Joint Research Initiative on Cyber Risk

The challenges of Cyber Insurance

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

The research initiative “Cyber risk: actuarial modeling” has been supported by Fondation du Risque (Institut Louis Bachelier) since 2017, and AXA Research Fund and AXA Risk Management Group since 2018. The aim of this project is to gather expertise to provide statistical methodologies that allow to better understand the economic impact of cyber risk, and contribute to the development of the cyber insurance sector. The research topics cover actuarial pricing models adapted to cyber, stochastic scenarios generation, systemic risk (or accumulation risk). With this closing conference, the project enters a new phase, making the link between cyber and other emerging risks for which insurability is at stake (climate risk, pandemic, supply chain interruption…).

SUMMARY

CAROLINE HILLAIRET

Professor at ENSAE Paris, co-director of
the Joint research Initiative “Cyber risk: actuarial modeling”

The emerging and evolving nature of cyber risk and its systemic component make it one of the most important social and economic risks.

In a few years, cyber-risk has become one of the main threats weighing on companies and cyber-attacks constitute today the main threat to the global financial system, with an estimated cost of 1% of global GDP, that is approximately one trillion of dollars. In the face of this major risk, insurance has a crucial role to play to help for the resilience of the economy. It also constitutes an element of cyber-defense since physical cyber-security, that is essential for limiting and preventing attacks, cannot succeed in constituting an impenetrable barrier against these digital attacks. The ongoing development of the cyber-insurance market, with innovative offers that combine prevention, financial compensation, and support in the event of a crisis, is facing a certain number of difficulties. The Joint Research Initiative “Cyber risk: Actuarial Modeling” (between AXA GRM - ENSAE Paris - Sorbonne University) has led constructive contributions regarding the quantification of this risk, which requires in-depth mathematical and actuarial analysis.

Since the majority of information systems are interconnected, a cyber attack can lead to contagion and massive failures that can shut down an economy, or at least endanger the solvency of an insurer. Therefore, modeling the frequency of cyberattacks requires reflecting complex dependency effects. The standard Poisson model, based on the assumption of independence between the arrivals of claims, appears to be unable to take into account the effects of clustering as well as the auto-correlation between cyber-events. In [BBH21] and [HRR21], we propose an alternative model based on

Hawkes processes which have the ability to capture the self-excitation and interactions of cyber-events according to their characteristics, while benefiting from a interpretable and parsimonious parametric representation.

We have also developed a general and flexible methodology for generating stochastic scenarios of cyber-incident accumulation, using epidemiological models and integrating network effects ([HL21], [HLOS22]). Indeed, a massive attack, like the one of the Wannacry ransomware in 2017 which led to the contagion of more than 300,000 computers in more than 150 countries, can undermine the principle of mutualisation, which is at the heart of the insurance business.

Furthermore, if a large number of policyholders are simultaneously victims of an attack, the insurer's response capacity may become saturated. Indeed, in addition to financial compensation, cyber policies generally provide assistance during the crisis, by teams of experts (such as cyber security firms) to help the insured party recover. This inability of the insurer to intervene appropriately within a short time induces additional losses (financial penalties, damages to reputation, but also increased damage for the policyholder). Our studies can help insurance companies design their strategies against such cyber-pandemics in order to size their response capacity, anticipate responses and their impacts in reducing cyber threat.

References

[BBH21] Y. Bessy-Roland, A. Boumezoued, C. Hillairet. *Multivariate Hawkes process for cyber insurance*, Annals of Actuarial Science, Volume 15, Issue 1, March 2021.

[HL21] C. Hillairet, O. Lopez *Propagation of cyber incidents in an insurance portfolio : counting processes combined with compartmental epidemiological models*, Scandinavian Actuarial Journal, 2021(8), 671-694.

