Six Questions on Cybersecurity to…

Nynke Brouwer

After 11 years, Nynke made the switch from Dirkzwager Legal & Tax to Stibbe, where she focuses on data protection, cybersecurity and cyber insurance. In the past few years she has investigated the functioning of cyber insurance on the Dutch market and published a book on the subject. We spoke with her about her book.

Question 1) You have done at least four years of research to write this book. What was the starting point for your research and thus for writing this book?

I started focusing on liability and insurance aspects of cyber risks quite early in my career. It quickly appeared to me that there was a great need for more knowledge about cyber risks in practice. I found the insurance aspects particularly interesting, because of the importance and urgency of properly insuring this risk and its complexity. When I started my research, legal literature on cyber insurance in the Netherlands was scarce. I figured a better understanding of cyber insurance within a legal context could contribute to its further (legal) development, so that is where I started my research at Radboud University Nijmegen.

Question 2) What is the main audience you want to address with your book?

My research is obviously aimed at the research field of law, but I think my book will also be valuable for insurers, insurance brokers and intermediaries, risk managers and directors of companies and organizations.

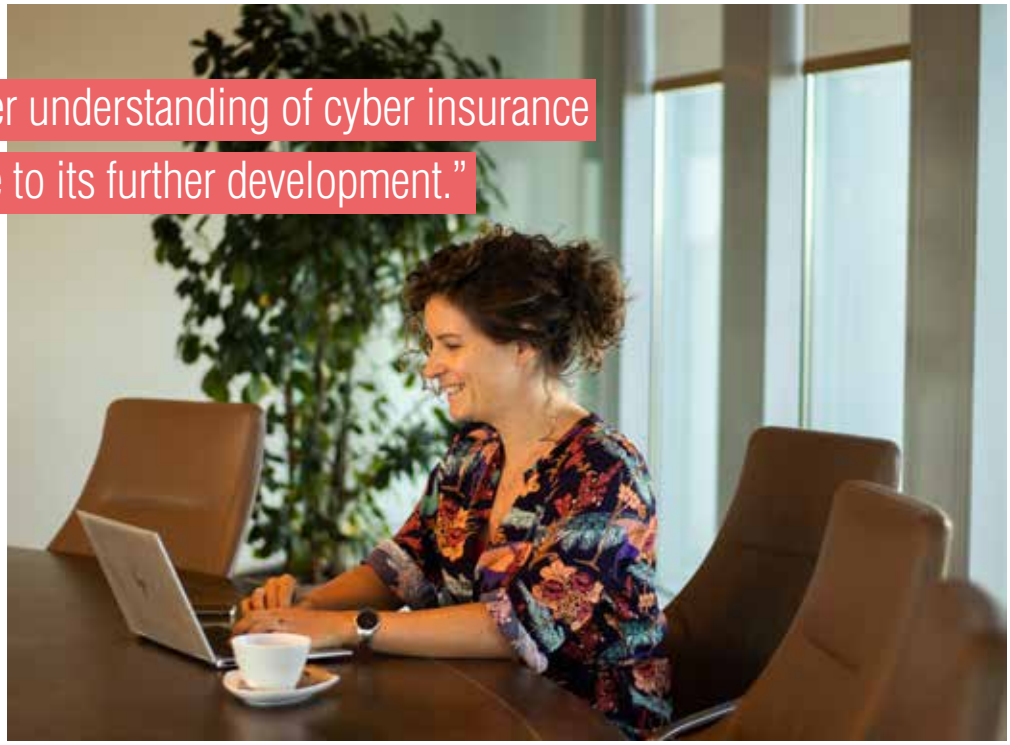
Question 3) What obstacles have you encountered during your research when it comes to cyber insurance?

