OPINION: CYBER INSURANCE

Insurance: a cornerstone of cyber risk management

Adapting to risks in a rapidly changing digital landscape

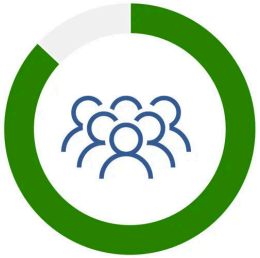
Joachim Wenning

Chair of the Board of Management, Munich Re

The dynamic adaptation of advanced technologies, new digital services and applications is an integral part of our digitalised world. Cybercriminals and other threat actors are taking advantage of the increasing interdependencies and interconnectedness that are being created. In this context, cyber insurance has become an established part of risk management, but it requires a greater contribution from all stakeholders in society.

The digital world presents both opportunities and risks

Digitalisation is fundamentally changing the economy and society, as evidenced by the global adoption of generative AI technology. It is driving innovation, productivity, and economic growth, and also has an impact on political participation. According to global decision-makers participating in the Munich Re Cyber Risk and Insurance Survey 2024, the most relevant technologies in the next two years will be artificial intelligence and cloud computing. Yet while everyone is embracing digitalisation and its rapid adaptation, there is also growing concern about increasing risks: 38% of the global decision-makers surveyed are ‘concerned’ and 34% are even ‘extremely concerned’ about a potential cyberattack. In light of this, it is more than surprising that the company leaders surveyed are not confident that their companies are adequately defending themselves against such attacks.



87%

of all C-Level respondents report that their company is not adequately protected against cyber-attacks.

Source: Munich Re

Cyber risks and loss drivers

Ransomware, business email compromise (BEC) and data breaches will remain the main loss drivers for risk owners and cyber insurers. According to Munich Re's experts, these key loss drivers will also be affected by the dual use of artificial intelligence, the criticality and vulnerability of supply chains, and the tense geopolitical situation that is shaped by wars and deepening conflicts.

The table below shows the cyber threat landscape in 2024 and its impact on cyber insurance.

Impact on cyber insurance

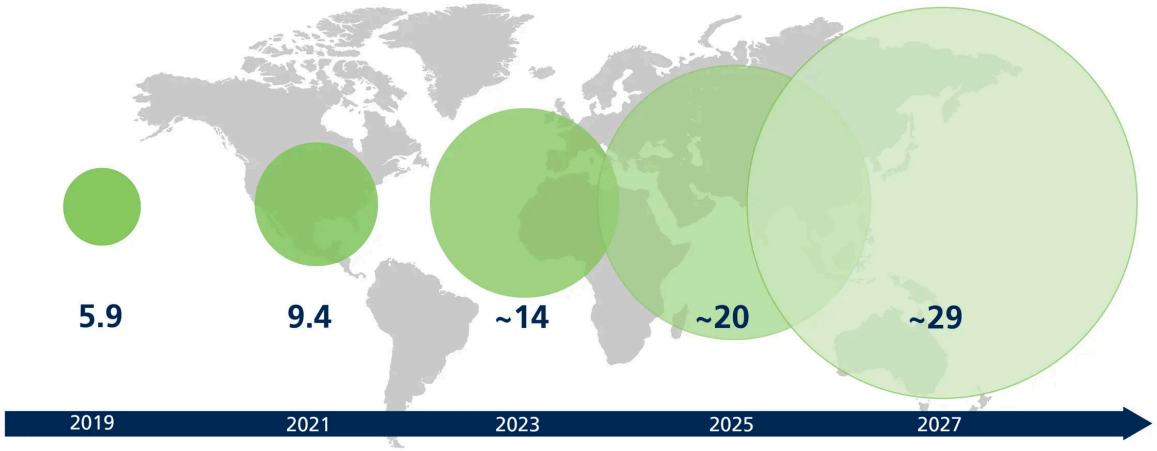
Notes:
Network and information systems 2 (NIS2)
Digital Operational Resilience Act (DORA)

Source: Munich Re

Cyber insurance market trends

Munich Re estimates that the global cyber insurance market has reached USD 14bn in 2023 and will increase to around USD 29bn by 2027. In addition to digital transformation and increasing technological interdependencies, significant growth potential will be driven in particular by increased reporting requirements and regulations that go beyond data protection laws, as well as growing liability for decision-makers. In addition, damaging and costly cyberattacks – especially against industry peers or even their own company – will raise awareness further. Finally, cybersecurity requirements will not only be set by legislation but also result from the needs of supply chains, business partners or end customers.

Cyber insurance market: gross written premium (GWP) expectations 2019-2027



Source: Munich Re

Despite these opportunities and the positive outlook for the cyber insurance market, insurers will also face challenges. One of these is certainly improving the relatively low penetration rate. The gap between economic losses and insured losses is still too wide, given the highly dynamic threat landscape. Risk transfer with adequate coverage and service remains a key pillar to protect digital assets and to increase the resilience of the economy and society. At the same time, the offerings on which risk owners rely have to be sustainable. The natural limits of the insurance industry's risk-bearing capacity must therefore be clearly recognised. Indeed, catastrophic systemic events such as cyber war or the failure of critical infrastructure cannot be modelled and have the potential to exceed the capacity of cyber insurers, or indeed of the insurance sector as a whole.

As such scenarios pose a threat to political, societal and macroeconomic stability, the involvement of governments in managing these potentially catastrophic cyber risks is necessary in order to rapidly build efficient and proactive economic protection, including against catastrophic cyber events. Munich Re is a strong advocate for effective public-private partnerships as a precautionary measure of last resort. Promising dialogues on "government backstops" for catastrophic events have already begun. With accumulation modelling and risk quantification among its core competencies, Munich Re will help provide governments with the relevant knowledge. In addition to adequate in-house expertise, such multi-stakeholder cooperation will also be necessary to exploit the opportunities offered by technology and digitalisation and to limit the associated risks.