Book Review - *Cyber Risks Insurance: Law and Practice*[*]

Dr Franziska Arnold-Dwyer[**]

Cyber risks insurance is concerned with any risk of financial loss, physical damage, business interruption, private data breach losses, crimes losses and reputational damage arising from a failure of information technology systems. These risks can be endogenous (risk exists or is created inside the business) and exogenous (risk created by an external actor). Insurance coverage of cyber risks is relatively new and still evolving. Some of the challenges faced by the insurance industry in relation to cyber risks are the constantly evolving technologies, the multitude of potential causes for cyber losses and the scarcity of loss data, all of which make modelling and pricing difficult.

Celso de Azevedo's book *Cyber Risk Insurance: Law and Practice* takes on the difficult task of taking stock of the legal and practical issues in relation to cyber insurance under English law and from a London Market perspective, although there are some interesting comparisons to developments in the US. The book is structured as follows: Chapter 1 and 11 provide a market overview of the cyber insurance and reinsurance market, explain what type of risks are captured and how cyber risks are underwritten. Chapters 2 and 3 trace the evolution of silent (non-affirmative) cyber cover in traditional property insurance wordings, via cyber risk exclusions, to stand-alone (affirmative) cyber cover. Chapters 4, 5 and 6 deal with stand-alone cyber risk insurance (i.e. a policy specifically dedicated to cyber risks cover) covering first party cyber risks in respect of costs and expenses, data breaches and business interruption coverage, respectively. Chapter 7 then moves on to third party liability coverage and Chapter 8 addresses cyber-crime cover, such as extortion, computer fraud and funds transfer fraud, identity theft and hacking. Chapter 9 deals with exclusions that are specific to stand-alone cyber insurance and Chapter 10 deals with claims issues, such as notification. Chapter 11 addresses cyber risks reinsurance and insurance-linked securities.

The author is an international insurance and litigation solicitor advocate and is clearly drawing on a great amount of knowledge and experience in this area. The book maps out market practice by reference to specific clauses, cyber policy wordings and underwriting practices. Helpfully, the author has appended policy wording materials. The comparative analysis of different cyber risk exclusion clauses as used for different classes of risk in traditional policies, found in Chapter 3 is particularly insightful. Similarly, Chapter 6 gives a detailed account of the different types of cyber-risk related business interruption cover, highlighting imprecise drafting in relation to some key concepts and evaluating the effectiveness and appropriateness of different bases for calculating business interruption loss. There is some detailed legal commentary and analysis, for example on the applicability of 'physical damage' concepts (Section 2.2) insurability of fines (Section 5.6), the recoverability of ransom payments

[*] Cyber Risks Insurance: Law and Practice. *Celso de Azevedo, solicitor advocate, barrister, attorney (New York). Sweet & Maxwell, London (2019) xxxii and 284 pp, plus 104 pp Appendices and 4 pp Index. ISBN 978-0-414-07034-9. Hardback £160.*

[**] Lecturer, Centre for Commercial Law Studies at Queen Mary University of London

(Section 8.1) and notification of circumstances (Section 10.3.2), and comparative legal analysis with the US position on traditional property and liability policy coverage (Section 2.3 and 7.6).

There is a legal publishing trend towards ever more specialist titles. The challenge for any author writing in a niche area is to strike the right balance between including and excluding more general background. True to its title, this book retains a narrow focus on insurance and reinsurance law and practice in relation to cyber risks and assumes that the reader has a solid pre-existing understanding of general insurance law principles and practices. In some instances, it might have been more instructive to err on the side of inclusiveness: for example, there is only a very short paragraph on the application of s.11 of the Insurance Act 2015 to exclusion clauses (Section 3.1.2). Given the prevalence of cyber exclusion clauses in traditional policies and the numerous specific exclusions clauses in stand-alone cyber risks policies, a more detailed evaluation of whether or not specific exclusion wordings might fall within the scope of s.11(1) would have been useful. Examples of issues that would have merited consideration in the cyber context but are not discussed are the legal and practical problems that can arise when insurers take control of the defence vis-à-vis a third party claim (which could have been covered in Chapter 7 or 10), and the thorny issue of overlapping claims where two or more policies respond to the same loss. The book does not address jurisdictional issues and the extent to which traditional consumer policies cover cyber risks either by way of silent cover or cyber risks add-ons. Perhaps these are topics that the author could consider for inclusion in his second edition.

The author is to be commended for making a significant contribution to a still evolving subject-matter and for assembling the existing market developments into a coherent exposition. The book should serve as a useful guide for cyber risks underwriters and brokers, as well as for insurance law practitioners.