MILLIMAN WHITE PAPER

Cyber risks: What are the challenges for insurers?

Mohamed Benkhalfa, Director
Eliott Pradat, Senior Consultant

On 12 May 2017, more than 300,000 computers in over 150 countries were infected by the WannaCry ransomware, a virus which held personal data hostage. From British hospitals to the French carmaker Renault, thousands of companies and organisations were affected around the world.

Due to its magnitude, this attack has highlighted to the world the *potential of cyber risks to cause significant losses for many companies and over multiple geographies*. Cyber experts have recently estimated that worldwide cybercrime costs will hit $6 trillion annually by 2021.[1] In comparison, the total estimated cost of natural disasters in 2020 was $268 billion,[2] which is about 20 times less than the estimated cost of cyber risk. Looking at these figures, one may ask if cyber risks are insurable. For instance, a major insurance player AXA has called for the setting of alliances between governments and insurers to deal with systemic risks.[3]

How can cyberattacks could cause such huge disasters?

This is mainly due to the highly interconnected nature of IT systems as well as strong dependencies (for instance with the dominance of some cloud service providers and more and more intermediate businesses such as software suppliers), *which make the cyber field prone to the accumulation of risks*. Furthermore, we can consider accumulation as the concentration of insured risks or insurance coverages that may be affected by events or circumstances that cause substantial losses under several insurance policies and potentially over multiple years and geographies.[4]

However, the world is not standing still in response to this threat. Cybersecurity budgeting has been increasing steadily as executives realise the importance of investing in this field. While 2020 was a record year in terms of investments in cybersecurity,

[1] Morgan, S. (13 November 2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. Retrieved 16 December 2020 from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[2] Easton, D. (1 July 2021). The industries most at risk from extreme weather – and how to protect them. World Economic Forum. Retrieved 16 December 2021 from https://www.weforum.org/agenda/2021/07/the-industries-most-at-risk-from-extreme-weather-and-how-to-protect-them/.

[3] Poullennec, S. (1 October 2020). Cyberattaques: AXA en appelle à l'Etat pour protéger les entreprises. LesEchos. Retrieved 16 December 2021 from https://www.lesechos.fr/finance-marches/banque-assurances/cyberattaques-axa-en-appelle-a-letat-pour-proteger-les-entreprises-1250852.

[4] CRO Forum (October 2015). Casualty Accumulation Risk. Retrieved 16 December 2021 from https://www.thecroforum.org/wp-content/uploads/2015/10/CROF-Casualty-Accumulation-Risk-FINALv11.pdf.

with almost $8 billion committed globally,[5] 2021 should outpace this record amount and investments should keep growing. Indeed, most companies still have unprotected data, and poor cybersecurity practices in place while they are handling more data, and with a level of remote working which has reached unprecedented levels following the COVID-19 pandemic.

Where are the insurers in all of this?

As with any other business, cyber insurance solutions are designed to help policyholders better manage their risks, secure their growth and help them expand and play an important role in risk prevention. Insurance can be used to mitigate cyber risks but, as discussed in this document, *several challenges remain open in order to achieve a secure and mature insurance system for this emerging risk*.

First, what is covered by cyber insurance?

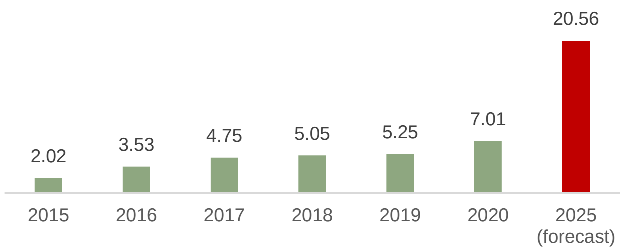
Cyber insurance policies include three types of covers:

- Crisis management, which deals with emergency measures but also the cost of managing the crisis and complying with data protection regulations.
- First-party coverage, which concerns costs incurred by the policyholder following the attack like data recovery, ransom payment (which is currently under legislation review in France) or business interruption.
- Third-party coverage, which provides liability coverage for businesses when a data breach occurs on a third party's network or systems. For example, it includes coverage for lawyers' fees or penalty costs related to the data breach of laws.

