PERSPECTIVES

Cyber insurance – Understanding and assessing the threat to build the right insurance policy

May 2023

Though the criticality of cyber risk is now at the forefront of every economic actor's mind, the technical complexity of this risk and the constant changes to the threat continue to make it difficult to create insurance products that are adapted to the needs of the client and profitable for insurers.

In light of what can be vital stakes facing market actors, it is necessary to answer the taxing question of cyber risk insurability. To do so, knowledge of the threat and financial quantification must come together to build credible scenarios on which to base the insurance models that will enable stakeholders to agree.

Accuracy combines its skills in financial modelling with risk quantification technology drawn from Citalid's dynamic analysis of the cyber threat in order to inform its clients' decision-making in this critical area.

—

Cyber insurance first came to light at the beginning of the 2000s and has since developed significantly, growing from risk coverage linked to viruses and data loss to civil liability and operating losses.

Though the global cyber risk insurance market, representing around $9 billion today, is essentially captured by the US market, the same risk targets European actors, who, as a result, have the same insurance needs. However, the high loss ratio in 2020 in the context of a very narrow client base led insurers to tighten their conditions generally and even to withdraw certain offers. In 2021, the French cyber risk market represented around €220 million in revenue, that is, 3.1% of property damage insurance premiums for professionals, valued at €7 billion over the same period, and 0.35% of property and liability insurance revenues. This low level of coverage extends to only 0.2% of SMEs, against 9% of intermediate-sized businesses and 84% of large groups. Yet, SMEs are the most exposed to cyber risk; available indicators tend to show that 60% of SMEs go bankrupt within 18 months of a cyberattack.

The need for cyber insurance is there, but many factors are hindering its emergence.

First, cyberattacks seem difficult to predict and understand. They can effectively be undertaken in highly sophisticated ways and the modi operandi are constantly changing. Modelling credible risk scenarios is therefore a complex exercise.

Second, the cost of damage caused by a cyberattack can be considerable and often includes financial losses, loss of intellectual property, violation of personal data, reputational losses, and more. The financial quantification of risk scenarios is made all the more complicated by the multiplicity of parameters.

Third, regulations in terms of cybersecurity vary from one country to another, making it difficult to create standardised insurance products for international businesses. Insurers must also comply with regulations in terms of personal data protection, which makes them more vulnerable to legal proceedings in case of violation of privacy.

Finally, the cyber maturity of businesses requiring insurance depends on numerous factors, in particular their IT systems and their internal policies and procedures, as well as how the users of their systems behave. Assessing these criteria – no easy task in and of itself – can often be hampered by the natural reluctance of companies to share details of their IT infrastructure and security policies. Determining the level of risk exposure and the relevant risk premiums is therefore not just a standardised task.

Whilst the cyber insurance market struggles to find its model faced with (i) a risk that is not easily definable and whose impact is difficult to grasp, (ii) a base of insurance clients that is under construction and (iii) a changing regulatory environment, it is urgent to shed light on it through credible risk scenarios and sound financial quantification. That is the objective of Accuracy's work in partnership with Citalid: it aims to identify attack scenarios by specifying their frequency and the magnitude of losses incurred, in light of the vulnerability of the company under consideration, thanks to the analysis of the company's cyber maturity and the market in which it operates.

The objective and quantified information obtained from this work is intended to enable the company seeking insurance or wishing to evaluate the quality of its coverage to identify the most appropriate solution for its own configuration. Conversely, for the insurer, it contributes to the construction of relevant and long-lasting offers, as well as to the assessment of the insurability of clients.

Contact

Arthur Couvreur
Director
arthur.couvreur@accuracy.com
+33 6 66 69 65 15

Accuracy partners and professionals are available to discuss your needs and design an appropriate solution with the relevant experts.