UNDER EMBARGO UNTIL 8:00 AM, 6 JUNE 2022

PRESS RELEASE

CYBER RISK AND INSURANCE: PERFECTING GOVERNANCE CHALLENGES AND QUESTIONS

A new guide, the second in our series "perfecting governance", published by Airmic partnered with McGill and Partners, answers 12 questions associated with cyber risk and insurance, posed from a director's perspective.

The World Economic Global Security Outlook concludes that "The potential cyber risks and vulnerabilities of these new technologies should be on minds of every leader when considering technology adoption and implementation." The challenge is how to translate leaders' concerns about cyber security into constructive action at board level.

The publication aims to provide an insider's guide to cyber risk and insurance for end users, and for board members in particular. Twelve questions make up the core of the guide, focusing on practical issues that commonly arise. The answers are intended to provide general guidance as to the likely position, subject to the significant caveat that no two cyber risks or cyber insurance policies are the same. The questions are posed from the point of view of directors and board members themselves:

1. Assuming I have no particular background or experience in IT, what level of expertise with respect to cyber risk will be expected of me as a member of the board?
2. As a prospective or newly appointed board member how might I get comfort that the company's cybersecurity systems are as robust as they need to be?
3. Is there a board-level cybersecurity review blueprint or checklist I can use to ask the right questions, such as those set out in question 2?
4. How might I be potentially liable if the company is the victim of a major cyber-attack?
5. There are a number of descriptions applied both to cyber related dangers faced by companies and the means of protecting against them. These include cyber risk, cyberattack, cyber security and cyber resilience. They often seem to be used interchangeably – what do they all mean?
6. What is the potential impact of a cybersecurity event to significant or public infrastructure/services if our company manages or operates these?
7. What role should I as a board member play in cyber security and cyber resilience for the company?
8. What is my role as a board member if my company experiences a cyber event?
9. What does a cyber insurance policy cover?
10. What does a cyber insurance policy not cover?
11. How do I determine the right level of cyber insurance coverage for my company?
12. Is cyber insurance the new 'D&O' as a necessary insurance purchase?
    Although the UK Government National Cyber Security Strategy published in 2022 is government-led, the private sector and citizens are assigned responsibility to manage cyber risks. The Strategy assumes that cyber risks will become pervasive, increasing the volume of personal and sensitive data generated and the potential impact if systems are breached. Against this backdrop, the threats in cyberspace will continue to evolve and diversify as high-end cyber capabilities become commoditised and proliferate to a wider range of states and criminal groups. The number of actors with the ability and intent to target the UK in cyberspace, and threat actors will employ a wider range of levers to conduct disruptive activity.

Julia Graham, CEO, Airmic, commented: “There is no “one size fits all” approach to addressing cyber risks with specific business circumstances varying greatly from organisation to another. It may be appropriate for organisations to consider accreditation or certification from a recognised body, such as Cyber Essentials, Cyber Essentials Plus or ISO270001. These accreditations may help an organisation, however, accreditation alone is not enough. Asking the “right” questions before a problem arises, makes good management sense. This guide is an important contribution to our members who support their leadership, as they collectively navigate an increasingly complex world and associated governance responsibilities”.

Francis Kean commented: “No directors can afford to ignore the ever evolving and expanding cyber threats posed to companies on whose board they sit. Given that most board members are not IT experts, how should they go about the task of assessing both the nature and level of these threats and the state of the company’s preparedness and resilience to meet them? We hope this Guide will prove a useful and practical tool to enable them to do this whilst at the same time providing some useful clarity both as to certain key definitions and expressions and as to the role cyber insurance can play in risk mitigation”.

ABOUT MCGILL AND PARTNERS

McGill and Partners is a boutique specialist (re)insurance broker focused on large clients and/or clients with complex and/or challenging needs. Launched in 2019, the firm has significant backing from funds affiliated with Warburg Pincus, a leading global private equity firm. McGill and Partners is a rapidly growing British-based firm, headquartered in London with offices in Bermuda, the US and Ireland.

www.mcgillpartners.com

ABOUT AIRMIC

The leading UK association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 1,500 individual members. Individual members are from all sectors and include company secretaries, finance directors, and internal auditors, as well as risk and insurance professionals. Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com