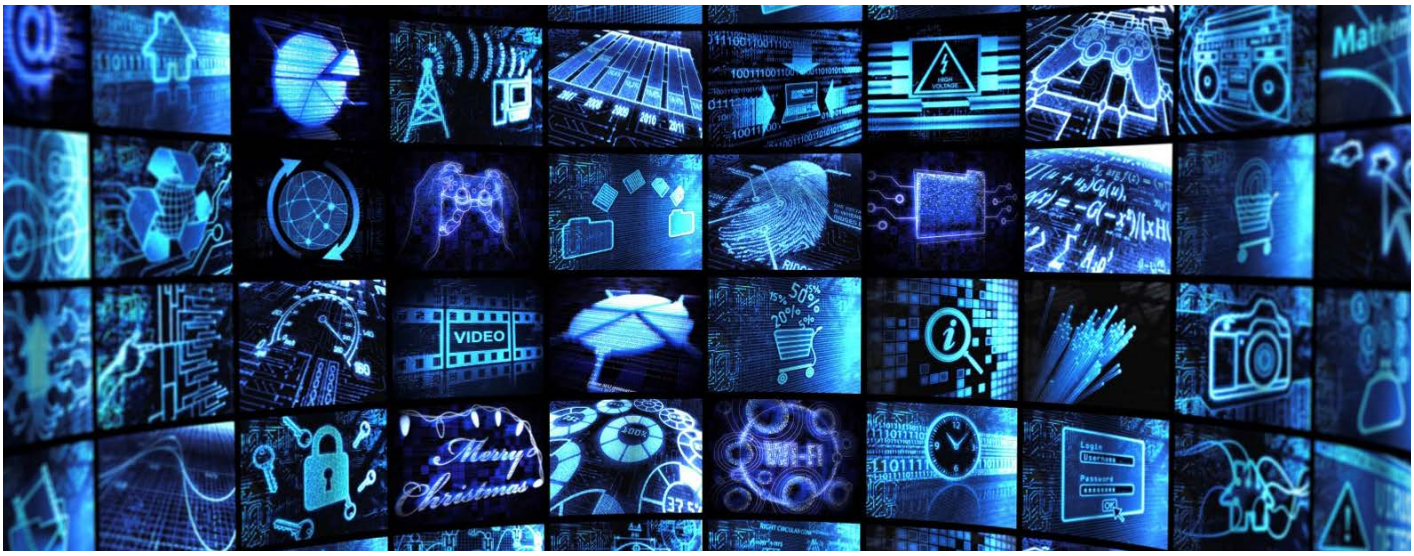
Deloitte.



Cyber insurance: What you need to know, and how to seize the opportunities

The development of connected technologies, or cyberspace, is leading to business opportunities as well as increasing risk. This provides space to develop new and improve existing insurance, leading to premium products. To seize these opportunities to their full potential, non-conventional approach is needed. While insurance business is traditionally built on providing stability by being stable, market needs require insurers to provide stability by being flexible. The reason for this is simple. Due to (exponential) cyber developments, changes in risks as well as markets will happen ever more quickly, so in the not too distant future, only the insurers who know how to service their customers with these changes will remain. Understanding cyber risk and its fundamental role for the future of insurance is a good start.

> "Insurers must either get involved in cyber insurance or see their business fail in the years ahead"
>
> **Maarten van Wieren, Cyber Risk Quantification Leader, Deloitte**

What is cyber risk?

The increasingly rapid entry into cyberspace has already led to a significant increase in operational risks and the risk of cyberattacks. Cybercrime has increasingly become a society-wide issue that is receiving a lot of attention from governments across the globe. Projects around data protection and the funding of research into cyber insurance illustrate the challenges around cyber risk and also their importance. Further technological innovations, such as the internet of things, artificial intelligence, health-tech, robotics and 3d-printing, for example, will further increase cyber risks and lead to the emergence of new and unforeseen risks. And with changing risks comes the need for better insurance.

What is cyber insurance?

Cyber insurance as a product has been around for 17 years but has certainly not yet matured. It has seen strong growth over the last years, with healthy margins seen in the US, for example. And with the persistent threats and incidents in the field of cybercrime, it is likely that cyber insurance will continue to keep growing globally.