… and the current state of cyber insurance in the world?

Sources such as Globaldata suggest that cyber insurance premiums will see double-digit growth, with a forecast of more than $20 billion by 2025. However, these figures are still relatively low in comparison with the potential losses mentioned above for cyber risks.

FIGURE 1: GLOBAL CYBER INSURANCE MARKET ($ BILLIONS)



Source: Globaldata.

While the economic cost of cyber-crime in 2020 was around $1 trillion,[6] S&P notes that, over the same time period, less than $5 billion in damages were insured (*implying a coverage ratio of less than 1%*). Given the premiums forecast, this ratio will remain relatively low with significant differences between companies. Small and medium-sized companies are less insured than the largest companies.[7] As a comparison, natural disasters caused overall losses of more than $5,200 billion since 1980, of which "only" 72% were uninsured losses.[8]

Moreover, quite significant discrepancies can be observed in terms of offers across the world. The significant players in cyber insurance are based in the United States and Great Britain (such as AIG, CHUBB, AXIS and Liberty Mutual) and, in that context, the resilience of European players can be questioned.[9]

A double risk for insurers

In case of a cyber event, policyholders will logically turn to their insurers to be compensated for the losses they have suffered. But what happens if their insurers are also impacted and cannot provide services for an indefinite period? What would be the consequences for the policyholders of not receiving their payments on time? Consequences could be disastrous and negative impacts could spread among businesses.

When it comes to cyber risks, *insurers, like their policyholders, are exposed to cyberattacks, especially because insurers possess large amounts of personal information*. This threat represents the insurer's own cyber risk and is accounted as one of its main adverse likely scenarios in terms of operational risk.

[5] Crunchbase. Report: The Rise Of Global Cybersecurity Venture Funding. Retrieved 16 December 2021 from https://about.crunchbase.com/cybersecurity-research-report-2021/.

[6] Ramasubramanian, S. (7 December 2020). Cybercrime could cost the world almost $1 trillion in 2020, McAfee says. The Hindu. Retrieved 16 December 2021 from https://www.thehindu.com/sci-tech/technology/cybercrime-could-cost-the-world-almost-1-trillion/article33269047.ece.

[7] L'AMRAE (26 May 2021). L'AMRAE éclaire la cyber-assurance avec son étude Lucy. CIO. Retrieved 16 December 2021 from https://www.cio-online.com/actualites/lire-l-amrae-eclaire-la-cyber-assurance-avec-son-etude-lucy-13199.html.

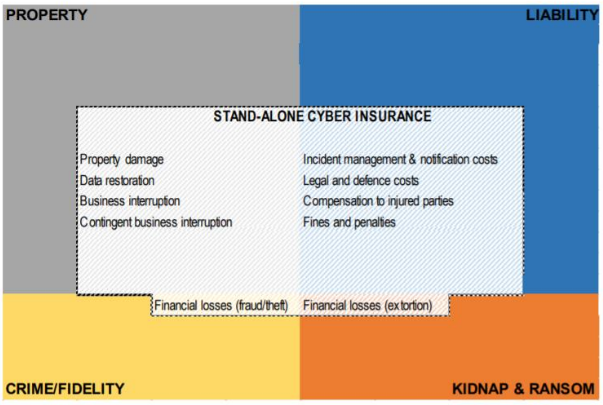
[8] Munich Re. Risks posed by natural disasters. Retrieved 16 December 2021 from https://www.munichre.com/en/risks/natural-disasters-losses-are-trending-upwards.html.

[9] French National Assembly (2021). Rapport: La cyber-assurance. Retrieved 16 December 2021 from https://www.lassuranceenmouvement.com/wp-content/uploads/2021/10/Rapport_La-Cyber-assurance_Valeria_Faure-Muntian_13102021.pdf.

Why do we talk about affirmative and non-affirmative cover?

Besides coverage provided through stand-alone cyber insurance policies, underlying cyber risks might also be covered by other insurance policies which are referred to as non-affirmative or silent cover.

