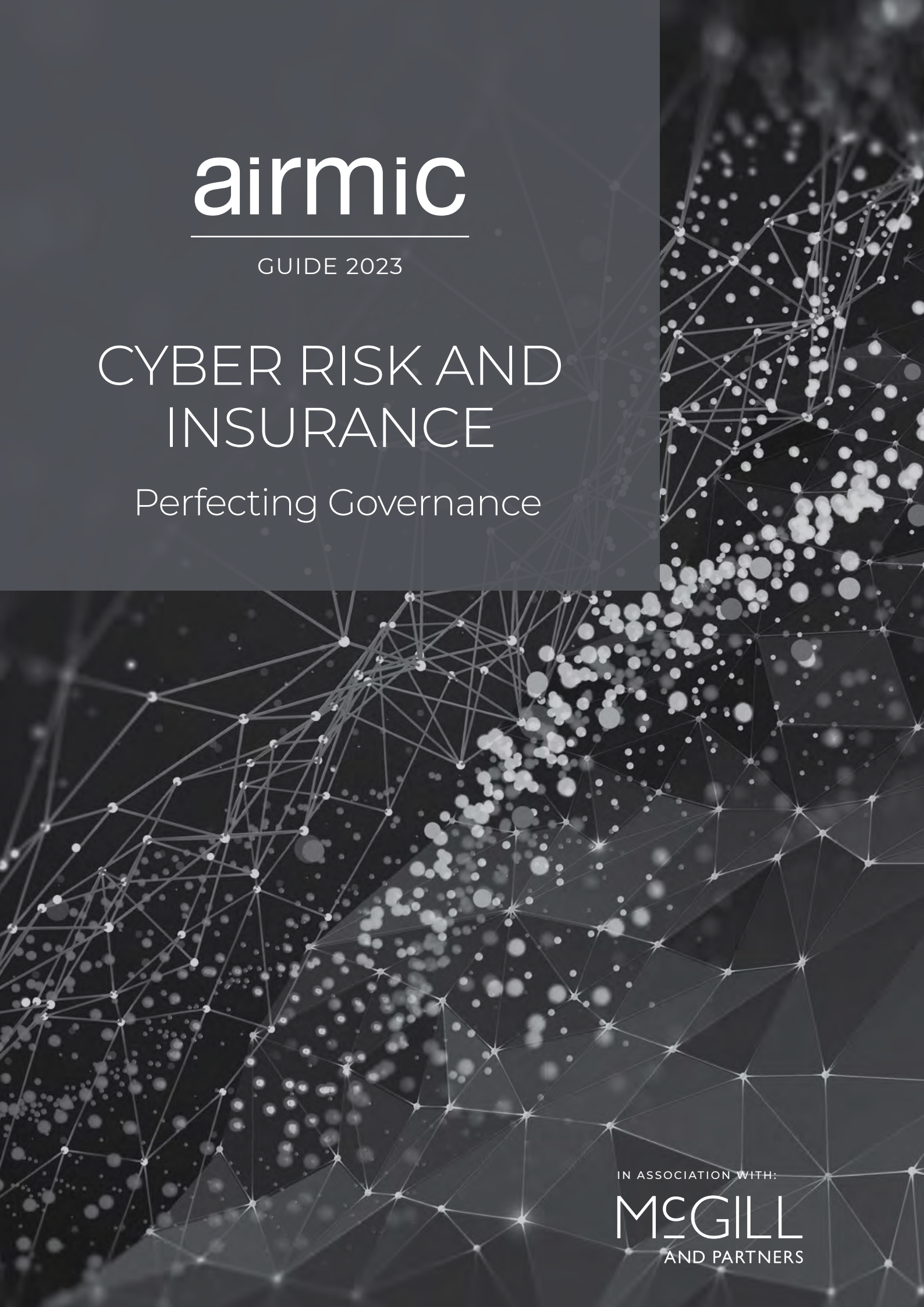
airmic

GUIDE 2023

CYBER RISK AND INSURANCE

Perfecting Governance



IN ASSOCIATION WITH:

McGILL AND PARTNERS

Acknowledgements

About McGill and Partners
Shannan Fort is a Partner within the Financial Lines team at McGill and Partners, where she leads the Cyber and Commercial Errors & Omissions team. Shannan has spent over 15 years in the Cyber Insurance industry, has extensive experience with complex cyber insurance programmes, policy drafting and cyber insurance product development. She is a frequent contributor to publications, panels and conferences on the topic of Cyber.

