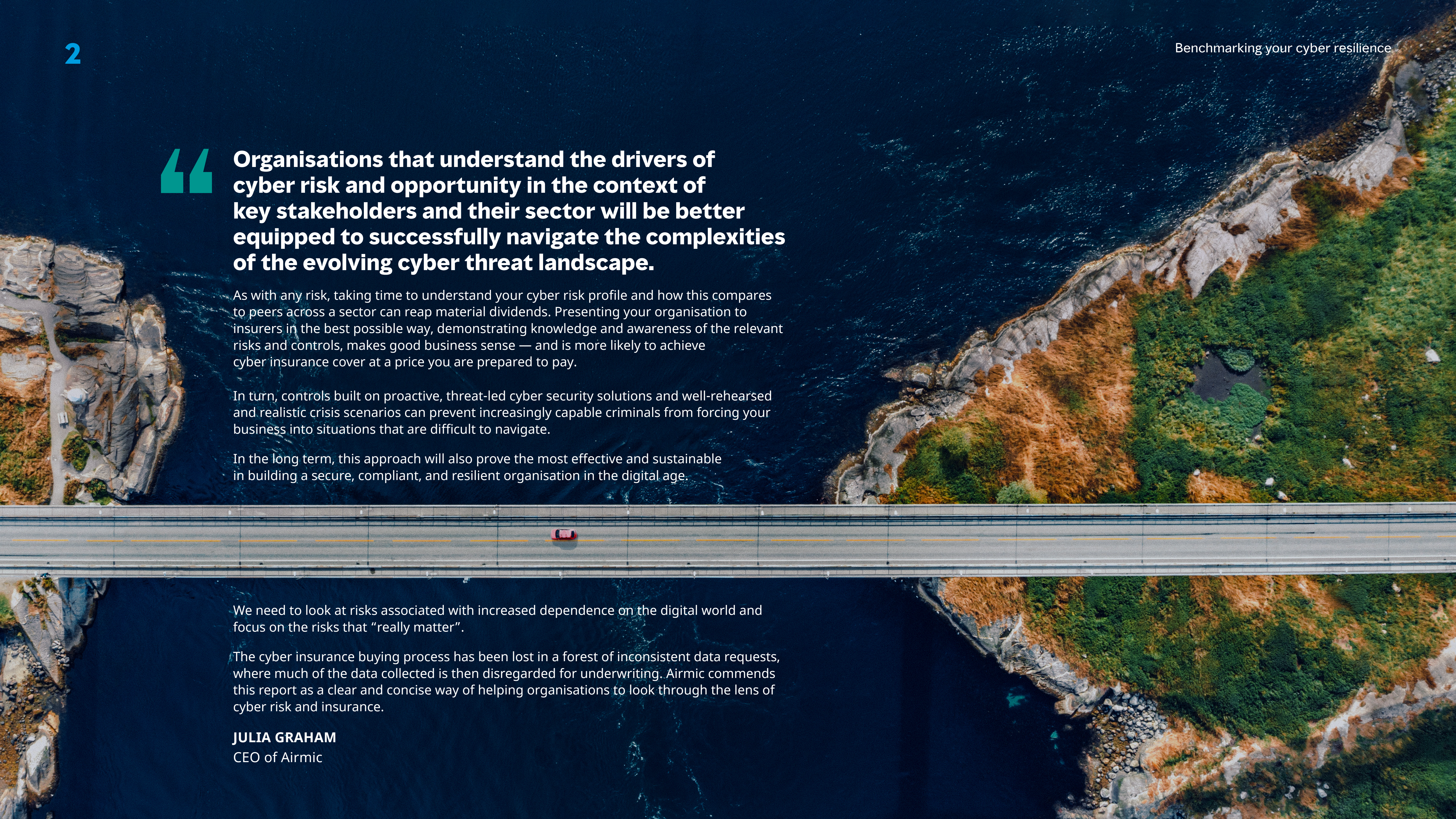
Marsh | airmic

Benchmarking your cyber resilience

How do you rank against your peers?



> **Organisations that understand the drivers of cyber risk and opportunity in the context of key stakeholders and their sector will be better equipped to successfully navigate the complexities of the evolving cyber threat landscape.**

As with any risk, taking time to understand your cyber risk profile and how this compares to peers across a sector can reap material dividends. Presenting your organisation to insurers in the best possible way, demonstrating knowledge and awareness of the relevant risks and controls, makes good business sense — and is more likely to achieve cyber insurance cover at a price you are prepared to pay.

In turn, controls built on proactive, threat-led cyber security solutions and well-rehearsed and realistic crisis scenarios can prevent increasingly capable criminals from forcing your business into situations that are difficult to navigate.

In the long term, this approach will also prove the most effective and sustainable in building a secure, compliant, and resilient organisation in the digital age.

We need to look at risks associated with increased dependence on the digital world and focus on the risks that “really matter”.