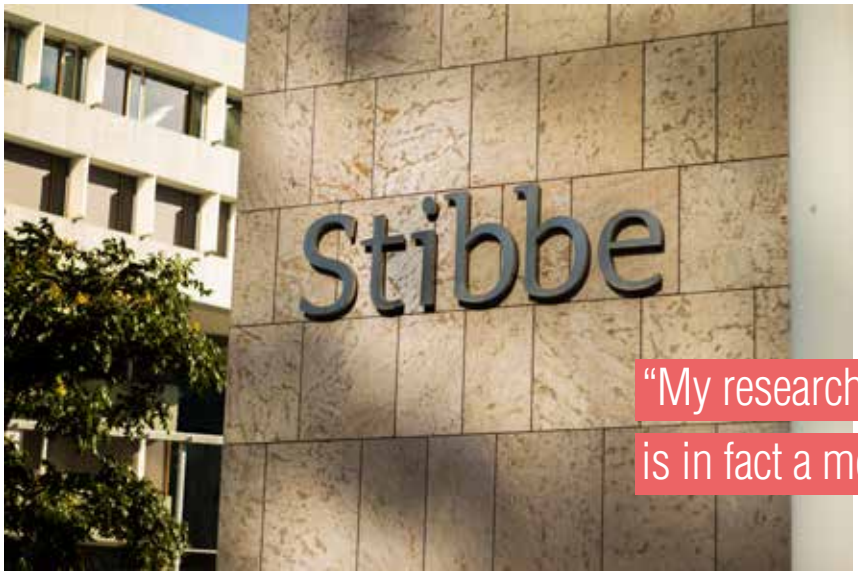
My research object, cyber insurance, is in fact a moving target. Both the technology and this insurance product develop very quickly, so that requires constant alertness. On the one hand, this was pleasant: I was able to respond to very current developments and was therefore on top of things. On the other hand, it required both strict delineation and, paradoxically, a high degree of flexibility.

Question 4) The book suggests that there are many uncertainties about the interpretation of cyber risk and cyber insurance. What uncertainties are you referring to and why are there so many uncertainties?

These are particularly uncertainties about the meaning of terms and concepts in the policy wordings. Ultimately, those terms determine the extent of the coverage. If it is not clear what exactly is stated, both the insured and the insurer can face unpleasant surprises when a loss occurs. A concrete example of such a lack of clarity is the central concept of 'cyber incident'. There is no clear definition for this concept in common parlance. The same applies to terms such as phishing, malware, privacy incident, etc. The definition in the policy is therefore very important. However, the policy wordings are often multi-interpretable, which causes uncertainty.

"I figured a better understanding of cyber insurance could contribute to its further development."





"My research object, cyber insurance, is in fact a moving target."

Question 5) What do you personally see as the biggest cyber risk and do you have any tips for what people should definitely insure?

Ransomware still remains a major risk. Ransomware does not only lead to business interruption, but in most cases, it is also a direct violation of data protection law, i.e. privacy. These incidents require a rapid, multidisciplinary response. Cyber insurance provides coverage for incident response services by experts from different disciplines. These services can mitigate the loss and damage enormously and therefore are of great benefit.

Question 6) At the end of the book, you provide an overview of cyber insurance coverage. Without giving too much away, what is the message you want to convey to your audience?

In my view, insuring cyber risks is an important tool to compensate companies for damages, but also to make society in a broader sense a little safer. It is therefore important that cyber risks remain insurable. That also requires something from companies themselves, namely that they invest sufficiently in technical and organizational security measures. Taking out insurance is a final element in risk management. By combining knowledge, insurers can also give direction in this respect. I also think it is important that a dialogue takes place about the limits of insurability and whether there isn't a role for the government as an ultimate safety net. A number of such discussions are already taking place. I hope that my book has contributed to this.

About the author

Nynke Brouwer is a lawyer and expert in cybersecurity and data protection at Stibbe. She has specific knowledge in the field of cyber insurance. She regularly provides incident response services after cyber incidents, such as ransomware attacks. Nynke has written numerous research papers and case commentaries and in 2021, she was awarded the title of Legal Woman of the Year.