Francis Kean joined McGill and Partners in 2020 bringing with him thirty years of experience in the industry. Francis is a Partner within the Financial Lines team. Previously, he was a partner at the law firm Barlow Lyde and Gilbert. Francis has handled a wide variety of financial lines claims for both insurers and clients, and has considerable experience of drafting policies and advising all parties in connection with coverage issues. He is a frequent author and speaker on liability issues affecting boards.

McGill and Partners is a boutique specialist (re)insurance broker focused on large clients and/or those 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 British based firm, headquartered in London with international presence in New York, Miami, Chicago, Bermuda, Switzerland, Germany, Sydney and Dublin.

www.mcgillpartners.com

McGILL
AND PARTNERS

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 1,800 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

airmic

CONTENTS

01 Introduction

The cyber insurance market has experienced significant upheaval since 2020. Dramatic increases in frequency and severity of insured cyber losses (particularly the impact of ransomware) have led to pricing increases, reduction in capacity and restriction in coverage, while the market grappled with a more consistent approach to minimum security standards required for coverage.

This period of correction is ushering in lasting change while also attracting new capacity and market innovation, leading to more choice and fit-for-purpose coverage for insureds.

The profile of cyber risk has increased over the past two years, in large part because of the increase in remote working and cloud computing during the pandemic and, more recently, because of the geopolitical climate since the invasion of Ukraine and a concurrent increase in malicious cyber activity. In the 2022 survey of Airmic members, they reported cyber risk as the risk that concerns them most.

Although the UK Government National Cyber Security Strategy (originally 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 cyberattack 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 will increase, and these threat actors will employ a wider range of levers to conduct disruptive activity.

"Cybersecurity (the protection of devices, services and networks, and the information on them, from theft or damage via electronic means) is not a separate technology but rather a foundational set of systems, spanning technology, people and processes for the Fourth Industrial Revolution." This is the view of the managing director of the World Economic Forum (WEF), expressed in its Global Security Outlook 2022. There is an ever-improving understanding of cyber risks and the importance of cybersecurity, at the highest levels of organisations, though challenges remain: "Overall, the study indicates that business leaders are more aware of their organisations' cyber issues than they were a year ago. They are also more willing to address those risks. Nonetheless, cyber leaders still struggle to clearly articulate the risk that cyber issues pose to their organisations in a language that their business counterparts fully understand and can act upon. As a result, agreeing on how best to address cyber risk remains a challenge for organisational leaders." (WEF, as expressed in its Global Security Outlook 2023)

The challenge remains how to translate leaders' concerns about cybersecurity into constructive action at board level.

"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."

Julia Graham – CEO, Airmic

The aim of this Guide is to provide a toolkit to assist directors in understanding and keeping pace with the ever more complex cyber-related threats faced by the companies they serve. It takes the form of 12 questions designed to break a diverse set of issues down into a manageable series of topics. The list is not exhaustive and the answers to each question will vary tremendously depending on the size, maturity and nature of the company's operations. Nevertheless, in response to each question, we identify a range of issues which are likely to be relevant.

One of the threshold challenges with respect to cybersecurity for directors relates to language and communication within the company. A key finding of the WEF Global Security Outlook 2023 is that 95% of business leaders polled believed that cyber resilience was integrate into enterprise risk management strategies; 93% of security-focused experts within the same organisations held that view, a significant shift from 2022 (up from 55%). Plainly, language plays an important role here too. For example, cyber resilience and cybersecurity are not synonymous. Please see question 5 for a short glossary of some important definitions.

Most of this Guide is devoted to issues of cyber, defence, security, resilience and insurance. We also touch briefly on the topic of data privacy, which can be an offline as well as an online issue for companies. We do not include questions relating to AI, where the challenge is often to understand in what ways the company deploys AI and the extent to which those uses (and the algorithms that underpin them) are sufficiently robust to defend against allegations of bias, unfairness and error.

