Cyber insurance

Exploration of the Dutch insurance market

27 February 2023

AFM

Society is getting ever more digitalised. We order our groceries online, we hold meetings via video conferencing and our homes are full of smart (IoT) devices. Our data are stored in the cloud instead of in filing cabinets, and companies offering platform services are among the most valuable companies worldwide.

This development creates new cyber risks. Companies are entirely reliant on the proper functioning of their internal and/or external IT infrastructure. If that fails, it brings the whole company to a standstill. There is also a big risk of theft of our personal data, which can have major consequences such as credit card fraud or identity theft. In addition, wars and terrorism now also take place online, as does theft of company data.

These new risks are dynamic, complex and increasing. There has been a huge increase in the number of ransomware attacks in recent years.[1] Hardware security vulnerabilities such as Meltdown and Spectre create new risks for consumers and companies.[2] It is hard to predict what cyber risks we will face in five years' time. From the discussions the AFM has had with insurers, it is evident that consumers and companies are still insufficiently aware of these risks.

There are insurance products on the market to mitigate the cyber risk. These cyber insurance policies cover risks around liability and damage and losses incurred by the company and its customers. They often also provide services when a cyber incident occurs. In this way, consumers and SMEs can cover their risks.

In recent months, the AFM conducted an exploratory study into the market for cyber insurance. We conducted this study because cyber risk is a relatively new type of risk and because the number of cyber attacks has increased significantly in recent years, particularly during the coronavirus pandemic, exposing consumers and companies to bigger risks. As the AFM considers it important to promptly identify potential risks, we have conducted an exploratory study into this insurance product. Based on the outcomes of this exploratory study, the AFM will be able to ask for more attention to this cross-border issue internationally. In addition, cyber risk is a cross-border risk in an international playing field of market parties to which the AFM pays particular attention.

The market for cyber risk insurance policies for companies (including SMEs) and consumers is still small, but it is expected to grow.[3] The size of the cyber risk insurance market was €36 million in 2021, compared with €850 for the liability insurance market. Only a few Dutch insurers offer cyber risk insurance products for businesses. A larger number of native Dutch insurers offer products for the consumer market.

The AFM has found that it is still difficult to compare cyber insurance policies, due to three reasons. These are the complexity of the policy conditions, different interpretations of key terms and the fact that insurers do not make it fully explicit exactly what is covered.

1. **The cyber risk and policy conditions are dynamic and complex.** As cyber risk is mainly an IT risk, understanding cyber insurance policies requires a certain knowledge of IT. This makes it more difficult to interpret policy conditions and requires that advisers acquire new/additional knowledge to be able to make a proper risk assessment. Given that cyber risk is constantly subject to change, the policy conditions are also constantly changing. Therefore, it is important that changes are clearly communicated to customers, that the PARP guidelines are taken into account in product development and that the policy conditions are formulated as transparently as possible. This will make it possible for customers and advisers to continuously assess whether the insurance product still fits in with the customer's personal situation and to keep putting the customer's interests first.

[1] Ransomware Attacks Hit Two Out Of Three Organizations In 2021: Here's What You Need To Know (forbes.com)
[2] Meltdown and Spectre (meltdownattack.com)
[3] *Cyberverzekeringsmarkt in 2021 gegroeid naar 36 miljoen euro* (Cyber insurance market grew to 36 million euros in 2021) (verzekeraars.nl)

2. **Different interpretations of key terms make it difficult to compare cover.** There can be big differences between the type of cover provided by insurance policies for consequential losses after a cyber incident, as different insurers apply different definitions of the term 'cyber incident'. This can range from policies that cover human errors, programming errors and hacks to policies that only provide cover for malicious attacks. Insurers also apply different definitions of other terms, such as 'infrastructure' and 'computer network', that have a big impact on the cover provided to customers. Applying the same definitions of these terms – in the interest of the customer – will make these products more easily understandable and easier to compare.

3. **Lastly, the AFM has found that insurers have not made all their policy conditions explicit.** An example of this is the exclusion of cover for damage and losses incurred due to war. This is no longer a hypothetical risk since Russia's invasion of Ukraine.[4] It is difficult to establish whether a cyber incident was an act of war, and many insurers rely on external experts or government authorities for this. The AFM has found that not all policy conditions make clear on which sources the insurer bases itself to establish whether a cyber incident qualifies as an act of war. At present, when a cyber incident occurs, it is not clear in advance whether it is in scope of the insurance cover, which creates uncertainty for the insured party. Ensuring that the information on insurance cover in policy conditions is a transparent as possible – and comparable – will make it easier to understand these products.

It is important that insurers continuously assess how they can communicate as transparently as possible about what is covered by their cyber insurance and that the sector jointly considers at this time how it can contribute to better comparability of cyber insurance products, given the growth of this market. The international nature of this market presents an additional challenge in this respect. Given the complexity and changeability of the structure of these products and of the cyber risk, it is all the more important with these products that the information provided to customers continuously contributes to their understanding of the product. Ensuring better comparability of the cover and functioning of these products can be conducive to this. This will enable customers and advisers to ensure that the right risks are covered today and in the future and to avoid disappointments that could have been foreseen.

[4] New "Prestige" ransomware impacts organizations in Ukraine and Poland – Microsoft Security Blog

The Dutch Authority for the Financial Markets
PO Box 11723 | 1001 GS Amsterdam

Telephone
+31 (0)20 797 2000

www.afm.nl

Data classification
AFM - Publiek

Follow us: →

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.