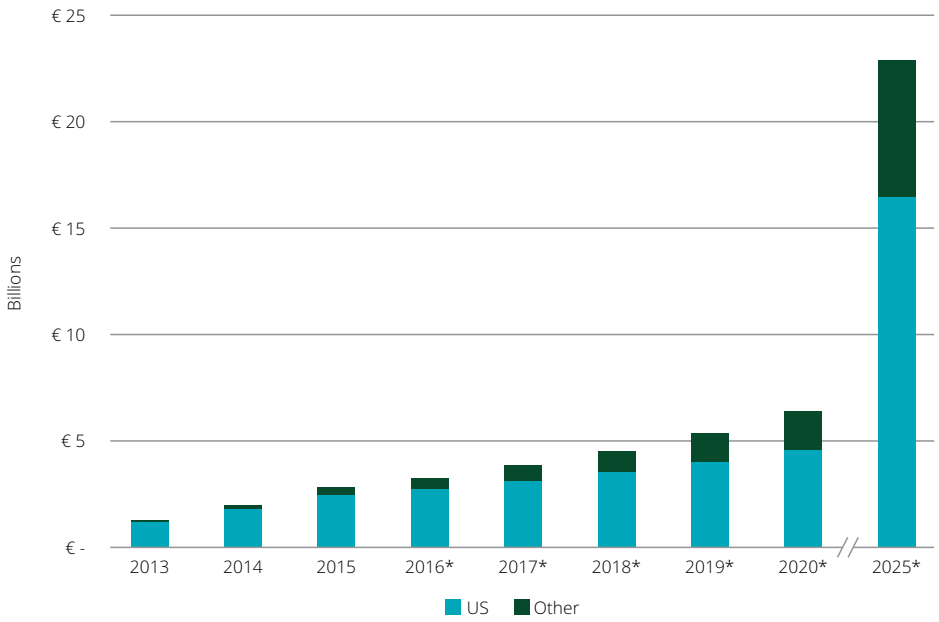
Also, traditional insurance products will increasingly involve a cyber component. Most obvious are the insurance against payments fraud or corporate liability insurance, while for some other products, like car insurance or health insurance, the impact is less obvious (think of car-jacking by wire, for example, or the required mass replacement of cyber-vulnerable implants).

The risks of not getting involved in cyber insurance

The insurance industry has met some significant challenges in the last decade. Partly due to changing regulations and competition but also because the risk landscape and risk appetites are always changing. We see cyber as the pinnacle of such change, because it fundamentally changes business models, while the accompanying risks are hard to measure and control. From the perspective of the insured, this has led to expensive products with many limitations. From the perspective of the insurers, it is vital to truly understand the holistic effects of these changes and the associated cyber risks because historic risk trends can be completely disrupted if unforeseen cyber vulnerabilities lead to mass claims for example. By building on old business models, insurers are investing in an industry of the past.

Opportunities in cyber insurance

Markets will increasingly be confronted with these emerging cyber risks. So, insurers who learn to provide their customers with ease of mind by balancing expert services on risk mitigation with limiting impact through fast incident response and solid after-care, will likely make the difference. Such services-oriented insurance need a high degree of flexibility to be effective and efficient and it takes time to develop such capabilities. In the long term, insurers who manage this well will have a significant advantage, also on traditional products, as these will increasingly contain exposure to the new types of risk.



Source: Munich Re, (*) concerns Allianz predictions.

How to seize the opportunities?

Strategic changes are needed to transform from the highly competitive P&C market to a premium market with innovative services that flexibly meet customers future needs. Insurers need to make the right choices and execute them well. They need to choose where they want to play and how they want to win.

Those who can develop the capabilities to safely develop a cyber-insurance portfolio will be also able to conquer the market, stay ahead with providing flexible risk services while making a sustainable profit. Just as the cyber risks themselves, these new products should be easy to export across different countries, providing a great international market and potential clientele.

To develop a healthy cyber insurance portfolio, a couple of elements are required. Of course, standard elements such as expertise, access to markets and data are required. In addition, since cyber insurance touches on all the main insurance risk types, out-of-the box thinking is needed for successful development of sustainable and flexible insurance services. The table below summarizes some innovative ways to meet the challenges that come with each insurance risk type, providing a sketch of the future of insurance.

Insurance risk type	Challenges facing cyber insurance	Innovative thinking that helps meet those challenges
Parameter risk	Data for calibration is hard to obtain, while risk trends are changing quickly.	A deep understanding of the risk structure and tracking of distinguishing characteristics will need to be developed. Need for more data or combination of automated data harvesting with powerful analytics.
Selection risk	Cyber risk is complex and opaque, so it's hard to identify bad apples.	Provision of cyber security services will shift focus from claims to prevention (through incentives). Insurance firms may look more like security firms.
Fraud risk	Identifying, and proving the nature and cause of a cyber incident, can be hard.	Security and forensics, with embedded blockchain technology will ensure finding and integrity of traces. Insurers should embrace such technology for own use and for serving their customers.
Pricing risk	Unsophisticated market entrants looking to buy market share may undercut rational prices.	Sharing cyber models and empowering the regulator will help weed out the unsophisticated competitors. Competition will remain when it comes to detail of data collection, models to interact with the data, and access to markets.
Concentration risk	Single events may impact a large part of an insurance portfolio.	Collaboration and information sharing is required between insurers and reinsurers to aid prevention.
Insufficient capital	Tail risk is hard to quantify and there is only limited capital available with a very high risk appetite.	Financial innovations that enable diversification with other types of (tail) risks could make a big difference.
Coverage misalignment	Reputational risk and trade secret risk are widely considered uninsurable so it's difficult to provide coverage in line with client needs.	Loss of market share can be insured by shifting the focus from compensation to enabling recovery. Pre-determined, fixed pay-outs for well-defined cyber events may enable strategic development of new market share.

Deloitte believes that companies who are willing to take a leap and truly innovate their business will reap the benefits associated with leading in cyber risk. This requires letting go of the more traditional perspective and venture into the relatively unknown "blue ocean" of cyberspace. In time, this blue ocean will further develop into the foundation of our digital society and it will pay to learn how to navigate it.

More information?
Please contact Maarten van Wieren
Tel: +31 (0)6 8201 9225
mvanwieren@deloitte.nl