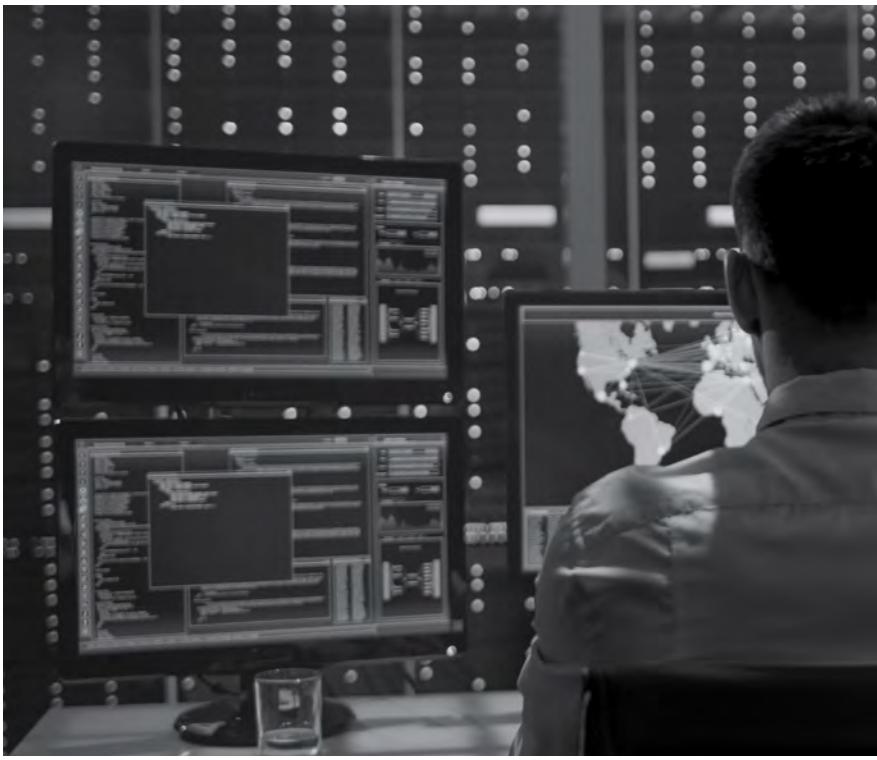
The Twelve Questions

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?

Your legal duty to supervise your company's activities, including those carried out through the use of computers, cannot be delegated. In order to discharge that duty, you must have enough expertise to understand both how a cyber event might affect the whole company and what the specific consequences might be for the area of your particular focus. You should have a working knowledge of the cyber risks the company faces, the benchmarks the company uses to measure these, the associated controls in place, and how risks will change and emerge with the advance of and heavier reliance on technology throughout the company (not just as it relates to consumer and client products/services offered by the company). Board members should also be aware of the cyber/privacy-related training the company has in place for employees and how the success of this training is measured.

"In the rapidly shifting sands of cyber security we hope that this focus on certain high-level principles and key definitions coupled with insights into the role of cyber-insurance will prove a valuable resource for directors."

Francis Kean – Partner, McGill and Partners



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?

There is no single answer comprehensive enough to capture all of the potential cyber risks that every company will face. The same is true of the cybersecurity systems designed to guard against them (but see the answer to question 3 for a list of important preliminary topics). Much will depend on the company's size, sophistication and business maturity, industry sector and sphere of operations. More important perhaps is an ability to communicate effectively with those in the company whose responsibility it is to maintain cybersecurity, including for larger companies, the Chief Information Security Officer (CISO).

Relevant questions to ask yourself might include:

a. Do I know who the relevant executives are?
b. Do I know how these executives report to the board?
c. Do I have an understanding of the executive skill sets, especially those required to protect the company's assets, which could range from network security to risk management and incident response?
d. Does the company have the necessary resources to manage cyber risk?
e. What is the cyber culture within the organisation? For example, what is the attitude to cyber training and skills? Do employees understand and accept their personal responsibility for cybersecurity regardless of their role or do they believe that cybersecurity is the job of the IT department? (See also the answer to question 6.)
f. How are cyber risks integrated into the overall risk management framework and risk reporting for the company?

Directors should use as many sources as possible to assess their cyber security risk, including feedback from insurers whose assessment for underwriting purposes has gone to another level in the hardening insurance market. Their independent scrutiny provides valuable insight into areas that may need to be strengthened.

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?

Setting and adhering to the appropriate culture, risk appetite and associated policies and processes is part of a board's responsibility, but there is no one-size-fits-all approach. You should ask yourself if you understand (and therefore have a reasonable level of comfort as to) the processes in place to:

a. manage cybersecurity risks emanating from third parties' (suppliers, clients and partners) network services and applications
b. ensure identification and allocation of appropriate financial and human resources
c. reduce security risks from employees
d. manage risks specific to confidential/sensitive data, in line with the regulatory requirements in the various jurisdictions in which the company operates, and
e. manage residual risk via cyber insurance or other forms of risk transfer.