[HRR21] C. Hillairet, A. Réveillac, M. Rosenbaum. *An expansion formula for Hawkes processes and application to cyber-insurance derivatives* (soumis 2021)

[HLOS22] C. Hillairet, O. Lopez, L. D'Oultremont, B. Spoorenberg *Cyber contagion: impact of the network structure on the losses of an insurance portfolio*. (To appear in Insurance: Mathematics and Economics, 2022)

XAVIER SERVEL

Head of Actuarial & Cat Man-made
at AXA GRM P&C

The development of Cyber insurance is an important strategic decision for insurers. AXA has supported its development of Cyber products with a strong Risk Management framework, and has invested time and resources into the elaboration of methodologies to assess Cyber risk. The Joint Research Initiative with ENSAE and Sorbonne Université was one of the components of this success.

Cyber risk has been a hot insurance topic in Europe in recent years. Being a significant concern for individuals and companies[1], the Cyber insurance line has grown tremendously in a few years and is expected to continue to do so[2]. Conversely, Cyber Risk troubles insurers and reinsurers alike as, to date, no one can say whether the portfolio could sustain an extreme accumulation event without going under[3].

It is well-known by Actuaries that when Natural Catastrophes occur affecting a high number of insured in one fell swoop, one of the core principles of insurance is undermined: the mutualization of risks. For decades, risk managers have thus geographically diversified their portfolio to restore mutualization at a higher level – a portfolio concentrated in one locality might be wiped out, but it could be compensated by the absence of events in other places.

The major worry on Cyber accumulation losses has to do with the fact that a single event (e.g. a malware attack like WannaCry or NotPetya) is not limited to geographical proximities as it is for a Natural Catastrophe. As it spreads in the digital world, a

Cyber event can easily reach another country or another continent. In this context, how can geographical diversification apply in the Cyber environment? Is the mutualization of risk still achievable or are insurers and reinsurers exposed to events that by nature defy mutualization? And in this case, is Cyber risk still insurable? Those are the questions that keep Cyber risk managers awake at night.

Fulfilling its role as of one of the leaders of the insurance market, AXA has been building its Cyber offer for clients for close to a decade. Structuring this product has meant putting in place a strong risk management framework to scrupulously monitor both the nature of the covers granted to the insured and their financial conditions, to capture at inception the emerging claims trends, and to regularly assess the cost of an extreme event that could spread in the portfolio beyond geographical borders. To this end, AXA has instituted several practices. First among them is frequent exchanges with brokers, consultancy firms, reinsurers, and peers as well as cyber modellers, who have either built their insurance expertise by selling solutions for Natural Catastrophe risk or have emerged from more IT-company backgrounds. This ensures AXA gets and shares knowledge with the market, and that AXA and its peers overlook no significant aspect of Cyber risk in their journey. Secondly, AXA has built a Cyber module for its Solvency II Internal model that has been validated by ACPR. This module brings together the expertise of all the Group's Cyber actors, be they from the Underwriting, Pricing, Claims Handling, Cybersecurity, Information Risk, and Risk management professional families and it is regularly challenged and updated to keep up with the evolving underlying risk. The module analyzes two scenarios: an attack on a major Cloud breaching extensive data and a massive ransomware attack damaging the Affirmative Cyber portfolios. In the past year, a strong focus has also been put on creating or adjusting scenarios for Silent Cyber. This Cyber risk is "silent" as it is embedded in the policies of traditional lines due to the absence of exclusion. A major project has thus been undertaken in parallel to transform Silent covers into Affirmative ones. Thirdly, AXA has financed a Joint Research Initiative (JRI) with two renowned Actuarial universities: ENSAE and Sorbonne Université. The JRI has been entrusted with researching and publishing academic articles on various aspects of Cyber risk, notably the risk of frequency (attritional claims), the risk of severity (large claims), and the risk of accumulation (catastrophe claims). Through this initiative, AXA's long-term goal is to support the elaboration of a Cyber risk Actuarial corpus. AXA is therefore particularly proud to host this event celebrating the achievements of these 4 years of collaborative work on Cyber risk.

Notes

[1] *The Global Risk Report 2022* of the World Economic Forum mentioned that "Cybersecurity failure was identified […] as a critical short-term threat to the world", *AXA Future Risk Reports 2021* also concluded that it was the second-most worrying emerging risk, after climate change and before infectious disease, and scoring first for the Americas.

