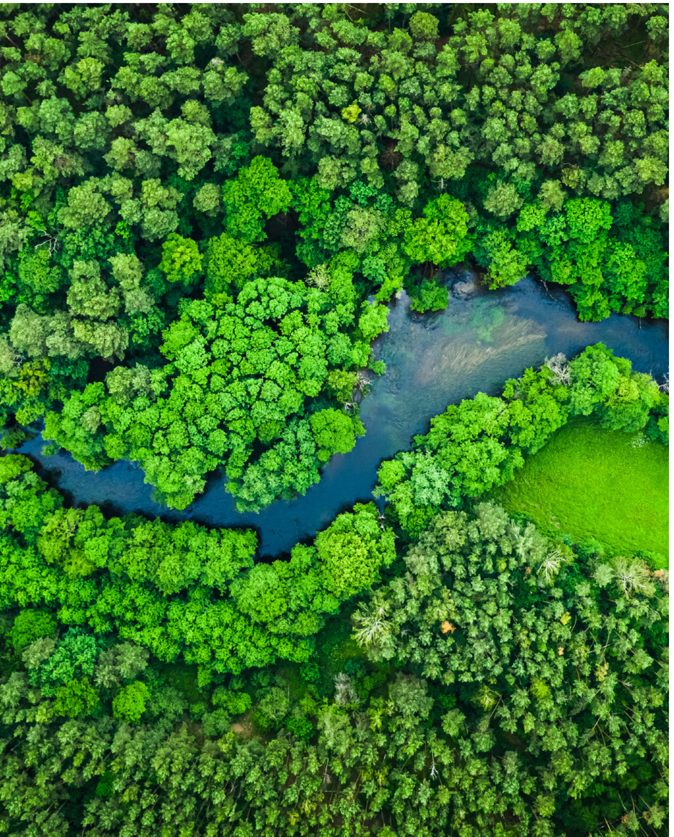
MarshMcLennan

Using data to prioritize cybersecurity investments

Marsh GuyCarpenter Mercer OliverWyman

Contents



Executive summary

In an industry first, Marsh McLennan's new report, *Using data to prioritize cybersecurity investments*, shows how the use of previously unavailable data for analytic research can help organizations evaluate the impact of their cyber controls. At the same time, this groundbreaking approach to evaluating the impact of cybersecurity controls has practical applications in prioritizing investments and developing strategic roadmaps.

The adoption of certain cybersecurity controls is now a minimum requirement to securing cyber coverage, with organizations' potential insurability and pricing at stake. However, while an array of cybersecurity controls have been established as critical for years, many organizations are unsure which to adopt, and have been slow to do so.

In the past, companies typically relied on expert opinions, not on data, to recommend which cyber controls were important. Now, for the first time, analysis of proprietary data by the Marsh McLennan Cyber Risk Analytics Center shows how cyber controls compare in terms of their effectiveness.

For the report, Marsh McLennan paired its extensive proprietary dataset of cyber claims with the results from Marsh Cybersecurity Self-Assessment (CSA) questionnaires, which are composed of hundreds of questions and responses from individual organizations. When combined, the two datasets allow for deep insights into which cybersecurity controls have the greatest effect on the likelihood of an organization experiencing a cyber event.

Such innovative use of data and analytics can help companies identify which controls to prioritize. In turn, this can help position an insured favorably during cyber insurance underwriting.

KEY FINDINGS:

- Automated hardening techniques — by a wide margin — have the greatest ability of any control studied to decrease the likelihood of a successful cyberattack, making it a key control to prioritize in order to minimize losses. Hardening limits the means of attack by applying baseline security configurations to system components, including servers, applications, operating systems, databases, and security and network devices.
- The finding on hardening is an eye opener because, until now, the top three controls brought up by most insurers have been endpoint detection and response (EDR), multifactor authentication (MFA), and privileged access management (PAM).
- Long a staple among cybersecurity tools and recommendations, we found that MFA has a strong positive impact only when implemented fully. Companies that fail to use MFA broadly across their organization run a greater risk of experiencing a successful cyberattack, showing the importance of using a defense-in-depth approach to cybersecurity.
- The key controls that were least likely to be implemented were EPM tools and patching high severity vulnerabilities within seven days. This held true across the select industries evaluated.

Introduction

As cyberattacks and related insurance claims continue to grow, insurers are increasingly selective about underwriting cyber risk. The adoption of certain cybersecurity controls is now a minimum requirement of insurers, with favorable policy pricing, terms, and conditions — and even an organization's insurability — potentially at stake.