Equally critical is ensuring that you understand what plans the company has in place to respond to cyber events (and what role the board can take to support the preparedness plan), including:

a. remediation practices
b. cyber-specific incident response and business continuity plans
c. the process for plan testing and rehearsals
d. how lessons learnt from 'near misses' are reported, evaluated and incorporated into the risk management framework of the company
e. guidelines on communication to stakeholders, including shareholders, regulatory authorities and employees, following an event.

These practical steps can be applied to any company and any industry – and can support your understanding of (and thereby comfort with) the company's assessment and mitigation of risk, and response to cyber events.

> "There is no 'one-size-fits-all' approach to addressing cyber risks, with specific business circumstances varying greatly from one 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."
>
> *Julia Graham – CEO, Airmic*

4 How might I be potentially liable if the company is the victim of a major cyberattack?

Various attempts have been made, particularly in the USA by plaintiffs' lawyers on behalf of shareholders, to bring breach of duty claims against directors following serious cyber events that resulted in share price falls, significant financial loss and/or loss of reputation. The general case theory underpinning such actions has been that, given the vulnerability of the company's defences to attack (evident after the event), the risk of attack was (or should have been) foreseen by the board, who should have taken steps to prevent it. Such cases are always heavily fact dependent, but so far, directors have been able to defend themselves successfully on the basis of evidence as to the steps they took at the relevant time to provide oversight and ensure compliance with the implementation of appropriate measures in line with the policy and processes of the company.

A separate source of potential corporate legal and regulatory liability relates to failure to comply with disclosure requirements, whether under the General Data Protection Regulation (GDPR) or other legal data privacy or infrastructure frameworks, including the increasingly wide-ranging rules imposed by the US Securities and Exchange Commission (if applicable to your business). Disclosure of data breach or cyberattack may be mandated not simply to regulatory authorities but also to shareholders and/or directly to those individuals affected. You should also be aware that, in certain jurisdictions, the mishandling of cyber events could also lead to criminal penalties against board members personally (for example, under the UAE Penal Code and Cybercrimes Law).

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, cybersecurity and cyber resilience. They often seem to be used interchangeably – what do they all mean?

There are numerous terms applied to the cyber-related dangers faced by companies, which are often used interchangeably when discussing this topic. They include cyber risk, security, incidents and resilience. The definition of these terms is not universally agreed. For the purposes of this Guide, we set out below some common ones:

a. Cyberattack – deliberate entry into a computer system, with the intent to alter, corrupt or remove systems/data, irrespective as to the identity of the perpetrator
b. Cyber event – general collective term encompassing cyber incident, cyberattack and/or data breach
c. Cyber incident – accidental or unintentional alteration, corruption or failure of computer systems/data
d. Cyber risk – the risk of loss, damage or disruption to a company emanating from its network systems and/or data
e. Cyber resilience – the ability to anticipate, identify, recover from and/or withstand cyber events
f. Cybersecurity – the processes, practices and technologies employed to protect the company's network systems and data
g. Data breach – loss, theft or unauthorised disclosure of confidential/personal data whether on computer or otherwise
h. System failure – unplanned and unintentional outage of a computer system.

Please also see the response to question 9, which provides further descriptions and definitions as they relate to cyber insurance.

