# Cyberinsurance, a risk nearly like the others?

**Benjamin Ducos** & **Luc de Lignières**,
*AXA*

***Abstract***:
"Cyberinsurance" is still a niche market worldwide. Given new uses, regulations, and ever more frequent incidents, this market is growing strongly. To respond to the demand for solid coverage, insurance companies must draft quality contracts with high guarantees. Among the assets of the big, global insurance firms are their actuarial know-how, granular knowledge of cyberrisks and the models of risks they have built… but cyberinsurance has noteworthy technical particularities. Furthermore, insurers must protect themselves against such risks, which ignore borders and could incapacitate insurance firms.

For several months now, the sharp increase in the number of cyberattacks and their extreme effects on the operations, finances or reputations of the targeted organizations have intensified the need of firms and institutions for efficient protection. The cyberinsurance market, though estimated at less than five billion euros, is experiencing strong growth (30% per year). Two questions have cropped up for insurance companies. How can their offers of cyberinsurance help protect clients, whether individuals or firms? And how will insurers hedge against the operational risk of not being able to compensate the insured when targeted by cybertattacks?[1]

## Cyberinsurance, a risk (nearly) like the others?

The risks covered by cyberinsurance share characteristics with the traditional risks covered by insurance policies that offer to compensate damages. The risks are uncertain and unpredictable; coverage is defined in terms of guarantees and offered to individuals and firms; and it may be extended to one or several insured parties. A final similarity with traditional insurance, prevention is decisive.

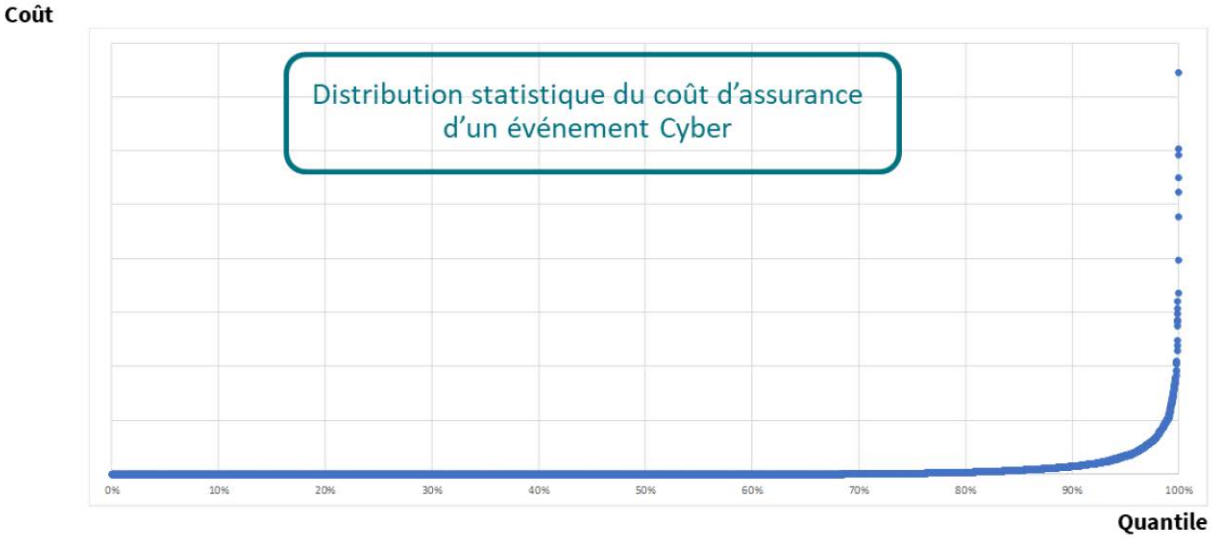
Nonetheless, the risks covered by cyberinsurance have specific characteristics. First of all, they are systemic. Like an earthquake, the effects spread rapidly and simultaneously affect all categories of the insured, whether private persons or firms. Unlike an earthquake however, the potential risk has no geographic bounds; and we do not know much about it. The distribution model for the risks covered by cyberinsurance resembles a Dirac delta function (*cf*. Figure 1). Compared with average events with a moderate impact, the big event corresponding to a cyber-related risk is deemed to be very rare but to have extreme consequences.[2] Till now, no major event has happened such that we could calculate the impact! The cost of the "big one" is, therefore, subject to interpretation and to the estimates made by the adjustors, computer scientists, model-builders, etc., who simulate risks. As a consequence, insurance premiums imperfectly reflect the risks covered by insurance. As long as the big event does not happen, there will be no certainty about how to build a model of cyberinsurance's profitability. A final difference: cyberthreats correspond to a constantly evolving

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in March 2020.