FIGURE 2: OVERLAPS IN COVERAGE FOR CYBER RISKS


PROPERTY
LIABILITY
STAND-ALONE CYBER INSURANCE
Property damage
Data restoration
Business interruption
Contingent business interruption
Incident management & notification costs
Legal and defence costs
Compensation to injured parties
Fines and penalties
Financial losses (fraud/theft)
Financial losses (extortion)
CRIME/FIDELITY
KIDNAP & RANSOM

Source: OECD.

These silent covers represent a real challenge for insurers and amounts at stake could ultimately be much more important than anticipated. For example, cyber analysts have found for two large cyber attacks (Petya and NotPetya) *that nearly 90% of the losses incurred could be attributed to silent covers*.[10]

Whereas silent cover is a major concern for insurers because it could represent a significant unexpected risk, it is also a concern for policyholders because the lack of clarity in some standard insurance contractual terms can lead to a misunderstanding about the extent of coverage for cyber risks.

In this context, the Organisation for Economic Co-operation and Development (OECD) mentioned in its report "Encouraging Clarity in Cyber Insurance Coverage"[11] that providing greater transparency on coverage in the insurance contract for cyber risks was one of the most important actions to support the development of the cyber insurance market; even if significant efforts have been made by insurers on the convergence of policies (harmonisation of coverage definitions and exclusions).

From a regulatory perspective, regulators have expanded their consultations and recommendations regarding a better control of the silent cover risks over the last few years. The Prudential Regulatory Authority (PRA) indicated in 2016 that it was concerned about the poor progress made by insurers in dealing with cyber risks. In 2019 it launched a new survey which found that quantitative assessments of non-affirmative risks were still not sufficient except for the most advanced companies conducting detailed analyses. More recently, the European Insurance and Occupational Pensions Authority (EIOPA) concluded, in the report "Understanding Cyber Insurance,"[12] *the need for the European market to go on investing in solutions to quantify non-affirmative exposures (or silent covers)*.

What are the solutions to assess silent cover?

Even if the assessment of silent covers is deemed difficult and complex for insurers, some solutions exist, such as building scenarios and stress testing portfolios. In addition, EIOPA has summarised a list of initiatives to address silent covers: development of risk profiles, revision and standardisation of the wording in insurance contracts, evaluation of losses using surveys, use of realistic disaster scenarios and development of risk assessment guidelines. US insurers have indicated that they will start affirmatively covering or excluding cyber exposures for most of their commercial property and casualty (P&C) policies.

The process of modelling cyber losses

As explained in the prior section, the cyber risk exposure is made of affirmative and non-affirmative risks. For the latter, models need to expand to a larger number of business lines and will have to take into account the important uncertainty around the correct estimation of the accumulation risks; these characteristics will not be addressed in this paper.

The following section focusses on the underwriting cyber risks (operational risks are addressed in the section “Other challenges related to cyber risks”).

Mapping of risks

As a first step, risks must be identified, along with definitions and examples to list and illustrate the risks addressed. It is also important to know the typology of risks and for instance the possible types of cyberattacks: phishing, ransomware, spyware, theft of strategic information, distributed denial of services etc.

Therefore, insurers must:

- Assess their exposure through portfolio analysis and lines of business impacted as well as identifying dependencies and interconnections
- Classify risks according to their probability of occurrence and severity (and take into account existing and future mitigation actions)

[10] New York State Department of Financial Services (4 February 2021). Cyber Insurance Risk Framework. Retrieved 16 December 2021 from https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

[11] OECD (2020). Encouraging Clarity in Cyber Insurance Coverage. Retrieved 16 December 2021 from https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.

[12] EIOPA (2018). Understanding Cyber Insurance – A Structured Dialogue With Insurance Companies. Retrieved 16 December 2021 from https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf.

Ultimately a mapping of risks can be established and be refined along with the following steps of modelling.

Identification of cause and effect dynamics

This second part focusses on better understanding the risk. For several years now, the systematic integration of the cause-effect chain has been used in natural disaster modelling because it has allowed insurers to assess risks with greater accuracy, to transfer findings from data-rich regions to others with more sparse data and to better understand the process of loss generation.