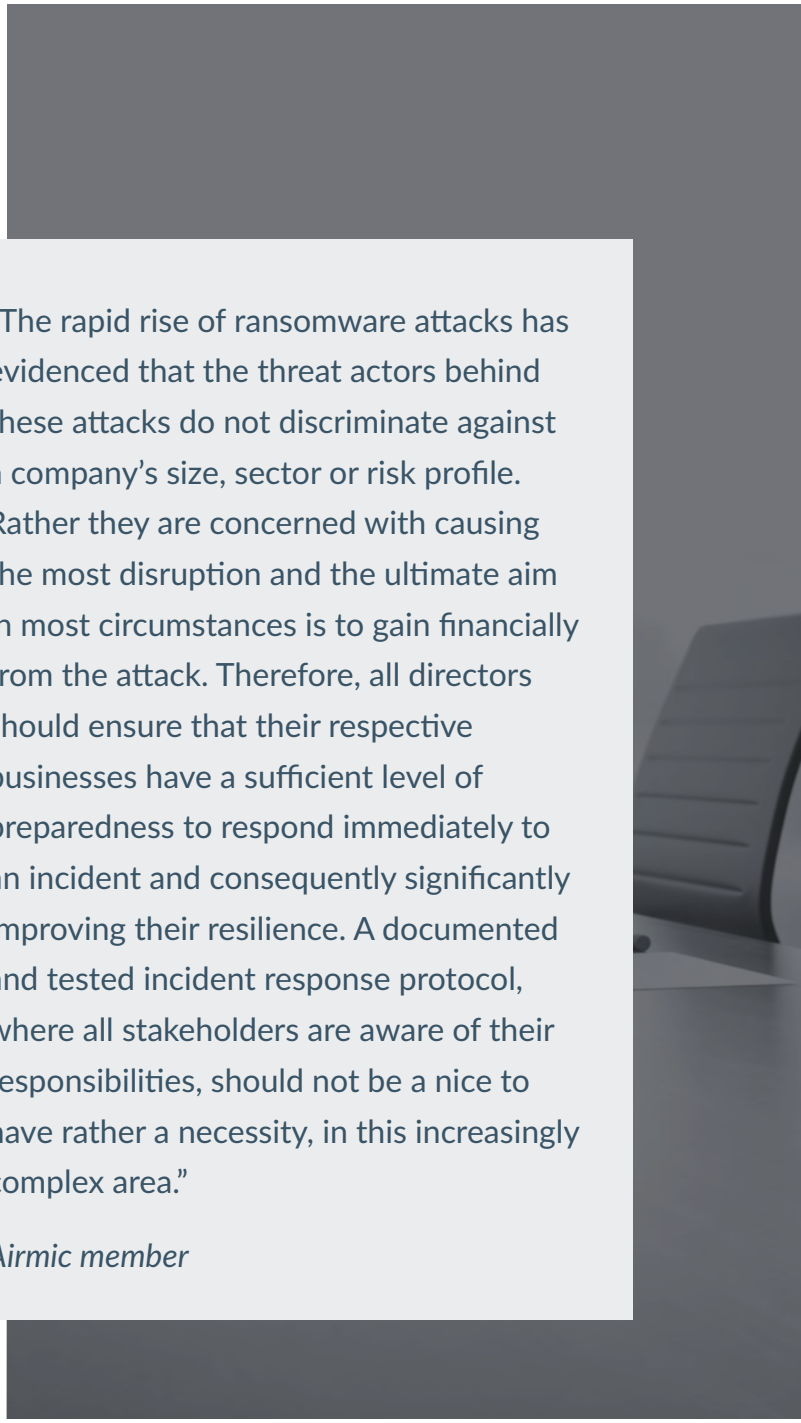
6 What is the potential impact of a cybersecurity event to significant or public infrastructure/services if our company manages or operates these?

Separate legal and regulatory frameworks apply in different jurisdictions to companies within vital sectors that rely heavily on information networks, such as utilities, healthcare, transport and digital infrastructure companies. For example, in the UK, the Network and Information Systems Regulations apply to all "operators of essential services". If you are a director of one of these companies, you will also need to:

- understand that there are additional requirements to notify serious incidents to the relevant national authorities
- obtain comfort that appropriate and proportionate measures have been taken to meet the enhanced threat and consequences of a cyber incident, and
- know the extent of the additional regulatory risk (in the form of severe fines and penalties) faced by the company in the event of a breach of the relevant regulations.

7 What role should I as a board member play in cybersecurity and cyber resilience for the company?

Unless you have expertise and/or specific IT-related roles or responsibilities, it is unlikely you will be required to take an active role in the response to a cyber event. That said, you should seek comfort that those entrusted to manage, mitigate and respond to cyber events are adequately prepared. This comfort can be gained through direct interaction with the members of your organisation most directly responsible for cybersecurity – including, but not limited to the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Information Officer (CIO), Information Technology Director (IT Director), Data Protection Officer (DPO), Human Resources Director (HR Director) and Risk Manager (RM). Are you satisfied that these individuals, the relevant business units and the company as a whole communicate effectively? Research has shown that 88% of UK data breaches are caused by human error (according to a study of data breaches reported to the Information Commissioner's Office).