[2] The Dirac delta function is infinite at zero but equals zero everywhere else. Applied in cyberinsurance, this means that an event with a (nearly) zero probability has an extreme cost whereas the other events in the distribution cost (nearly) nothing.

risk, dependent on advances in digital technology — the advances made by information system operators, advances in the security procedures adopted by clients, and advances in hackers' ingenuity.

**Figure 1**: Statistical distribution of the insurance cost of a cyberattack




Insurers look at cyberthreats from two positions. In the front seat, they sit behind the steering wheel as the experts for insuring this risk; but in the back seat, they are passengers, a major industry in the business world and, therefore, a potential target of cyberattacks. An insurance company's strategy is thus two-pronged: be capable of offering insurance protection against cyberthreats to clients while protecting itself against the operational risk of cyberattacks against the company. For this reason, the services managing information about the insurer's own operational risks must work very closely with the services of sales and expertise (for pricing products or assessing risk exposure) in order to gain qualitative and quantitative knowledge about the risks related to cyberthreats.

Qualitative knowledge comes from the monitoring, day after day, of the risks and threats of concern to insurance companies and, too, from a close dialog between persons at every level in control functions so as to mutually improve the stock of knowledge with information on the types of incidents that have affected the insured. Lines have to be regularly drawn between events in order to increase our understanding of the latter. A week does not go by without a cyberincident triggering a technical investigation (by the insurance company or by the insured party). Quantitative information provides a key to improving our understanding, since it helps us know and, therefore, act on the level of acceptance of cyberthreats. For this purpose, insurers have to gauge their exposure to such risks both in their worldwide insurance business and in their own operations. Studies that quantify these risks must come out of a fine, statistical understanding of the insurer's global exposure to cyberthreats.

As a top-ranking financial institution that is exposed to cyberattacks against its clients and against itself, insurance companies are well positioned on this topic. As both a target of cyberthreats and a major player in prevention and protection, they are able to devote more means than other businesses to understanding these risks. Furthermore, this "intimate" knowledge can be shared with the function of expertise that insurers perform for the clients who take out insurance policies.

### *From "nonaffirmative" to "affirmative" coverage*

For insurance companies and policyholders, two cases exist in case of a cyberattack:

● either an implied protection in traditional policies (of insurance for damages to goods or civil liability) cover the ensuing risks. This is called "silent" or "nonaffirmative coverage".

● or else the insurance policy spells out a specific protection. There are three sorts of this so-called "affirmative coverage":

- *a)* for firms, "first party" damage insurance covers the losses related to the policyholder's goods or property (data, the interruption of business, the ransom paid, acts of extortion, etc.);
- *b)* for firms, third-party (civil liability) insurance protects the policyholder against claims for damages to third parties (leaked personal data, errors and omissions due to cyberthreats, etc.); and
- *c)* for persons, coverage is offered for identity theft, payment card theft, disputes with e-businesses or actions for restoring the person's e-reputation on the Internet.

We might imagine that silent coverage would sufficiently protect a policyholder against cyberthreats and, therefore, that affirmative coverage would be useless. This is not so, because affirmative coverage carries quite real advantages. To illustrate the difference between the two, let us suppose that a cyberattack has disrupted a factory's computer programs and, in addition, has caused a fire to break out in the factory. Silent coverage comes into play when the fire damages goods, whereas affirmative coverage will also take in charge losses related to data. Let us suppose that the factory does not burn down but that it can no longer operate. Silent coverage is of no help if there is no material damage (to machines for example); and the losses due to an interruption of business resulting from material damages are not covered. In contrast, affirmative coverage will not only compensate the loss of data but also serve as a first-party business interruption insurance.

## Cyberinsurance: New uses

Cyberinsurance is a product of its times, its development resulting from a combination of factors related to technology, regulations and events. First of all, the massive use of data and the rapid digitization of exchanges with users or clients has exposed organizations to information-related risks (leaks, piracy, etc.). The new uses of dematerialized and shared services (such as the cloud) increase the surface attack by expanding it (via outsourcing) beyond an organization's usual bounds. Concomitantly, regulatory measures and judicialization have given the American cyberinsurance market a head start over the rest of the world. As of October 2011, the Securities and Exchange Commission (SEC) required that the companies that manage savings report cybersecurity incidents immediately. Since then, lawmakers (in particular in Europe) and regulatory authorities in the insurance market have been goading operators to adopt robust security procedures. Insurance has thus come to be seen as a mainstay for managing cyberthreats.