When looking at cyber insurance, *the lack of big data sets and the permanent evolution of the risk landscape should encourage actors to consider this approach*.

The risk drivers affecting cyber losses are numerous and examples are illustrated in the table in Figure 3.

FIGURE 3: EXAMPLES OF RISK DRIVERS

Environment	Causes	Effects
New technologies New computer legislation Electoral events …	Hacking Human error Technical failure Physical attack Natural events Indirect events …	Covered and noncovered losses Market impact Policyholder default Reputation Cyber underwriting Cyber management …

Data

When it comes to modelling cyber risks, one of the main challenges remains the availability of data because there are very limited historical data sets of claims available (and would be claims not systematically reported). Hence the integration of expert judgement and external data will be a key factor in the modelling to improve the predictability of cyber risk losses.

To date, the majority of cyber risk claims data comes from the US. However, most cyberattacks go unreported because generally companies are not compelled or incentivised to report cyberattacks, so they are missing from the data. In France and in Europe, there is currently no public database that can be used for insurance modelling of this risk but *EIOPA intends to promote the development of a harmonised risk insurance system* and taxonomy to record cyber incidents to underpin the cyber underwriting model, *using a centralised, anonymised cyber incident database (per the French National Assembly)*.

After identifying the risks, its causes and effects and data availability, the next step is to select approaches to model the underlying risks. Two approaches are proposed below.

Examples of modelling approaches

Scenario-based approach

The scenario approach allows complex relationships between observable risk factors and losses to be taken into account. Three steps are defined below for this approach:

1. Setting up relevant scenarios: This step consists of building scenarios reflecting potential risk accumulations and taking into account the chains of cause and effect and other dynamics on a consistent and realistic basis. In particular, the following elements must be taken into account when building scenarios: trigger events, spatial timelines and consequences.

2. Estimated probabilities of the determined scenarios can be based on expert opinion and/or the observation of similar historical events identified beforehand: *The probability of occurrence of the scenario can also be estimated on the basis of frequency modelling*.

3. Link to the portfolio exposure: The modelled scenarios should be linked to the portfolio in order to model losses, which may require additional assumptions for the exposure measures.

Frequency-severity approach

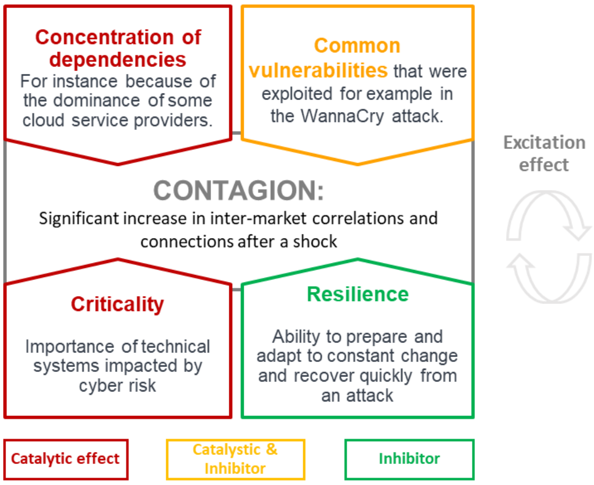
Frequency models: Among the models that can be considered, the Hawkes and epidemiological models are particularly suitable to the generation of losses for accumulation risks where interconnections and interdependencies are key factors.

Both models are particularly well suited for modelling contagion risks, which can be defined as a significant increase in intermarket correlations and connections after a shock. Contagion risks include cyber risk, as illustrated in Figure 4.

- Epidemiological models: They allow a detailed modelling of the existing links between the different insured populations and aim at establishing propagation scenarios.

- Hawkes models: These processes were initially developed for earthquakes and are used for counting claims just like Poisson processes. However, the latter are not adapted due to the observed accumulation when it comes to cyberattacks. Hawkes processes are able to detect self-excitation, which allows modelling of cluster effects, i.e., coming from the same origin. Moreover, clusters can also interact with each other; each event in a cluster increases the probability of the occurrence of new events in other clusters (for instance the banking sector with the insurance sector).

