate from a local device, such as a PC or “mainframe “, into the cloud. This transfer of both data and process not only creates new risks, as we discussed earlier, but also the whole framework is different in terms of ownership, responsibility, regulation and so on.

PW> This has been an excellent discussion, but time is indeed upon us. However there is one last point, if I may ask, which I would like to get some comments from both of you. It is clear from our discussion that the professional’s task to tackle these challenges will require broad skill sets spanning both technical and business areas. I am fortunate to have the opportunity in meeting many very talented candidates through my role in Dorigo AG. And equally I am fascinated by my clients’ vision of their ideal candidate profile for these very challenging roles particularly, in this rapidly innovating part of the insurance. What career advice do you have for candidates interested in these roles?

DW> Petra, I envy your opportunity to speak with so many interesting and talented candidates. I am probably not the kind of people to give career advice. My background is in infrastructure security – firewall, network penetration testing, server hardening, security policy development, IT audit etc. It was a deep learning curve to understand the structure and culture of the insurance industry. Insurance is fundamentally a risk transfer process rather a technology challenge. It is largely based on people’s perception of risk and their risk appetite. Self insurance is an easy way out when the perception of risk is hard to define. As Steve explained, maintaining strong underwriting discipline is a foundation to limiting accumulation risk.

Moreover, it helps to some basic knowledge in psychology when developing pricing strategy for any services or products. It is about creating value proposing. A key concept is Anchoring[9]. As Steve noted in his paper “…Cyber accumulation modellers .. must deal with the idiosyncratic features of measuring exposures for cyber risk and assessing claims that may arise from these exposures …”. If I can paraphrase (Steve please correct me if I am wrong), candidates should be prepared to think outside the box and not to confine themselves only to certainties in technology.

SW> Petra, you make a very astute point that professionals and executives now need to be knowledgeable about many technical aspects of their work. I was just recently talking to a lawyer who was telling me about the transformational impact of technology in terms of its power to extract and analysing data embedded in documents. This will have enormous implications for the skills needed and for the staff structures of law practices. So, I would advocate up and coming professionals ensure that they keep abreast of these technological changes and be willing to adopt new and, in some cases, radically different working practices.

PW> This has been an excellent discussion outlining how important it is that the insurance markets manage the accumulation risk and learning to understand it better so the market can continue to expand. We have discussed the role of cyber insurance in supply chain risk management and learned that the beneficiaries of the cyber insurance policy in a supply chain context are generally not the policyholders. In the paper, which we have published on Pricing and Incentive model, we compared the cyber risks to the Third-Party Automotive insurance, showing the need for registration requirements. We are certain that cyber risks will take the same path.

I would like to refer to Steve’s paper on recommendation to improve “cyber resilience at source” which is consistent with Denny’s and my Pro-active Cyber Insurance approach.

[9] https://en.wikipedia.org/wiki/Anchoring

Denny and Steve, I thank you both for the fruitful discussion. The debate on managing accumulation risk in cyber insurance has been a pleasure.

I also would like to invite the audience for comments and feedback through the publication channels such as our blogs and websites.

Baseline research:

The Geneva Association (GA) released a research paper titled "Advancing Accumulation Risk Management in Cyber Insurance - Prerequisites for the development of a sustainable cyber risk insurance market". GA is a global think tank for the insurance industry with membership drawn from the CEO of the top 90 insurers and reinsurers.

Accumulation Risk represents the risk of large aggregate losses from a single event or peril due to the concentration of insured risk exposed to that single event or peril

Four key challenges:

i. A single large event or a series of consecutive events may make affirmative cyber insurance unprofitable;
ii. Insurers and reinsurers (for which risk accumulation may be more pronounced than for primary insurers) could underestimate non-affirmative cyber exposure leading to an unplanned shock from a major event;
iii. Data are of insufficient quality, are incomplete and/or lack the necessary consistency for more advanced modelling techniques; and
iv. Governments fail to provide commensurate frameworks for the sharing of large-scale terrorism-induced losses.

Three prerequisites for sustainability:

i. insurers must facilitate cyber resilience at the source of risk
ii. insurers need to make an acceptable return on capital
iii. the insurance industry needs to be able to withstand major shocks.

Proposed solution

i. insurers strengthen their core underwriting capabilities,
ii. insurers played an active role in helping companies build resilience
iii. underwriters implement proactive approaches, drawing on a range of internal and external inputs
iv. underwriters develop 'confinement zones' to capture complex and constantly evolving systems and networks in the corporate world
v. Develop innovative attempts to bypass data limitations due to data paucity
vi. Develop advanced techniques (e.g. machine learning, Bayesian hierarchical modelling) to allow for better measurement and understanding of new technological risks
vii. Develop granular assessments of cloud-related interconnectivity
viii. Develop stochastic scenario assessments for challenges related to malware and excessive reliance on one particular hardware or software (the 'monoculture' dependency)

Other related research:

MANAGING CYBER INSURANCE ACCUMULATION RISK
Cyber Insurance Exposure Data Schema V1.0
Policy measures and cyber insurance: a framework
Casualty Accumulation Risk
Cyber Insurance as a Risk Mitigation Strategy
Content Analysis of Cyber Insurance Policies

These represents main attempts for better classification of cyber incidents and claim handling. There is no specific model advocated to break down or contain accumulation risk.