THE IMPACT OF CYBER RISK ON RISK MANAGEMENT

BY **CLEMENS FREY**

The market for cyber insurance is growing steadily, not least because of the Corona pandemic. Although insurers are currently underwriting cyber risks more restrictively, the German Association of Actuaries (DAV) believes that the economic importance of this line of business will continue to grow. For this reason, further work should be done to better understand these risks and to tailor management to their specific characteristics.

According to a representative enterprise survey in Germany, two-fifths of companies said they had been the target of a cyber-attack in the past twelve months. In Germany, there were already nearly 100,000 cases of cyber-crime in 2018, and global damages amounted to one trillion, or 1,000 billion US dollars, at the end of 2020, according to a study by McAfee, almost doubling since 2018. The need for cyber insurance is growing accordingly. Current estimates of the market for cyber policies indicate a global premium volume of more than seven billion US dollars for 2020. By 2025, it is expected to grow to more than 20 billion US dollars, with annual growth rates of more than 20 percent.

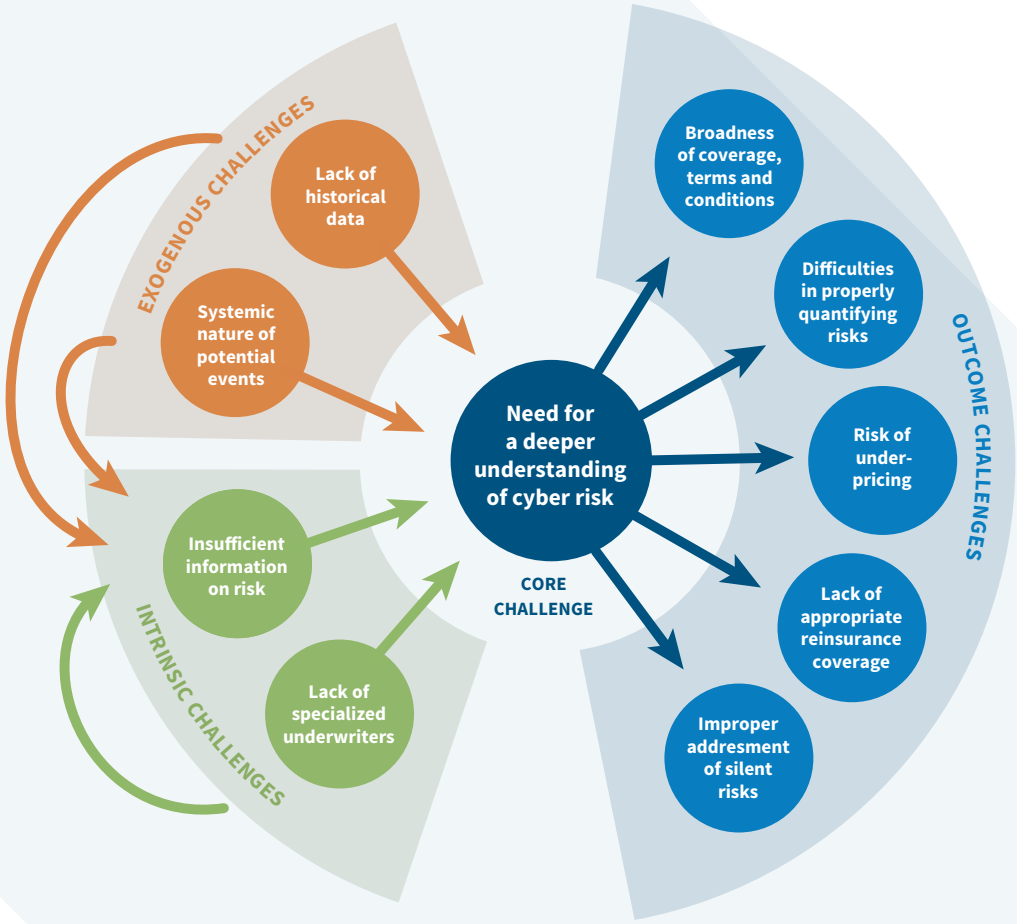
CYBER INSURANCE RISKS

Managing a cyber insurance portfolio poses several special challenges. Cyber risks tend to be different from other, classic insurance lines. They arise from three sources: from the insurance company's own business activities, from specially developed cyber policies and from classic insurance products where losses are also caused by cyber events – so-called silent cyber.