The use of certain cyber controls can help organizations positively differentiate their cyber risk management to insurers. However, while a variety of cybersecurity controls have been established for years as best practices, many companies are unsure which to adopt, or have been slow to do so.

Prioritizing which controls to deploy can help inform how your organization allocates limited budgets, ensuring that resources go where they will provide effective protection.

So the strategic question becomes: How can we decide which cyber controls to put in place?

As with many strategy decisions in an increasingly digital world, innovative use of data is a critical part of the solution. In this study, we show how data can help identify which cyber controls may lower the probability of a company experiencing a cyber event.

Marsh key controls

Beginning in 2019, the frequency and severity of ransomware attacks increased to an extent that it impacted the pricing and availability of cyber insurance coverage and the terms and conditions insurers offered. Some organizations found it difficult, and in some cases nearly impossible, to purchase insurance coverage.

Specialists at Marsh identified 12 specific cyber controls that organizations should focus on. Businesses that were found to be deficient in any of these controls ran an increased risk of being denied coverage. The identified cybersecurity controls are now a minimum requirement of cyber insurers, with organizations' potential insurability, pricing, and scope of coverage at stake. Overall, organizations now emphasize such controls to help mitigate risks and improve their cybersecurity position and resilience.

However, while these controls have been established for years as critical to maintaining cyber resilience, many organizations have been slow to adopt some of them, for a variety of reasons. For example, certain controls can be expensive to put in place, and with limited budgets it can be hard to know which to invest in. An effective way to prioritize is to identify those controls that have been shown to lower the probability of a company experiencing a cyber event.

12 Marsh key cybersecurity controls

- **Multifactor authentication (MFA)**
- **Endpoint detection and response (EDR)**
- **Secured, encrypted, and tested backups**
- **Privileged access management (PAM)**
- **Email filtering and web security**
- **Patch management and vulnerability management**
- **Cyber incident response planning and testing**
- **Cybersecurity awareness training and phishing testing**
- **Hardening techniques, including remote desktop protocol (RDP) mitigation**
- **Logging and monitoring/network protections**
- **End-of-life systems replaced or protected**
- **Vendor/digital supply chain risk management**

Datasets help outline cybersecurity posture

Marsh McLennan has a proprietary database, referred to as the Marsh Cyber Self-Assessment (CSA), composed of hundreds of questions and responses from individual organizations. When analyzed, they help describe an organization's cybersecurity posture. The questions in the CSA focus on the 12 key controls areas, along with other relevant facets of an organization's cybersecurity posture.

Additionally, Marsh McLennan maintains a proprietary historical cyber event dataset made up of our US-based claims. This database includes events dating back to 2010, and consists both of claims events that resulted in a cyber claim being paid, and notices of circumstances which did not cause an insured loss. When analyzed together, the two datasets provide powerful insights into which cybersecurity controls have the greatest effect on decreasing the likelihood of an organization experiencing a cyber event.

To focus this study, we only considered Marsh key control categories that would have a large impact on the frequency of a successful cyber event, as opposed to the severity of an event. These categories are:

Multifactor authentication (MFA)

Patch management and vulnerability management

Email filtering and web security

Privileged access management (PAM)

Endpoint detection and response (EDR)

Logging and monitoring/ network protections

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

End-of-life systems replaced or protected

Calculating signal strength helps to prioritize controls

Most of the questions in these categories were binary, allowing either a "yes" or "no" response. Where this wasn't the case, we adjusted the data to make them align.[1]

The company responses to the CSA were combined with a year of historical claims data from November 2020 to November 2021. Note that as threats and cybersecurity best practices evolve over time, the questions and potential responses in the Marsh CSA also evolve. This study includes the cybersecurity best practices at the time of the claims events.

Once all responses were in the yes/no format, we calculated signal strength. For each question, we calculated the conditional probability (that is, the likelihood of an event occurring) of experiencing a cyber claim or notice of circumstance, given that an organization did not implement the control. Additionally, we calculated the conditional probability of experiencing a cyber claim or notice of circumstance when an organization did implement the control. Each control was considered in isolation, irrespective of other controls a company may or may not have implemented. Therefore, these factors cannot be considered multiplicative, as the controls are correlated in actual practice.

The "signal strength" was then expressed as the ratio of the conditional probability given a "no" response to the conditional probability given a "yes" response. A signal strength above one indicates that the control in question decreases the probability of a cyber event. The higher the signal strength, the greater the impact the control has on decreasing the likelihood of an event, meaning the signal strength is a strong indicator of controls that should be prioritized. (Note that since each control is considered separately, the signal strengths are not additive.)