"The rapid rise of ransomware attacks has evidenced that the threat actors behind these attacks do not discriminate against a company's size, sector or risk profile. Rather they are concerned with causing the most disruption and the ultimate aim in most circumstances is to gain financially from the attack. Therefore, all directors should ensure that their respective businesses have a sufficient level of preparedness to respond immediately to an incident and consequently significantly improving their resilience. A documented and tested incident response protocol, where all stakeholders are aware of their responsibilities, should not be a nice to have rather a necessity, in this increasingly complex area."

Airmic member

8 What is my role as a board member if my company experiences a cyber event?

As indicated in answer to questions 3 and 6, ensuring adequate preparation for a cyber event is a key component of your cyber-related responsibilities and reinforcing a culture that values cybersecurity/cyber resilience will lead to more positive outcomes when (not if) an incident occurs. At that point and depending on the nature and severity of the event, you are likely to be involved or consulted as part of the Cyber-specific Business Continuity and Incident Response Plans specifically designed for the organisation. You should be familiar with the plans (ensuring they do exist) and should take an active role in testing the plans – including bringing together the various participants.

Testing the plans outside of a live incident will help identify weaknesses in the plan/approach. This may include the approval and use of various vendors, the process for contacting various stakeholders and the escalation of significant incidents. You should have input in the selection of key stakeholders and familiarity with their roles/expertise. When a significant incident is discovered, you should feel confident that these stakeholders have demonstrated the abilities needed to perform the roles assigned to them and be ready to discharge your oversight role in the execution of these pre-prepared plans.

9 What does a cyber insurance policy cover?

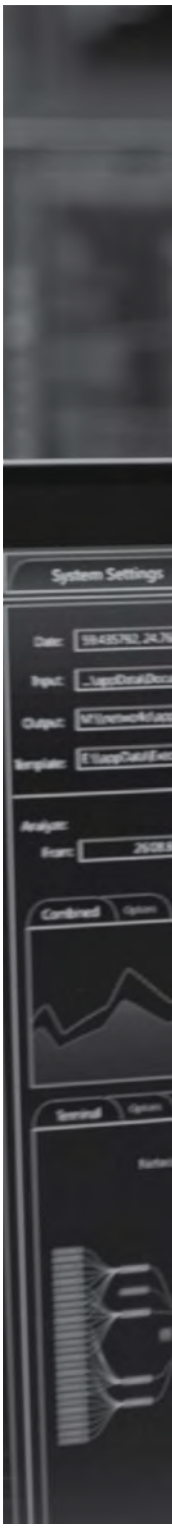
Fundamentally, cyber policies are about two concepts – the protection of confidential data and the interaction of network systems. When these two concepts go wrong (i.e. data breaches, ransomware, data corruption, system failure, malware, etc.), cyber insurance is designed to cover the organisation's resilience/response costs (first-party coverage) and liability stemming from these events (third-party coverage).

Though terminology is inconsistent across the market and coverage terms are complex, insurance protection generally falls into one or both of the two categories below:

a) First party – the company's own costs:
   I. Breach Response Costs – covers the immediate response costs following an actual or suspected breach; designed to mitigate the impact of the breach and provide some relief to consumers without the need for consumers to make a formal claim.
   II. Data Asset Costs – covers the cost to restore, recreate or repair the company's own data that has been altered, corrupted or destroyed as the result of a cyberattack.
   III. Business Interruption – reimburses for income loss and extra expense as the result of a cyber incident. The triggers can include cyberattack and/or system failure (unplanned and unintentional outage of a computer system) and can extend to critical IT vendors' systems on which the company relies.

b) Third party – covers the cost of defence, settlement and judgments from claims against the company by third parties such as customers:
   I. Privacy Liability – claims alleging financial harm from the loss, theft, disclosure of confidential information of third parties.
   II. Security Liability – claims alleging financial harm from the interaction of the insured's computer networks/systems with a third party's networks/systems (transmission of virus, malware, denial of service attacks, etc.)
   III. Regulatory Fines/Penalties – assessed against the insured by governmental authorities following the loss, theft, disclosure of confidential consumer data to the extent insurable.

However, no two cyber policies are exactly alike – cyber policies are designed as modular products offering different types of cover. The current (2022) harsh conditions in the cyber insurance market are unlikely to improve in the foreseeable future. Prices are on the road to stability, but as cyber risk continues to evolve, it is predicted that purchasers of cyber insurance will continue to experience significant premium increases combined with coverage and capacity restrictions.



