OPINION

Joachim Wenning
Chair of the board of management, Munich Re, Germany

CYBER RISKS

Under attack

The cyber threat to economies and societies is growing. Systemic risks and accumulation scenarios require sustainable, innovative insurance solutions.

Cyber criminals operate in highly professional, agile and networked ecosystems. The global economic damage can only be estimated, but we have seen a clear rise over recent years. The Munich Re Cyber Risk and Insurance Survey 2022, which surveyed over 7 000 executives and employees from various industries in 14 countries, underlines this development, revealing that, year-on-year, online fraud increased by 22% globally, while ransomware attacks and data theft increased by 33% and 34% respectively.

While prominent incidents create major headlines, the vast majority of successful cyber attacks usually remain uncommented on by the media, yet they cause severe challenges for the affected companies and organisations. Therefore, it is no surprise that the Munich Re Survey showed an increased awareness of this topic amongst global decision-makers. Nevertheless, only 17% of global heads reported that their company is already adequately defending itself against cyber threats. The findings show the importance of further increased resilience and preparedness in general.

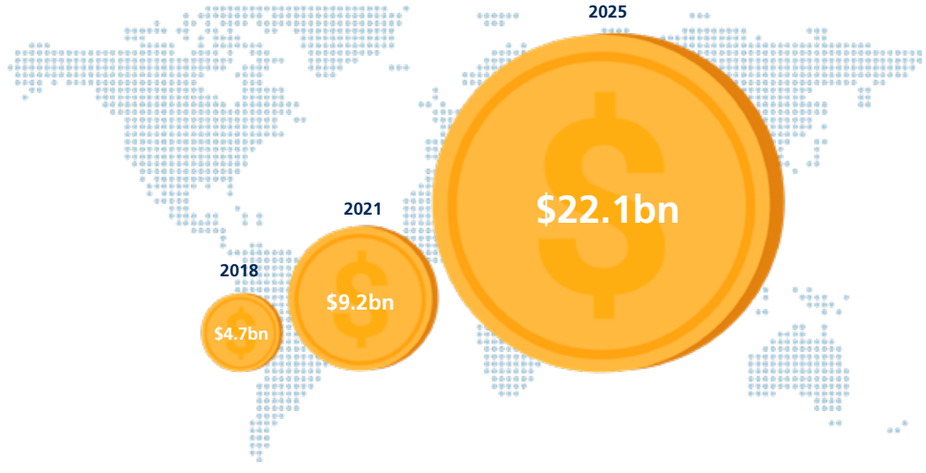
Major threat vectors

In light of the statistics mentioned above, it is crucial to have a thorough understanding of the threat landscape and an organisation's own vulnerabilities. For only then is it possible to protect oneself in a targeted manner by means of adequate prevention. Munich Re experts assume the risk situation will

Which of the following have you been affected by?

Source: Munich Re Cyber Risk and Insurance Survey 2022

Strong growth expected in the global cyber insurance market



Munich Re estimates, 2022

remain extremely dynamic, with rising vulnerabilities and attacks that are not always immediately and fully visible to the victim. We expect that the cyber-threat situation in 2022 and beyond will be mainly characterised by three factors:

- **Ransomware**
  Munich Re anticipates a continuously high number of ransomware attacks conducted by attackers relying on proven methods and on expanding their own tactics and procedures with so-called multiple blackmail schemes. In addition, by passing on their tools and expertise, criminal groups enable the participation of other perpetrators (affiliates), who can carry out ransomware attacks without much know-how of their own. For example, ransomware programs can be rented on the darknet for $40 (€38) per month.Besides an increase in frequency, we also expect more severe impacts due to successful ransomware attacks. This might be especially true when operational technology or critical infrastructure is affected.
- **Supply-chain attacks**
  Criminals are increasingly achieving particular reach-through attacks on or via the supply chains of companies. ENISA, the European Union Agency for Cybersecurity, also confirmed this attack pattern. According to its 2021 report, "Threat landscape for supply chain attacks", there was already a fourfold increase in 2021 in supply-chain attacks compared to the previous year. From an insurer's perspective, a single attack can cause damage to a large number of policyholders. Particularly-critical digital dependencies, such as the use of cloud providers, are therefore included in Munich Re's accumulation scenarios.
- **Attacks on critical infrastructure**
  Digital attacks on energy suppliers, food suppliers, hospitals, administrations and other areas of critical infrastructure reached a new peak in 2021. Given the war in Ukraine, we do not expect this development to slow down this year either. Attackers' motivation for targeting critical infrastructure is not limited to ransom demands. They also aim for destruction of processes and systems in order to trigger economic and political instability. To this end, some criminals also cooperate with state actors.

"Only 17% of global heads reported that their company is already adequately defending itself against cyber threats."

Growing demand for cyber insurance

The heightened awareness, as well as the politically and societally stronger focus on the topic of cyber security are a positive signal. It will lead to further demand for cyber insurance, which could continue to grow even faster than market capacity. We expect further demand from all industry segments and company sizes. In particular, loss-exposed sectors such as healthcare, professional services, retail, manufacturing, financial institutions, governmental institutions — including the education sector — and financial service providers are seeking more cyber-risk coverage.

Munich Re estimates annual global cyber premiums at more than $9bn (€8.25bn) as of the first quarter of 2022 and expects the global cyber insurance market to reach a value of approximately $22bn by 2025.

For the insurance industry, it is of the utmost importance to continuously improve its cyber offerings. These are committed to guaranteeing the performance of the insured, while digital dependencies are rising rapidly. The industry must ensure a balance that allows insurers to offer attractive solutions on the one hand and to achieve the necessary sustainability in the volatile cyber business on the other.

Sustainable insurance — one pillar in risk management

Cyber insurance business can only be written sustainably and reliably for insureds if key conditions are met. Transparency about the risks is an essential element of adequate risk management by companies and organisations. With the spread and use of new technologies and increasing digital dependencies, threat scenarios will also continue to evolve. As a consequence, the distinct definition of insurability of risks is crucial to a sustainable cyber insurance market.

There are systemic risks that exceed the limits of insurability; risk transfer to insurance carriers is therefore not possible. Such non-insurable risks, like the outage of telecommunication infrastructure or acts of war, must therefore be clearly and transparently excluded from cyber coverage. Other systemic risks, however, are considered to be insurable, including widespread viruses, multi-client data breaches or cloud outage scenarios.

As a market leader Munich Re continues to offer capacity in the cyber insurance market with expertise, a clearly defined risk appetite and strict risk management. For the client this means, for example, that implementing adequate cyber-security controls is a prerequisite for gaining access to the cyber insurance market.

Our experts continuously refine internal models based on our own and third-party data with a specific focus on risk accumulation. Together with our customers and partners, we are constantly improving our cyber offering and our data-driven and innovative solutions, thus strengthening the sustainability of the cyber insurance market along with the resilience of insureds.