In 2016, the EU's NIS Directive on the security of network and information systems required each member state to identify its critical economic sectors and reinforce cybersecurity there. Other rules and regulations have also probably accelerated the push for cyberinsurance. The new rules for protecting personal data (Personal Identifiable Information, PII), such as the Payment Card Industry Data Security Standard (PCI-DSS) along with the enforcement since May 2018 of the EU's General Data Protection Regulation (GDPR), have pushed firms to invest in protecting themselves and to fulfill requirements about reporting incidents to authorities. All this has probably led many a firm to take out insurance with better coverage.

However the international scope of cyberthreats is at odds with regulations that apply in geographically bounded zones. The nature of the coverage provided varies from country to country depending on events or the domestic market's maturity, which is highly variable between, for instance, the United States, Spain and France. Coverage for "ransoms" used to be scarce, but it has grown since the two major ransomware attacks in 2017 (WannaCry and NotPetya). The risks related to a cyberattack are obvious if the attack is sudden and worldwide (as in the case of WannaCry); but they are harder to gauge when the attack is stealthy and gradual (malware), when it is hard to relate damages to the attack. Given the guarantees stipulated in insurance policies, the difficulty of assessing damages has increased while the loss expectancy as calculated from past events (and normally used to draw up a list of specifications) is seldom known or even missing. Besides, clients might not be willing to report, for example, the points of vulnerability in their information systems or the demands for ransom they have received.

We are forced to admit that, although cyberattacks are ever more frequent and a week does not go by without a firm suffering losses due to the mounting sophistication of such attacks, a large-scale "cyberstorm" has not yet brewed that launches massive, simultaneous attacks for a single purpose against several institutions or organizations in several lands. In November 2018, Institut Montaigne worked out two scenarios of such a storm based on a quantified simulation by Lloyd's of London.[3] According to this assessment, losses worldwide (calculated by using data from 2017) would amount to between $4.6 and $53.1 billion, As we see, these scenarios vary widely owing to the degree of uncertainty. This is the context in which the market is looking for a solution. Insurance companies are undeniably a key player in this quest, owing to their capacity for analyzing data, building models of coming risks and, if need be, providing coverage for disasters.

For insurers, assessing the risks of a cyberthreat depends, above all, on what they know about their own exposure to such risks and on their ability to link each form of coverage offered to clients to an amount set in the insurance policy. This is the key to improving the visibility of cyberinsurance coverage. As for any insurance, this provides the grounds for calculating the amount of premiums for insurance policies. An insurer must know this amount for each type of coverage, each guarantee, figuring in the policy, and for each type of insurance by country and for the whole world. In the case of affirmative coverage, risk exposure is measured for each risk. In the case of silent coverage (in traditional contracts), it is measured by monitoring the exposure to damages (of property and goods) and in matters of civil liability. Finally, since cyberthreats are constantly evolving, this analysis of exposure must be regularly updated, along with the amount of funds to be set aside and the sorts of guarantees and coverage to be offered. Priority must also be given to monitoring loss expectancies. Insurance companies can gradually refine their view of cyberthreats by using the history of disasters, which grows longer over the years as the list of events to be covered expands and the market grows. As previously pointed out however, the events related to cyberthreats tend toward a Dirac distribution.

The pricing of premiums mainly results from the theoretically expected average of all potentially occurring disasters. When few disasters have occurred (as in the case of cyberinsurance), the historical average of disasters can be helpful for pricing insurance products. As we easily see from the curve in Figure 1 however, an extreme event will weigh heavily on the theoretical average — much more so than in traditional insurance policies.

Furthermore, insurance companies have to muster the funds needed to absorb the costs when the extreme event occurs. This capital cost must be factored into the premium calculated for a cyberinsurance policy. The return on capital is theoretically estimated to amount to a third of the premium for cyberinsurance, as compared with less than 10% for damage insurance policies. The extreme event, owing to its double impact on the insurance premium (via its share in the theoretical average and in the return on capital), becomes the major factor for setting the insurance premium. Neglecting to assess the extreme event means, for sure, underestimating cyberinsurance premiums.