"Whatever cover is in place, it is important that the company has a clear understanding of its coverage priorities with respect to insurable cyber risk, the declarations of controls made to insurers and the protocols to be followed following an event."

Airmic member

10 What does a cyber insurance policy not cover?

There are significant restrictions on the nature of cover provided under a cyber policy. These are set out below, but there is also a relevant and important insurance market trend driven in part by the UK's Prudential Regulatory Authority (PRA) to which we should draw attention. Driven by its concern about systemic losses caused by cyber incidents, the PRA has required insurers to address the risk of so-called 'silent cyber' across their entire books of business. For example, on a property or professional indemnity risk, coverage previously existed irrespective of whether the loss occurred through the use of computers, but that assumption should no longer be made. Insurers are instead being required expressly to state whether they are providing or excluding cyber coverage across their entire portfolios. This means that cyber insurance (both as to covered and non-covered loss) assumes additional importance.

As to what is typically not covered, it is important to understand that no cyber policy will cover the theft or loss of money or funds sustained by the company as a result of targeted cybertheft or cyberattack. To the extent this cover is available in the insurance market, this would be found within a commercial crime policy. Additionally, the following main exclusions are common:

a) Bodily Injury & Property Damage – direct and indirect bodily injury and property damage, often including loss of use, are excluded from cyber policies. The cyber market does provide products to sit in the gap that these exclusions create.
b) Infrastructure – failure of public utilities (including telecommunications providers) and failure or inaccessibility of the internet are excluded under cyber policies as they represent a particularly detrimental systemic risk currently uninsurable in the cyber market.
c) War (including Cyber War) – as the use of devasting cyberattacks becomes a more common weapon of conflict between states, the cyber market must reckon with the potential impact with insurable risk. This has led to revised war exclusions, which aim to clarify systemic from insurable risk with respect to cyberattacks perpetrated by nation-state actors.

11 How do I determine the right level of cyber insurance coverage for my company?

There is no single route by which the appropriate level of coverage can be determined. Competent insurance brokers are well placed to answer this question by reference to benchmarking and data analytics, including the cost of recent claims. This can provide a level of comfort, but as peer groups are sometimes elusive, the information can be incomplete and there remains the possibility that the relevant peer group has either underestimated or overestimated the appropriate level of cover. You should also potentially call for a cost/benefit analysis of some kind, especially given the current hard market conditions.

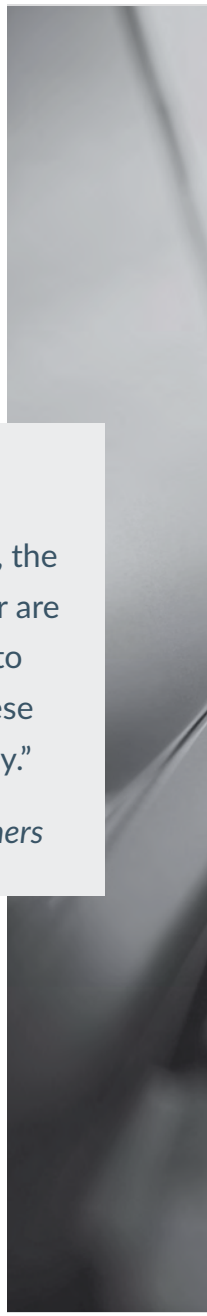
"The 'right level' of cyber insurance is not a static concept and should be continually reviewed as the nature of the risk, dependence, and interconnectivity of technology changes."