[2] according to the *CyRiM Report 2019*, which partners with several brokers and (re)insurers: "The expansion of the cyber insurance market is both necessary and inevitable […]. Although the majority of affirmative cyber insurance premium still comes from the US, there are now significant premiums being generated in another 30 countries, and the market is expected to be truly global in a few years."

[3] *in CyRiM Report 2019*, it is stated that "These catastrophe events form the tail risk for insurance lines, and many experienced insurance professions are concerned that the true catastrophe potential of cyber risk has not yet become apparent. Some commentators have suggested that this hidden potential for large future losses may make cyber uninsurable. *Lumière sur la Cyberassurance*, or *Lucy* also extensively covers this topic: "C'est aussi un frein au développement de l'assurance cyber : faute de mutualisation, avec un historique de données disponibles limité, les assureurs peinent à trouver un modèle économique viable pour ces garanties. On comprend mieux pourquoi le renouvellement des polices cyber est particulièrement tendu depuis un an."

4 QUESTIONS TO

ADAM DENYER-HAMPTON

Director of International Sales Engineering SecurityScorecard

In your opinion, which word would characterize at best the general context of cyber risk?

This word would be scalability. Cyber risk increases because we live in an heavily interconnected world. For criminals, this situations allows exploitation of vulnerabilities at a scale which has never been seen before. The ecosystem is more and more complex, connecting companies to partners and third party. The attackers have techniques and tools to automate an attack, with the ability to strike at a massive scale.

What is your methodology to quantify the vulnerability of a potential victim, and the ways to improve prevention?

The mantra isn't different to any other area of risk - be aware of what challenges you face, develop mitigation strategies and remediation plans, and have these fully demonstrable to progress to the final risk stage: risk transfer. These capabilities are fully within the grasp of all companies, as should the required skillsets not exist in-house then there are many organisations who can help an entity get to a baseline standard.

The idea is basically to use the same tools as the attackers but in a reverse way. We bring together a community of experts, with the objective to build a defensive line. To evaluate the risk, our approach combines an analysis of the visibility of the vulnerabilities with intelligence threat. Each of these two aspects is important, but it is the reunion of both concepts which allows to compute a kind of reliable temperature, without triggering too many false alarms.

The assistance the insurance industry, in collaboration with SecurityScorecard, can help provide is in identifying the key areas that are most exposed and then direct resources towards making the greatest difference in risk posture. What clients don't want is to spend money that doesn't provide a good return on investment - and this is often seen when there isn't enough insight available as to which areas of weakness pose the greatest risk to the business.

This is an area where using analytics captured during the underwriting stage and then throughout the insurance policy lifecycle, a process known as "continuous underwriting", is extremely valuable in several key areas. Firstly, any issues identified prior to policy inception are capable of being arranged in order of the amount of impact to the overall risk position and this then used as a roadmap for where financial resources should be deployed to combat the risk.

During the lifetime of the insurance policy, carriers can monitor the risk posture of the insured and alert them to new or developing threats when detected - as well as provide guidance on the best steps to take to resolve them before an incident occurs. The final stage is in the run-up to the renewal of the insurance policy, where an overview of the previous 12 months will depict the insured's attentiveness to cyber risk and this in turn allows the underwriter to then consider the terms for the new insurance contract accordingly.

There is a human factor in cyber risk. How is it possible to capture, to some extend, the effect of human behavior inside targeted organizations?

We can obtain some measures of this human factor, for example by monitoring the dark web and identifying usernames or passwords that have been compromised through social engineering. The volume of such compromised assets is an important indicator, since it can be used to identify if cyber education is at the level an organisation would like to reach.

Do you have concerns about insurability of cyber risk?

One of the greatest impacts to the question of insurability of cyber risk relates to a lack of actionable data upon which to rely, combined with the growth of ransomware to epidemic proportions. This perfect storm of limited historical data and large volumes of insured claims was a shockwave felt throughout the insurance industry and directly impacted the availability of capital in the market.