The cyber insurance buying process has been lost in a forest of inconsistent data requests, where much of the data collected is then disregarded for underwriting. Airmic commends this report as a clear and concise way of helping organisations to look through the lens of cyber risk and insurance.

JULIA GRAHAM
CEO of Airmic

As cyberattacks and related insurance claims continue to rise, insurers are becoming increasingly selective about the risks they will underwrite. Many insurers have made the adoption of certain controls — mechanisms or processes to protect an organisation’s cyber vulnerabilities — a minimum requirement for securing any level of cyber insurance, let alone coverage with favourable pricing and terms.

The use of certain cyber hygiene controls can help organisations positively differentiate their cyber risk management to insurers. Organisations that do not have particular controls in place may be at a strong disadvantage relative to their peers when seeking cyber insurance, and may face a higher risk of experiencing a cyber incident.

How does your organisation compare to your peers?

According to an analysis of data from several hundred Marsh UK clients conducted by the Marsh McLennan Cyber Risk Analytics Center, most clients deploy five basic account monitoring and protection controls (see Figure 1).

01| Most Marsh UK clients deploy basic account monitoring and protection controls

Marsh cyber self-assessment category	Control	Affirmative response rate
Account monitoring	Accounts are disabled upon termination of an employee.	99.6%
Protection capabilities	Incoming emails are filtered/ scanned for malicious attachments and links.	98.9%
Account monitoring	Minimum password requirements are in place.	96.9%
Protection capabilities	Anti-malware solutions are installed on at least 75% of endpoints and regularly updated.	96.3%
Protection capabilities	Firewalls are configured to prevent unauthorised access, and the firewall configurations are reviewed at least annually.	96.2%

Implementation of cyber controls varies by and within industry sectors (see Figure 2). Failure to adopt the above controls may have more impact on an organisation's insurability, depending on how widely those controls are used by peer organisations.

02| Implementation of the most common controls varies by industry

Implementation rate by industry for Marsh clients

Marsh cyber self-assessment category	Manufacturing	Education	Wholesale and retail trade	Professional, scientific and technical services
Accounts are disabled upon termination of an employee.	100%	100%	98.3%	100%
Incoming emails are filtered/ scanned for malicious attachments and links.	100%	100%	98.1%	100%
Minimum password requirements are in place.	96.7%	100%	94.8%	100%
Anti-malware solutions are installed on at least 75% of endpoints and regularly updated.	94.4%	100%	98%	98.2%
Firewalls are configured to prevent unauthorised access, and the firewall configurations are reviewed at least annually.	96.7%	88.5%	92.9%	100%

At the same time, the absence of certain controls can both increase the risk of a cyber incident and create concern among insurers (see Figure 3). If your organisation does have these controls in place, its risk is reduced compared to its peers, potentially positioning your organisation more favourably in the eyes of insurers.

03| Most Marsh UK clients typically lag in adopting a number of cyber controls

Marsh cyber self-assessment category	Control	Affirmative response rate
Incident response	The organisation conducts incident response exercises at least quarterly	18.1%
Account monitoring	System accounts are monitored and have an expiration date	18.7%
Software management	Critical systems configured such that only applications on the whitelist can be run	26.5%
Protection capabilities	Remote access solutions that perform pre-login assessments before allowing access to corporate network are in place	28.1%
Software management	File integrity checking tools validate software has not been modified prior to execution on a system	29.8%

Again, it is instructive to identify how widely these controls are implemented in specific industries, as implementation rates will vary. If your organisation has controls implemented that are not widely used by your peer organisations, this could make you a more attractive risk to insurers (see Figure 4).

04| Implementation of less common controls varies by industry

Implementation rate by industry for Marsh clients

Marsh cyber self-assessment category	Manufacturing	Education	Wholesale and retail trade	Professional, scientific and technical services
The organisation conducts incident response exercises at least quarterly.	6.9%	21.7%	10.5%	21.1%
System accounts are monitored and have an expiration date.	13.3%	11.1%	13.8%	20%
Critical systems configured such that only applications on the whitelist can be run.	11.3%	28.6%	27.1%	35%
Remote access solutions that perform pre-login assessments before allowing access to corporate network are in place.	21.7%	26.9%	42.1%	26.7%
File integrity checking tools validate software has not been modified prior to execution on a system.	22.6%	14.3%	32.2%	35.5%