Shannan Fort – Partner, McGill and Partners

12 Is cyber insurance the new 'D&O' as a necessary insurance purchase?

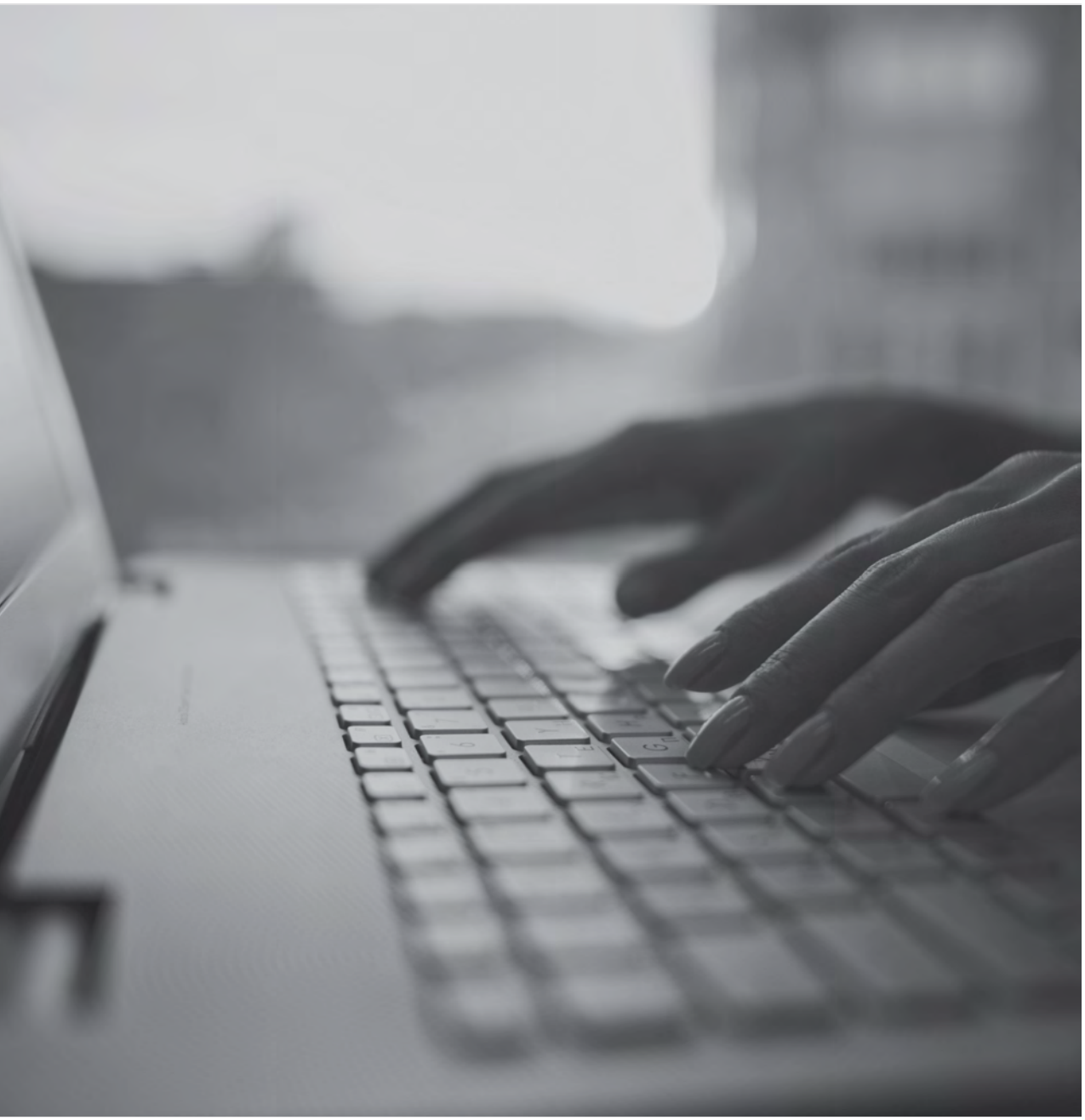
The question as to whether D&O insurance is a necessary company purchase is one that did not feature among the 12 questions comprising the first of our boardroom guides published in 2021 on that subject. Few if any large or public companies would any longer consider D&O insurance a discretionary purchase. Yet, D&O is a relatively young class of insurance – the first such policy having been sold within the last with 50 years – nor was it universally adopted at the outset. There are perhaps some parallels.

Cyber is also a relatively new class of insurance, where the onus is on the industry to explain the benefits in order to justify the premium spend, whilst also being clear as to the limitations of coverage in order to minimise the risk of significant expectation gaps arising. Given the rapidly evolving cybersecurity threat levels faced by all companies, what can perhaps safely be said is that this form of liability protection and loss mitigation should not be ignored. A reasoned and documented case (whether the decision is taken to purchase or not) based on appropriate analysis and input from brokers and other industry experts is far preferable to the more dangerous assumption that this class of insurance can be ignored until it matures further.



"Cyber and D&O insurances do share some commonality – most importantly, the underlying risks that they seek to cover are not going away and will only continue to evolve in scale and complexity, and these are not risks that should be taken lightly."

Shannan Fort – Partner, McGill and Partners



airmic

Marlow House
1a Lloyd's Avenue
London
EC3N 3AA
+44 207 680 3088
enquiries@airmic.com
www.airmic.com