OPINION

CYBER INSURANCE AND ITS INCREASING ROLE IN THE INDUSTRY

BY PHILIPPE COTELLE, FERMA BOARD MEMBER

Philippe Cotelle is the Head of Insurance and Risk Management of Airbus Defence & Space since 2014, gathering all Airbus activities in Space, Defence and Military Transport Aviation.
Since 2006, he was in charge of Insurance Risk Management for Astrium, gathering the Space activities of Airbus including the 3 business units EADS Astrium Satellites, EADS Astrium Space Transportation and EADS Astrium Services. Philippe Cotelle is graduated Engineer from Ecole Nationale Superieure de l'Aeronautique et de l'Espace and Executive MBA from Essec & Mannheim 2007.

Although insurance capacities are available, a gap remains between the supply and demand for cyber insurance. A joint effort of cyber insurance market participants is needed to develop the market.

As the Federation of European Risk Management Associations, FERMA represents nearly 5,000 European corporate risk and insurance managers in a wide range of business sectors. Most of them are playing a crucial role in determining if cyber insurance products are relevant for their organisations. Many such organisations in Europe have been offering cyber insurance for more than 10 years now and it is possible to draw some first conclusions regarding the advantages and drawbacks of such a process.

Europe's cyber insurance market is gradually catching up with its U.S. counterpart, pushed by recent cyberattacks causing not only high financial losses and attracting media attention, but also prompting to lay down new regulations with mandatory reporting for personal data breaches and cyber incidents affecting critical infrastructures. Although insurance capacities are available, there are some obstacles to the development of the market, and a gap remains between the demand and the supply side.

While businesses and organisations need to adjust their corporate governance to the new digital environment to fully understand the magnitude of cyber risks for their activities, the lack of actuarial data and the aggregation of risks pose a serious challenge to the insurance sector and its ability to price cyber risks and manage their exposures.

Key factors in a cyber insurance purchase decision

Risk managers are responsible for supporting their organisation's strategic objectives by mitigating the risk exposures created by digitalisation. Since digitalisation is now the growth engine of many organisations, company valuations originate mostly from intangible assets. Therefore, it has become necessary to identify, assess and analyse risks in this category of assets to define and implement an appropriate response with a risk management strategy.

The purchase of corporate insurance is only one of the possible outcomes of an internal, methodical process that draws upon the Enterprise Risk Management (ERM) principles of risk identification, analysis, evaluation and treatment. The organisation should be convinced that cyber insurance is the right solution and be able to justify and document it.

The organisation must resist the temptation to purchase cyber insurance to merely tick the boxes. Undoubtedly, management can draw some comfort from the fact they have insurance cover for cyber events, but more importantly, they need to understand what they purchased, why they did it and how the coverage will actually work if a cyber incident occurs.

The process starts with defining a cyber risk exposure. This is a pre-condition for allowing the organisation to clearly articulate its expectations to the insurer regarding the coverage it needs and to evaluate if the offer is attractive and adequate. To assess the 'true nature' of the cyber risk, the risk manager will take a broad approach, considering not only malicious events, malfunctions and errors but also everything else that may affect digital assets and lead to financial losses.

For a corporate risk manager, understanding the cyber risk exposure is a matter of rationality, credibility and cost effectiveness. An insurance broker can play a supportive role at this vital stage of the risk assessment. By knowing the residual cyber risk to be transferred to the insurance company and by benchmarking with others in terms of scenarios, impacts and remediation, the risk manager and broker can ensure that both the cover and premium for the chosen cyber insurance solution are appropriate and in line with the market practices.

The ultimate objective of a cyber risk management strategy is to maintain and increase the resilience of the organisation without seeking absolute security as that is impossible to achieve. The voluntary and well-recognised National Institute of Standards and Technology (NIST)[1] cybersecurity framework has established five basic functions of a cyber risk management strategy: identifying, protecting, detecting, responding and recovering. These core functions need to be performed, but exclusive reliance on the frameworks and standards is both unrealistic and dangerous as it can create a false sense of security. Compliance with standards like ISO 27000 alone is simply not enough. Such norms incorporate strong risk factors, but they are never exhaustive. Sooner or later, a hostile party will find a weakness that will jeopardise the organisation.