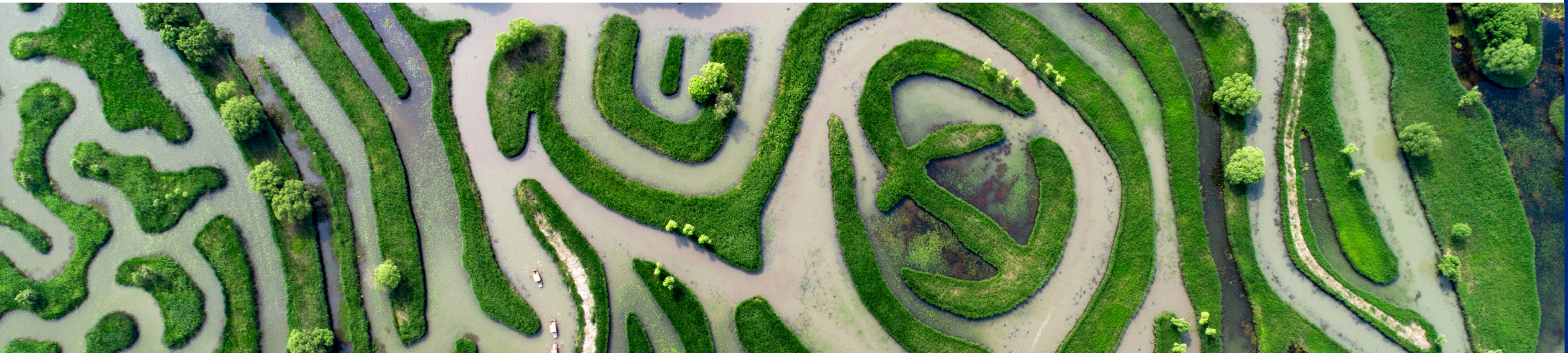
Although these controls have been established as best practices for several years, some companies have yet to adopt them, for reasons that may include costs, lack of understanding, and/or a failure to see the need. However, by having these controls in place, a company may reduce its chances of experiencing a headline-worthy breach, while also earning preferential treatment from underwriters. As the frequency and severity of cyberattacks continue to increase, identifying, evaluating, and understanding your cyber exposures is critical.

A holistic view of your cybersecurity risk profile can identify measures that will help to boost your organisation's insurability. By thoroughly reviewing your organisation's cyber hygiene and incorporating enterprise-wide cyber risk management practices, you can better position your organisation to achieve heightened cyber resilience and insurability.

STUDY METHODOLOGY

Marsh developed the cyber self-assessment (CSA) questionnaire to help companies examine their cyber risks and streamline the cyber insurance application process. Aligned to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, the self-assessment includes a risk-scoring mechanism that enables organisations to address vulnerabilities prior to underwriting discussions.

Marsh CSA questionnaires were obtained from over 700 companies based in the UK. These questionnaires consist of hundreds of questions relating to a company's cybersecurity posture, interactions with third-party vendors, demographics, governance, and more. This initial list of questions was reduced to around 100 questions directly related to cybersecurity controls. The question's "response rate" is simply the percentage of companies that responded "yes" to a question from the total number that responded to it.



Contacts

For more information on how your business can better understand, measure, and manage cyber risk, please contact your local Marsh office or visit **marsh.com.**

Scott Stransky
Head of MMC Cyber Risk Analytics Center

+1 (617) 4601803
scott.stransky@mmc.com

Brian Warszona
UK Cyber Deputy Practice Leader

+44 (0)7392 123 570
brian.warszona@marsh.com

Marsh

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on LinkedIn and Twitter or subscribe to BRINK.

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 1,750 individual members. Individual members are from all sectors and include finance, sustainability, information and technology, internal audit, and legal professionals, as well as risk and insurance professionals. With our partners, and in collaboration with affiliate associations and institutes, 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

This is a marketing communication. The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Marsh Ireland Brokers Limited, trading as Marsh Ireland, Bowring Marsh, Charity Insurance, Echelon Claims Consultants, Guy Carpenter & Company, ILCS, Insolutions, Lloyd & Partners, Marsh Aviation Consulting, Marsh Claims Management Services, Marsh Claims Solutions, Marsh Specialty, Marsh Reclaim, and Marsh Risk Consulting, is regulated by the Central Bank of Ireland. Marsh Ireland, Bowring Marsh, Charity Insurance, Echelon Claims Consultants, Guy Carpenter & Company, ILCS, Insolutions, Lloyd & Partners, Marsh Aviation Consulting, Marsh Claims Management Services, Marsh Claims Solutions, Marsh Specialty, Marsh Reclaim, and Marsh Risk Consulting are trading names of Marsh Ireland Brokers Limited. Marsh Ireland Brokers Limited is a private company limited by shares registered in Ireland under company number 169458. VAT Number IE 6569458D. Registered Office: 4th Floor, 25-28 Adelaide Road, Dublin 2, Ireland, D02 RY98. Directors: T Colraine (British), P G Dromgoole (British), A J Croft (previously Kehoe), J Flahive (British), J C Grogan, P R Howett , C J Lay (British), S P Roche. Marsh Specialty is a trading name of Marsh Ltd. Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511). Registered in England and Wales Number: 1507274, Registered office: 1 Tower Place West, Tower Place, London EC3R 5BU.
23-1031389243