[3] *Cf*. the thirteen recommendations for increasing the cyberresilience of our economy and society in: INSTITUT MONTAIGNE (2018) *Cybermenace: avis de tempête* (Paris: Institut Montaigne), 120p., available via https://www.institutmontaigne.org/publications/cybermenace-avis-de-tempete.

The foregoing remarks draw our attention to the reinsurance market. This market for insuring insurers helps companies reduce the cost of the extreme event either by setting a ceiling on it (what is called an "excess of loss" reinsurance) or by sharing it (what is called "quote share" reinsurance). Other sorts of coverage, such as catastrophe bonds (catbonds), can also help reduce the risks for insurers who offer cyberinsurance. Under these bond-related arrangements, the extreme risk is shifted onto the financial market under predetermined conditions (market index, amount, etc.).

### *A sharp rise in demand*

The businesses that take out cyberinsurance policies are mostly financial services, software editors or developers and, too, companies in the hotel industry and retail trade, not to forget health-care firms. They are all trying to protect themselves against the losses and extra costs that would result from a cyberattack (costs related to communications and the management of the return to normalcy). In the United States or United Kingdom, one out of two firms has declared that it has taken out cyberinsurance.

While usefully helping to cover the risks for policyholding firms, insurance companies are prudent, as AM Best has pointed out in its report, "Cyber insurers are profitable today, but wary of tomorrow's risks".[4] In effect, these insurers see to it that their exposure relative to their financial capacity and policyholder surplus is limited. Although the world market for cyberinsurance was estimated to amount to approximately $5.3 billion in 2018,[5] aggregate statistics on cyberinsurance worldwide are still lacking either because of the varieties of regulations and regulatory authorities (EIOPA in Europe, NAIC in the United States, OSFI in Canada, etc.), or because insurance operators are not subject to similar reporting requirements. Nonetheless, we observe a strong growth in subscriptions to cyberinsurance policies. In a market growing by about 30% per year, analysts estimate that the cyberinsurance might double by 2020 and gradually rise to about $20 billion by 2025.[6] The American market, older and maturer, started growing at the turn of the century; in 2017, its insurance premiums amounted to $3.1 billion.[7] By comparison, French cyberinsurance is relatively young, amounting to about €80 million at the end of 2018.

## Insuring clients and the company's self-protection

The major cyberevents to which AXA might be exposed entail risks of two sorts: those related to the coverage provided to policyholders and those related to an attack that affects AXA's own operations.

Hackers are the major source of these risks. Their interventions either target as many victims as possible and cause massive damage or else take aim at a single firm, after having sounded in advance its points of technological vulnerability, and try to do as much harm as possible. An example of the first case: the ransomware WannaCry in May 2017, which took advantage of a flaw in Windows that the editor had patched two months earlier — a patch that several companies had not yet installed. The virus infected many unpatched computers and caused big losses even though the target was not specific. An example of the second case: the attack in December 2013 on Target, a firm ranking third among American supermarkets. The target was specific; and the collateral damage on other firms, very small. Under extreme scenarios, the risks for insurance companies is maximal in the first case, since the amount of compensation depends on the number of victims, which cannot be predicted, whereas, in the second case, damages cannot exceed the limits set under the insurance policy taken out by the targeted firm.

[4] https://www.insurancejournal.com/news/national/2019/06/18/529747.htm

[5] PwC (2015)"Insurance 2020 & beyond: Reaping the dividends of cyber resilience", 20p. available via https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience,pdf.

[6] See the PwC report mentioned in the foregoing note and Munich Re (2018) *Cyber insurance market outlook* at https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-market-outlook-2018.html.

[7] National Association of Insurance Commissioners' s report in August 2018.

In contrast with these risks to policyholders, if its operations are specifically targeted (the second case), the risks for AXA will be maximal. whereas the repercussions of an attack corresponding to the first case will be contained within the limits of a "standard" protection.

To keep track of the risks covered by its insurance policies, AXA has developed a multistage model. The first stage identifies and collects information on the exposure to cyber-related risks by policy (the types and amounts of coverage). During a second stage, existing or potential scenarios are "physically" built to determine AXA's maximal exposure. During the final, third, stage, this view by scenario is statistically transposed to assign costs of the policy for AXA itself to the periods when the events covered by insurance actually occur. This approach is updated annually with: the new occurrences of such events, the feedback about the disaster, and improvements in data collection and model-building. As we see, the second stage is the key to measuring AXA's exposure to the extreme risks covered by cyberinsurance. It involves three principal actions:

- Forming and updating the library of scenarios. Which scenarios are to be deemed critical given the typology of risks (categories of clients, types of coverage, etc.)? Which market scenarios serve as benchmarks?
- Designing the "physical" model. As in an industrial process and depending on the scenario used, AXA establishes hypotheses to build a model. How does an event spread in the cyber realm? Who is affected? How destructive is it? The degree of destruction depends, among other things, on the sorts of clients affected. The answers to these questions and the model built will enable us to estimate the theoretical maximum costs to which AXA will be exposed.
- Presenting findings to experts (whether from AXA or academia) or running comparisons with other models on the market.