Cyber risks themselves are subject to strong dynamics in terms of the product landscape, the legal situation, and the risk situation. It can be assumed that the first two will continue to consolidate over time, but the risk situation will remain dynamic due to constantly new attack and defence mechanisms.

Furthermore, cyber risks have a high accumulation potential: a single cyber event can cause an enormous number of individual losses and hit insurers on both sides of the balance sheet. This potentially leads to a large overall loss that is not geographically limited - unlike storms or earthquakes. >

FIGURE1: CHALLENGES OF CYBER RISKS (ACCORDING TO EIOPA, 2018)



Finally, insurers face the challenge of measuring cyber risks with appropriate mathematical models, pricing cyber products appropriately and managing the overall risk situation. There are several challenges at all points in this process - most notably the issue of insufficient data. The European Insurance and Occupational Pensions Authority (EIOPA) has already summarised the relevant challenges in 2018 (*see Figure 1*).

DYNAMICS AND ACCUMULATION RISK

How can insurance companies deal with the special challenges of cyber risks? In order to be able to react to the dynamics of cyber risks and new risk scenarios, an active management of covers and exclusions is necessary. This should be based on current loss scenarios as well as industry benchmarks.

At the same time, constant monitoring of the risk situation in terms of the 'gap' between the threat situation and the available defence measures is necessary. Technological expertise, such as IT/cyber expertise, is also increasingly anchored in risk management, similarly to legal expertise. Only experts can provide an immediate assessment of impacts as well as suggest measures, for example in product design. Accumulation management for cyber risks requires detailed and flexible analysis options of the existing cyber exposure. As part of the analyses, comprehensive extreme scenarios should be considered that test the impact of cyber events on the entire balance sheet.

Frequently, assistance is part of cyber policies, providing post-claim support and reducing the overall financial loss. In the case of accumulation, however, the loss-reducing might fade due to the mass of claims. This effect should be considered in risk measurement. Finally, insurers themselves might be seen as primary targets due to their data treasures, so they should protect their own operations against cyber damage accordingly. >

DATA AND MODELLING

The basis for cyber risk management measures are comprehensive, up-to-date, and detailed information - both about past claims and about current and potential future threats. The required data should be collected in a structured manner and made available for prompt and flexible analyses.

Data citizenship – i.e. broad access to available data – is particularly important in the context of cyber risks due to the large number of experts involved. As there is often a lack of reliable data on cyber risks, insurance companies will continue to rely on external data pools.

Insurers often use mathematical models developed by external third parties to measure risk; however, due to the large number of model variants used, it is essential for insurers to also develop their own understanding of the specific risk scenarios and modelling approaches.

MANAGEMENT OF CYBER RISKS

Due to the dynamic nature of cyber risks, it should be possible to make portfolio-wide adjustments to cyber policies at short notice. Therefore, shortening coverage periods could be conceivable as well as adjusting coverage or price during the year.

In the context of risk management, the fit of the primary product side and reinsurance coverage is of particular importance. Especially regarding silent cyber, it should be ensured that any exclusions in reinsurance contracts match the original risk to avoid unexpected coverage gaps.

CONCLUSION: CYBER REMAINS A MAJOR CHALLENGE

IT and cyber are increasingly perceived as risks by the general public. The overall economic demand for cyber insurance will continue to rise, so insurance companies have to manage special challenges. To this end, all elements of the value chain must be included, from product design to risk management and claims settlement. In addition, it is necessary to think beyond the boundaries of lines of business, functions, and areas of expertise. In this context,

the integration of technological know-how is just as important as monitoring developments in cyber-specific liability law. At the same time, the collection and use of data must be intensified, for example by capturing cyber claims and silent cyber data. Overall, insurers are about to improve their data situation and risk management, since for cyber, a flexible and timely reaction to emerging risk scenarios is essential. <

DR. CLEMENS FREY, ACTUARY DAV, CERA, is Partner at EY in Munich and Head of Data, Analytics and Artificial Intelligence in Germany. He is member of the General Insurance and the International Committees of DAV and leads the DAV Working Party on Cyber Insurance.