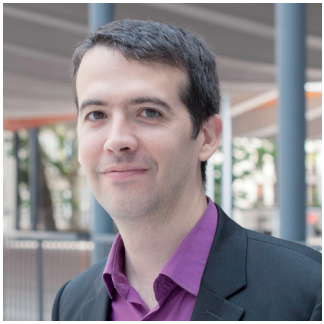
The key issue is to be able to adapt quickly enough. What we have since seen is the growth of companies who can provide data to insurance underwriters and brokers that can be deployed to make cyber insurance a viable sector. Underwriters can articulate to their financial capital providers they have access to data that accurately underscores their risk appetite and selection rationale, whilst at the same time brokers are able to have open conversations with their clients on the specific risks that without due attention being given may have an impact on their business and therefore negatively impact their insurance purchase process.

Unlike any other type insurance, there is no long history of data, no clear indications on how to address the market. The continuous monitoring that we perform precisely aims to fil this gap. This data awareness, and stricter controls around the types of clients insurance carriers are willing to provide insurance to, has led to the perception in some quarters that cyber risk is uninsurable - however this is inaccurate. What has changed is the removal of the commoditisation of cyber insurance as a light-touch nice to have product, into a core tenet of a businesses' risk transfer process with a requirement for organisations to demonstrate a positive cyber risk approach to gain access to insurance products. This has helped underpin a healthy ecosystem where customers can obtain quality products from insurance providers who themselves maintain a large enough reserve of funds to pay claims when made.

OLIVIER LOPEZ

Professor at Sorbonne Université, director of ISUP, co-director of the Joint Research Initiative “Cyber risk: actuarial modeling”

Understanding how risk factors affect the outcomes of cyber events is a key issue to reduce uncertainty and offer affordable insurance coverage, without deteriorating the perimeter of the policies.



The consequences of a cyber incident can be severe for the victim. Ransomware attacks can for example paralyze a company during weeks or months. Apart from direct damages, the consequence can be a slow regime activity that can last additional months and lead to business interruption. Although some claims are more benign, this extreme volatility is a difficulty for the equilibrium of an insurance contract.

Pricing of insurance contracts is not only a matter of finding the most likely scenario. Premiums should incorporate safety loadings that are here to ensure that there will be a reserve large enough to absorb situations that may be less probable, but not unlikely at all. Analyzing these pessimistic scenarios is the task of extreme value analysis, which focuses on the tail of the probability distribution of the losses.

Extreme value analysis is a powerful fields that tries to extrapolate from historical data and determine scenarios that may be beyond the scope of what has been observed before. The robustness of this extrapolation is based on mathematical grounds that allows to assess its reliability and compute confidence intervals.

Nevertheless, extreme value analysis and heterogeneity do not necessarily go well hand in hand. If a portfolio contains a large variety of policyholders, with different risk

factors, sector of activities, and potential consequences in case of attack, an extreme value analysis of related data will tend to provide pessimistic projections: if one considers the subpopulation with the worse extreme case scenario, this scenario will tend to capture all the attention of the statistical methods. It will then consider that this worst case scenario applies to every category of policyholder, although it is improbable that the attack on a small SME has the same consequences as one on an energy provider.

Distinguishing between classes of policyholders is standard in insurance, but the task is more challenging when it is not only question to differentiate the central scenario (which is typically what is done in pure premium computation) but to look at how different categories behave under stress scenarios. An important field of research that we developed consists in combining machine learning techniques with extreme value analysis to perform this efficient segmentation.

The application are important in view of achieving an efficient risk pooling. Once these classes are identified, strategies can be define to optimize the premium so that the safety loadings paid by the less exposed risks are reduced, without penalizing significantly more risky categories. Moreover, these quantitative tools may help to determine a clear frontier between classes of risk that must be transferred or could not be insured through traditional means.

The aim is to enhance efficiency of the economic model of cyber insurance to facilitate its blooming and building a resilient and affordable framework of products.