FIGURE 4: CONTAGION FOR CYBER RISKS


Concentration of dependencies
For instance because of the dominance of some cloud service providers.
Common vulnerabilities that were exploited for example in the WannaCry attack.
Excitation effect
CONTAGION:
Significant increase in inter-market correlations and connections after a shock
Criticality
Importance of technical systems impacted by cyber risk
Resilience
Ability to prepare and adapt to constant change and recover quickly from an attack
Catalytic effect
Catalystic & Inhibitor
Inhibitor

Source: Milliman.

Severity models: The severity and development of the risk can be modelled by applying classical actuarial models—generalised linear models on gamma distribution, generalised Pareto distribution (GPD) or Classification and Regression Tree (CART) algorithms—to new models more specific to the cyber insurance. For example, proxy formulas can be used such as the model proposed by the Ponemon Institute, which expresses the cost of claims as a function of the volume of stolen data. Also, for instance, when GPDs result in a distribution of cyber claims with infinite tails (i.e., the risk is not insurable when policies have no limit of cover), then they can be combined with CART models to produce right-tailed homogeneous risk buckets before using GPD fitting (more details are available in the article “Cyber claim analysis through GPD Trees with applications to insurance”[13]).

The last step consists in generating losses from frequency-severity models by taking into account the dependency between these two components, especially on extreme adverse scenarios. This is an additional challenge in comparision with classical models, becaise for adversarial risks like cyber the frequency and severity are not independent (this relation could be modelled for example by applying a factor fitted from the difference between the actual severity and modelled severity by frequency[14]).

Ultimately the frequency-severity models can also be calibrated on the basis of previously defined scenarios. The point can then be underlined that the *combination of scenario/statistical approaches can be an efficient solution to achieve a more accurate assessment of the risks*.

Approaches to cyber risk modelling

Underwriting cyber risk

As presented in the previous section, multiple approaches exist to model cyber risks and the choice of approach should be made based on the conclusions of risk mapping, identification of causes and effects and the data collected.

For instance, the multivariate Hawkes process is well suited to capture self-excitation and interactions as detailed in the article "Multivariate Hawkes process for cyber insurance"[15] and these characteristics apply for instance to data breaches in cyber insurance.

In addition, the techniques used for modelling cyber risks can be extended for many accumulation risks, for instance in modelling COVID-19 impacts, as illustrated in the paper "Pandemic risk modelling in Solvency II internal models: Example of COVID-19,"[16] where susceptible, infectious and recovered (SIR) models are investigated to replicate the specificities of COVID-19.

FIGURE 5: EXAMPLES OF ACCUMULATIONS RISKS

Asbestos
Pandemic
Cyber Risk
Nanotechnology
Climate Change
E-cigarettes

Source: Milliman.

Operational cyber risk

The most common approach for insurers to assess their own cyber risks is handled through a scenario-based approach: multiple sets of scenarios are calibrated and tested. Statistical models can be used as an alternative to the scenario-based approach but it requires historical data for calibration, which is not always available when modelling a company’s cyber risk. Modellers must then turn to industry data pools or expert opinion.

However, the limits of these approaches are twofold; first, there is no guarantee that external data fits with a company's own structure, and secondly expert judgement should be extrapolated into a loss probabilistic distribution function, which can be complex and must not be considered as robust statistical outputs.

[13] Farkas, S. et al. Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance. HAL. Retrieved 16 December 2021 from https://hal.archives-ouvertes.fr/hal-02118080v2.

[14] Zhou, J. (May 2016). GLM With Correlated Frequency & Severity – An Ontario Persona Auto Application. Casualty Actuarial Society. Retrieved 16 December 2021 from https://www.casact.org/sites/default/files/presentation /spring_2016_presentations_c-9.pdf.

[15] Bessy-Roland, Y. et al. (June 2020). Multivariate Hawkes process for cyber insurance. Annals of Actuarial Science, 15(1), 14-39. Retrieved 16 December 2021 from https://www.researchgate.net/publication/342246321 _Multivariate_Hawkes_process_for_cyber_insurance.