Given all this, the following skills are needed to discern the risk to be insured: knowledge of the insurance business (of the mechanics of cyberinsurance and of the types of coverage); actuarial qualifications (data collection and statistics); and understanding of the sort of risk. Ransomware or an attack against shared, dematerialized computing services, such as the cloud do not have the same market impact. AXA is developing in house this knowledge, which is enhanced with academic research, in particular through a joint research initiative with ENSAE (École Nationale de la Statistique et de l'Administration Économique) and Sorbonne University. The AXA Fund for Research finances chairs in this field and thus helps to bring in-house and academic research into contact.

As an operational risk for the insurance company itself, both well-honed risk-management skills and a vast knowledge of information systems are needed. AXA has built models of plausible scenarios under which all or part of its information systems would be attacked and become unavailable or have their data corrupted. These scenarios are analyzed, dissected and assigned units of value (costs of personnel and of remedial actions, operating losses, etc.). A realistic cost can thus be set for the scenario. The data used come from the firm itself (data about computers, etc.), from recent incidents it has experienced and, in some cases, from well-informed sources outside the firm (consultancy firms, other insurance firms, trade associations). These scenarios are updated annually, with information collected throughout the AXA group. The sum of these scenarios, or their correlation, can be used to calculate a capital requirement under the EU's Solvency II directive. Besides satisfying regulatory requirements, this work helps us quantify the eventual impact of major events and rank the priorities related to preventing such events or amortizing their impact.

This work on quantification is not bunkerized; it is performed within a global organization with complementary lines of defense. Operatives are in the front rank of managing the risks affecting their activities, but they have the backing of experts who refer to the cyberdefense strategy that Axa Group's division of security has set and monitors. Positions in this second line of defense have been set up in risk management. They help us anticipate risks by building a model and, too, raising questions about the decisions to be made during meetings so as to obtain a reliable control environment. These risk-management experts also help to see to it that means are allocated to the right priorities and to organize the feedback to be transmitted to the risk-management committee. For top-level governance and decision-making, the Group Information Risk Board decides whether to commit the Group to preventive or remedial actions. Such actions are, of course, regularly audited for the sake of making improvements.

## Conclusion

In general, the decision to take out insurance to cover a risk is motivated by the disaster that will cause major economic losses. The disaster underscores the need for the protection of a policy that insures goods (private persons) or business activities under any circumstances (client firms). Insurers base their activities on an estimate of the risks given the past losses due to such risks. The operational risks under the Solvency II Directive are limited to the firm. They are managed by anticipating the extreme events with which the firm might have to cope; and they are very marginally based on past events. These two approaches (the risks related to policies and the risks to the insurer's own operations) are hard to follow in the case of cyber-related risks. These risks are new to insurance; and no one knows how to quantify past losses, nor to fully assess risks that they are ceaselessly evolving. For example, a current problem is: when should acts of piracy be considered to be acts of war? Nonetheless, as we all know, cyber-related risks are potentially very dangerous, and this justifies the protection provided by insurance. Given the demand for this protection, insurance companies have to assume an unknown risk that they are unable to assess in terms of past events.

Cyber-related risks are now inherent in all activities, whether entrepreneurial or individual. Insurers must accompany their clients by providing advice about prevention and solutions for protection in line with the client's needs. The stake for insurers is to always be capable of serving their clients. In ordinary times, they protect the data entrusted to them; and in case of a disaster, they assist policyholders. In the case of a natural catastrophe, policyholders legitimately expect their insurance companies to stay capable of responding. This expectation still holds for cyber events: the insurer must be capable of withstanding an attack. Insurers must, therefore, anticipate risks and always be in the forefront of protection. The situation in the case of cyberattacks comes down to being capable of offering clients the coverage they demand; but to do this, insurers must aim at a very high level of protection of their own operations — a new, but stimulating, challenge!