References

[FLT21] Farkas, S., Lopez, O., & Thomas, M. (2021). *Cyber claim analysis using Generalized Pareto regression trees with applications to insurance*. Insurance: Mathematics and Economics, 98, 92-105.

[FHLT21] Farkas, S., Heranval, A., Lopez, O., & Thomas, M. (2021). *Generalized Pareto Regression Trees for extreme events analysis*. arXiv preprint arXiv:2112.10409.

PHILIPPE TALLEUX

Vice President

at “Institut des actuaires”

Cyber risk is one of the major concerns of economic actors. The demand for protection does not always find an offer for insurance capacity. Many factors could explain that this market has not yet reached a sufficient level of maturity to fulfill customer expectations.

This developing risk is a question at all the different levels : governments and states, industrial and commercial companies, individuals and also insurance companies. Cyber-risk has specificities that disarm the traditional methodologies and question the tools usually used by the insurers.

At the core, the available data is rare and needs to be cleaned and structured to be used under a risk perspective. In this emerging market, the actors of the cyber risk value chain are not organized and may not ever organize themselves to build together structured data. Market competition rules do not allow what was possible after the second world war when insurers shared their data to build the fire claim repositories and a pricing handbook by nature of occupancy (France APSAD). However, the quickly growing cost of claims and the quick evolution of the events embarked under the name of “cyber risk” require a robust data framework which is not currently available. Segregation of claims by nature would lead to a better understanding of the trend, which in turn would help the insurers build capacity and propose adequate guaranties at economical cost.

In addition, cyber risk characteristics push the insurers to rethink their risk acceptance framework:

- Regarding property lines, contrary to casualty lines, the aim of guaranties is to compensate for damages whatever the cause is. In particular, when cyber cause is not formally excluded, physical damages may lead to silent covers. And silent covers are by nature difficult to identify.
- Severe accumulations are more likely to occur as has already by past events.
- Similarly to pandemics, consequences of a cyber event could hit numerous business lines: motor, property, liability, director & officer insurance…

Insurers need to take into account that large catastrophic events could have a comprehensive scope and massively hit their balance sheet. For large accumulation, insurers risk appetite, which is a protection against their bankruptcy, is a strong limitation to their offer. Without a private-public solution, such as the one available for terror risks (e.g. US:TRIA – France: GAREAT…), part of the insurance demand will not be met. The first alerts such as Wannacry have raised the level of insurance company awareness regarding of this accumulating risk on a worldwide basis.

By opposition, data will support a good understanding of what could be considered within a reasonable probability as non-accumulative events: it is a first step to increase the insurers interest for this market and build a broader insurance capacity for some events.

The difficulties the insurers face to build cyber-risk products is amplified by the lack of concern from small and medium-sized industries regarding cyber risks while cyber criminality pressure is quickly rising: for them, cyber-attacks may lead up to bankruptcy. Large companies are so far overweighed in insurance portfolios. This creates an over-exposure to peak risk for insurers, and prevent them from structuring their portfolio around a sustainable mutuality. It could lead insurance market to withdraw after cyber risk casualties.

Finally, the difficulties faced by the insurance market are an illustration of the public authorities concerns. As cyber risk is a matter of national resilience, it is surprising that protection and prevention efforts from both public services and commercial and industrial companies are not broadly promoted by the public authorities. To make these actions efficient, data remains key. Such actions will help reduce claims and also steer customers towards insurance. The community in its whole will benefit from these actions: prevent, protect and insure being less expensive than repair.

To sum-up, the emergence of a cyber risk insurance as part of the national resilience could only be contemplated once the efforts to build an accurate data framework are done. This database is essential for further research on the nature of these polymorph and evolving risk.

RESEARCH INITIATIVE

Cyber Risk: Actuarial Modeling

For more information on the outputs of the research program and the links to the publications, please visit the website of the Joint Research Initiative:
https://sites.google.com/view/cyber-actuarial/home

INSTITUT Louis Bachelier

AXA Research Fund

ENSAE IP PARIS

ISUP