[16] Boumezoued, A. & Titon, E. (March 2020). Pandemic Risk Modelling in Solvency II Internal Models: Example of COVID-19. Milliman White Paper. Retrieved 16 December 2021 from https://fr.milliman.com/- /media/milliman/pdfs/articles/pandemic-risk-modelling.ashx.

To overcome those limitations of traditional models, Milliman proposes that, through its tool CRisALIS™, data-driven analyses such as expert-derived causal modelling and artificial intelligence (AI) can be used. In that case, this tool allows for a bespoke holistic forward-looking approach to model operational cyber risk.

More details on causal modelling are given in the Milliman paper "Know your blind spots."[17]

Other challenges related to cyber risks

The systemic nature cyber risk

As introduced in this paper, cyber risks are a type of accumulation risk which means that some cyber events could damage many policies at the same time, causing massive losses to insurers, as explained in the Milliman paper "Could cyber risk be the next Big Short?"[18] For example, the SolarWind attack, an enterprise network software which was the subject of a massive cybersecurity attack, spread to the company's clients, including Microsoft and US government agencies.

The question remains regarding the capacity of the (re)insurance market to handle alone the cyber systemic risk or *whether government support is needed in cases of extreme events*. According to Gabriel Bernardiro (chairman of EIOPA from 2011 to 2021), the insurance industry does not have the capacity to deal alone with systemic cyber events. Hence some forms of government backstop associated with private reinsurance coverage could be established (with a focus on not leading the insurance market to take on an irresponsible levels of risk) to provide coverage in the event of a systemic cyber risk event of a scale that has not yet occurred (as exposed in the Milliman paper "Towards covering operating losses?"[19] regarding operating losses induced by COVID-19). This proposal has also been submitted by AXA, which calls for alliances with governments.

Setting up and improving the cyber insurance framework

Evaluating systemic risks is an important and difficult challenge which should be comprised in a global framework. The latter is essential to ensure financial stability while underwriting (and managing) cyber insurance. Recently the New York State Department of Financial Services issued a cyber insurance risk framework with best practices, including:[20]

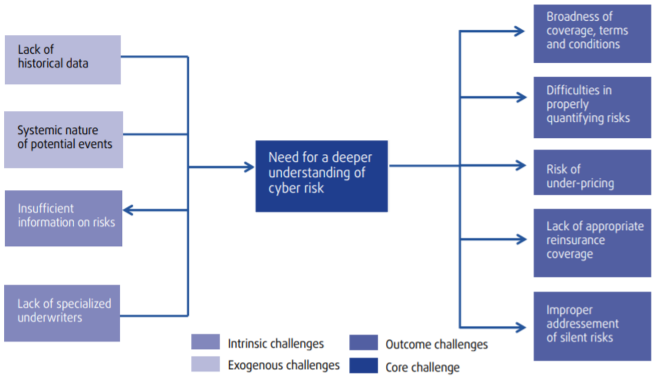
- Establish a formal cyber insurance risk strategy
- Manage and eliminate exposure to silent cyber
- Evaluate systemic risks
- Measure insured risks
- Educate insureds and insurance producers
- Obtain cybersecurity expertise

The last two elements emphasise the necessity of better understanding the cyber risk threats and impacts as detailed in the next paragraph. Moreover, insurers that do not write cyber insurance should still evaluate their exposures to cyber risks and take actions if necessary.

Better understanding of the cyber risk

As illustrated in the EIOPA report "Understanding Cyber Insurance,[21] *a deeper understanding of cyber risk is still needed and is identified as the core challenge for the majority of insurers*.

FIGURE 6: KEY CONCERNS RAISED BY INSURERS


Lack of historical data
Systemic nature of potential events
Insufficient information on risks
Lack of specialized underwriters
Need for a deeper understanding of cyber risk
Broadness of coverage, terms and conditions
Difficulties in properly quantifying risks
Risk of under-pricing
Lack of appropriate reinsurance coverage
Improper addressement of silent risks
Intrinsic challenges
Exogenous challenges
Outcome challenges
Core challenge

Source: EIOPA.