Finally, purchasing cyber insurance is a corporate decision that cannot be in the hands of the IT function only. It must also be clear that the accountability of the organisation's board and management to shareholders, customers and regulators cannot be transferred to the insurance sector.

The importance of cyber risk governance

In the context of cyber risk governance, increased organisational maturity is a pre-requisite for any decision about selecting and purchasing appropriate insurance products by an organisation. It is a process that needs to be embedded in the corporate risk management scheme. Similarly, the cyber insurance market will not be able to reach its maximum potential unless its customers adopt cyber risk governance principles.

[1] See https://www.nist.gov/framework

This is why in 2017, FERMA proposed a first cyber risk governance model that addresses the challenges of cyber risk identification and quantification within the organisation. The project rationale identified two areas where the challenges were most significant: a lack of focus on the risk governance aspect of cyber security and the need for top-down implementation of cybersecurity in the organisation, while it was recognised at the same time that companies must remain free to organise their risk management internally.

The model argues for the creation of a cross-disciplinary group to propose new ways to manage cyber risks internally. Such a group would build scenarios of critical exposures that are harmful to the company and credible from an IT point of view. Validated by both business and IT teams, the analysis of these scenarios would provide a basis for initiating a meaningful dialogue with the insurance sector.

Scenario planning exercises are very challenging. For example, the value of the loss of intellectual property for a pharmaceutical company at the early stages might be hard to quantify, since the revenues this asset could have generated in the future are unknown. Cyber risks are also rapidly evolving, which makes probability difficult to assess. Therefore, the quantification of the identified cyber risks, the measurement of the level of threat and the comparison of the maturity of the organisation's security with its peers require full cooperation between business units and the IT function.

Challenges for the cyber insurance market

SMEs

While large businesses might be in a better position to measure their cyber risk exposure due to more extensive resources they have, small and medium enterprises (SMEs) sometimes seem overwhelmed by the magnitude of the threats, not knowing exactly where to start. Although there is usually a reasonable level of risk awareness among SMEs, many of them are now seeking help to measure and manage their exposures. There is certainly a role here for government policy-makers to come up with public-private schemes that provide support for SMEs. Such programmes would facilitate the dialogue between insurers and SMEs and simplify access to cyber insurance for them.

SMEs are more vulnerable to a cyberattack than large enterprises as they often lag behind the latest cybersecurity developments. Standardised cyber insurance covers could have a positive impact on cyber risk prevention by proposing incentives to help SMEs strengthen their resilience to certain types of cyber incidents. Such products could provide an excellent opportunity to test an adopted cyber risk management process.

Data

The current inability of many SMEs to successfully manage their cyber risks contributes to a general lack of actuarial data on incidents, which is very problematic for insurers. Traditional risk modelling does not function well in the absence of historical data and geographical boundaries. Cyberattacks evolve rapidly as attackers are constantly learning. Estimates of loss without indications of probability make it difficult for insurers to assess the amount of capital that they need to allocate to support losses.

The way forward for the insurance sector is to invest in R&D and collaborate on cyber incident data collection so that underwriters gain the necessary knowledge to better understand cyber risks.

There is still much debate about the extent to which the reporting of cyber incidents should be mandatory, and methods to define/set the reporting parameters to avoid a sharp increase in the amount of data that would create a lot of noise and make relevant data difficult to identify. The issue of 'near miss' cyber events is also open although they are crucial to improving cybersecurity as they can reveal potential weaknesses and act as early warnings of an incoming cyber incident.

The active participation of business and organisations is necessary to build a useful data set. Several cyber incidents taxonomies exist, such as the CRO Forum[2],

[2] https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf

STIX[3] or CPS incident taxonomies[4]. They provide a standardised categorization of events by actors, means, causes, impact and victims. They also allow for a comprehensive analysis of any cyber incident and the ability to compare and share information.

Aggregation of cyber risks

The collection of cyber incident data is highly relevant for the (re)insurance industry to help it understand the aggregation of risks. Aggregation issues are well illustrated by the reliance of millions of businesses on cloud services. A report by Lloyd's of London released in January 2018 showed that an extreme cyber incident that would take down a top cloud provider in the United States for three to six days would result in economic losses of USD 15 billion on average and up to USD 3 billion in insured losses.[5]

There are also other scenarios that can lead to accumulations of risk. Organisations can be infected for years without even knowing it. These zero-day threats, where the vulnerability is known only to a handful of people and waiting to materialise, are a nightmare for every insurance community, especially the reinsurance sector.