It must be emphasised that all the work being done to better understand the risk should enable refinement of existing models and therefore help to tackle outcome challenges like quantifying risks, addressing silent risks or diminishing the risk of underpricing.

[17] Harner, C., Beck, C. & Fleisher, B. (November 2020). Know Your Blind Spots. Milliman White Paper. Retrieved 16 December 2021 from https://www.milliman.com/-/media/milliman/pdfs/2021-articles/3-19-21-know-your-cyber-blind-spots.ashx.

[18] Beck, C. & Harner, C. (March 2019). Could Cyber Risk Be the Next Big Short? Milliman White Paper. Retrieved 16 December 2021 from https://www.milliman.com/en/insight/-/media/Milliman/importedfiles/uploadedFiles/insight/2019/cyber-risk-big-short.ashx.

[19] Pradat. E. et al. (July 2020). Towards covering operating losses? The European Actuary. Retrieved 16 December 2021 from https://us.milliman.com/-/media/milliman/pdfs/articles/tea-23-jul2020.ashx.

[20] New York State Department of Financial Services, op cit.

[21] EIOPA, Understanding Cyber Insurance, op cit.

An example of proposed actions

The Insurance Study Group of the French National Assembly published a report in October 2021 which drew a picture of the current situation and proposed ways to improve it, through a series of governmental proposals.

This report lists 20 proposals in three areas:

1. **Clarification and establishment of a framework** by adopting a common definition of cyber risks and cyberattacks and clarifying the legislation around this risk.

   Among other proposals, the report suggests prohibiting insurance companies from paying ransoms, as it encourages cybercrime and there is no guarantee that the ransom paid allows a return to the original situation. Indeed, the ransom payment even encourages new designs of cyberattacks, and data suffering an attack is often permanently corrupted. This vicious circle promotes the development of a deep opaque ecosystem. On that point, AXA has already publicly announced it will not insure and compensate this kind of ransom in France.[22]

   Then, the report recommends that insurers focus more on prevention, support and covering financial impacts for companies such as operating losses and material damages (mainly IT system restructuring).

2. **Strengthen resilience and defence against cyber risks**

   This second area includes many proposals such as:

   - Promoting the cyber surveillance system cybermalveillance.gouv.fr to companies and authorities
   - Anonymous collection and development of a statistical database through this system
   - The increase of technical and financial resources (magistrate training, number of justice/police personnel),
   - Awareness campaign for employees of small and medium-sized companies as well as cybersecurity prerequisite for communities, governments and industry

   It can be noted that those proposals are aligned with best practices previously mentioned in the section above, "Setting up and improving the cyber insurance framework": the insurer must act not only to cover this risk but also to upstream and prevent this risk.

   In addition, it is proposed to encourage European institutions to introduce a "small business act" for cybersecurity in France to increase the use of best practices and to require companies working with the state or which have the status of Essentials Services Providers (OSE) or Operators of Vital Importance (OIV) to subscribe cyber insurance policy.

3. **Develop the cyber insurance market**

   This area includes the development and the harmonisation at the European level of cyber insurance offers and services. The strategy is built around four main lines of actions:

   - Encourage the creation of a mechanism for evaluating cyber insurance offers
   - Coordinate the players in the market in order to harmonise the vocabulary, the offers and the risk selection criteria (for example, by taking into account a grading of companies based on their cybersecurity protection)
   - Create a new insurance branch dedicated to cyber insurance
   - Develop hybrid cybersecurity and cyber insurance solutions for small and medium-sized businesses and communities, in order to reinforce the role of the insurer against this threat.

   As for the rest of the cyber insurance industry, the follow-up to this report will be closely scrutinised.

Milliman

CONTACT
Mohamed Benkhalfa, IA
mohamed.benkhalfa@milliman.com

Eliott Pradat, IA
eliott.pradat@milliman.com

[22] Bajak, F. (9 May 2021). Insurer AXA to stop paying for ransomware crime payments in France. Insurance Journal. Retrieved 16 December 2021 from https://www.insurancejournal.com/news/international/2021/05/09/613255.htm.