Accumulation management is usually the cornerstone of the reinsurance business; if reinsurers do not understand the potential accumulation of risk, they will be reluctant to provide capacity. This area of cyber risk management is still in its infancy, and reinsurers struggle to comprehend what provisions are necessary for a major event with an aggregation of cyber risks.

The scenario of a state-sponsored cyberattack targeting the financial system would be incredibly complex to deal with. The reaction to this 'digital' catastrophe would be a lack of appetite from insurers, resulting in a contraction of the cyber insurance market.

For this reason, there is an ongoing debate about public backstop schemes for cyber catastrophes similar to terrorism pools.

Although considered a last resort solution, such programmes might help the market by removing the uncertainty linked to aggregation issues where millions of events occur at the same time. Others will argue that it is better to keep governments at bay until this category of risks is fully understood. The difficulty is, indeed, to determine when governments should intervene because the consequences of a cyber incident could be 'too big' for private capacity to support.

In its Supervisory Statement published in July 2017, the Bank of England expressed concerns about the ability of insurers' boards to control the accumulation of cyber risks. Insurers need to understand what they underwrite to allocate capital properly so that they do not put their shareholders' capital at risk.[6]

Types of cover

The Supervisory Statement from the Bank of England also indicates that the cyber insurance market does not currently have a good handle on the so-called non-affirmative or silent cyber risk covers. Silent covers are often the result of historical insurance products designed before cyber risks existed. These covers usually do not specifically exclude cyber risks, and if they do, the policy wording is often unclear about how cyber incidents will or will not be covered.

As a result, many 'traditional' property and casualty insurance products contain such silent covers. As 'digital' is part of all business processes today, such covers will be activated following cyber incidents with physical losses. If cyber insurance is an iceberg, silent covers constitute the hidden part below the surface.

Silent covers are, in fact, quite 'noisy' risks for insurers, and improved communication between insurers and policyholders is necessary to achieve wording that is clear

[3] https://stixproject.github.io/about/

[4] https://scholarsarchive.byu.edu/etd/4345/

[5] https://www.reuters.com/article/us-cyber-cloud-disruption/u-s-cloud-computing-failure-could-spur-up-to-19-billion-in-losses-lloyds-idUSKBN-1FC1UC
https://www.lloyds.com/news-and-risk-insight/press-releases/2018/01/failure-of-a-top-cloud-service-provider-could-cost-us-economy-$15-billion

[6] https://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss

and unambiguous. With explicit exclusions of cyber events from traditional policies, cyber insurance can take the form of affirmative covers, either as an extension to an existing policy or a comprehensive, standalone insurance. The latter can cover a broad range of consequences arising from a cyber incident, such as data restoration, cyber ransom, data breach notification costs, reputational damages, loss of profit with business interruption, financial losses with intellectual property theft, fraud and so on.

The corporate client perspective: clarity, comparability and certainty

It is currently difficult for a corporate risk manager to have a clear view of the relevance of the various cyber insurance offers. Common understanding of the critical components of a cyber insurance contract among cyber insurance market participants would increase risk managers' ability to analyse the existing insurance products and get a clearer picture of what the cyber insurance market is offering.

The underwriting information that the client needs to prepare for insurers to receive a cyber insurance offer should be clarified. Claims certainty is another area for improvement. There are currently not enough examples of successful large claims to demonstrate that cyber insurance is an efficient tool that brings tangible added value for business and organisations.

Very little evidence exists to address the issues of cyber insurance claim notification and claim settlement. Because of confidentiality constraints and the difficulty to prove a breach, those elements can generate significant hurdles for the development of cyber insurance. Allowing external experts to access the organisation's internal systems in order to settle a claim creates new risks and might represent a deal breaker for the most sensitive sectors.

Therefore, it is becoming crucial to determine the elements that will define the claim process before the inception of the cyber coverage, for example information to provide and the duration of the waiting period before compensation. Without increased claim certainty for clients, cyber insurance will continue to struggle to demonstrate its relevance.

In 2018, FERMA is going to partner with insurance brokers and insurers to create a document to improve cyber insurance market practices and streamline the exchange of information between the insurers and the insured by building an effective tool for all market players. ■