[1] The responses to some questions were picked from a dropdown menu, such as a total percentage of endpoints affected or a timeframe in which a patch was applied. For these, a minimum value was identified below which an organization's answer was categorized as "no." For example, in one of the device management questions the minimum company response to be classified as a "yes" was 75% to 100%. Responses below this value were categorized as "no." Questions with a free-field (open) response type were not included in the study.

The higher the signal strength, the greater the impact the control has on decreasing the likelihood of an event.

Identifying correlations between cyber controls and cyber events

By looking at each question in the CSA and its correlation with cyber events, we identified those cybersecurity controls that had the largest impact on a company's probability of experiencing a cyber event (see Figure 1).

The question with the largest signal strength — and thus the largest effect on cybersecurity — relates to hardening techniques. Hardening is the best practice of applying baseline security configurations to system components, including servers, applications, operating systems, databases, and security and network devices. Without these hardening processes, bad actors are able to exploit weak default device settings or misconfigurations, making hardening a critical part of cybersecurity.

Many of these highly ranked cybersecurity controls come as little surprise. For example, hardening techniques and patching your network in a timely fashion are critical to preventing successful cyberattacks. However, it is a significant finding to see how strong an impact hardening has on cybersecurity.

The value in assigning a signal strength is to help a company identify which of the controls recommended by cybersecurity experts to prioritize when deciding how best to build and maintain a resilient system.

There were some questions that did not rank highly in this list of individual cybersecurity controls. For instance, multifactor authentication (MFA) has long been considered an important cybersecurity control, and is identified as one of the highest priority of the 12 Marsh key controls. So why is it not in the list of top controls in Figure 1?

To answer this question, we looked in more depth at how organizations implement controls. After all, it makes sense that using MFA in only limited cases is not sufficient; it should be in place for all critical and sensitive data, for all remote login access, and for administrator account access. Therefore, we looked at organizational responses to multiple related questions that involved MFA to see how they change the likelihood that an organization experienced a claims event (see Figure 2).

Taken individually, no single question involving MFA has a strong signal that would indicate a lower probability of a claims event if an organization were to implement the control in isolation. For example, if a company only required MFA for administrative access to accounts, the signal strength was below one, meaning it had no discernible effect on the success of a cyberattack.

However, when an organization implements MFA in a broad and robust manner — indicated by a "yes" response to all three of the MFA controls questions — their probability of experiencing a claims event is 1.4 times lower than an organization that has not implemented these MFA controls.

This result illustrates the importance of using a defense-in-depth approach to cybersecurity. Implementing MFA in a broad manner, across a company's attack surface, does more to increase cybersecurity posture than implementing MFA in a haphazard manner.

01| Marsh key controls with strongest effect related to experiencing a cyber event

Marsh key control category	Question*	Signal strength
Hardening techniques	Our system configuration management tools (such as, active directory group policy) enforce and redeploy configuration settings to systems.	5.58
Privileged access management	The organization manages desktop/local administrator privileges via endpoint privilege management (EPM).	2.92
Endpoint detection and response	The organization operates the following information technology (IT) and information/cybersecurity tools and capabilities: Advanced endpoint security[1].	2.23
Logging and monitoring	The organization operates its own security operations center (SOC) and/or has an outsourced managed security service provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds b) Security incident and event management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software	2.19
Patched systems	The organization's target timeframe to patch common vulnerability scoring system (CVSS) v3 high severity 7.0-8.9 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	2.19
Cybersecurity training	The organization conducts internal phishing campaigns at least annually.	1.76
Endpoint detection and response	The organization operates the following IT and information/cybersecurity tools and capabilities: Network intrusion detection/prevention systems (IDPS).	1.67
Patched systems	The organization's target timeframe to patch common vulnerability scoring system (CVSS) v3 critical severity 9.0-10.0 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	1.57
Email filtering	The organization implements the following malware protections: Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.	1.56
Logging and monitoring	In addition to the capabilities above, the SOC/MSSP capabilities include, but are not limited to, the following: a) 24x7 operations b) Mix of signature and heuristic-based detection c) Incident response, containment, and remediation capabilities d) Active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures e) Processes are continuously improved	1.56

* Questions are drawn from the Marsh CSA.

[1] Cybersecurity best practices have evolved since the time period of the cyber incidents, with managed detection and response (MDR) and extended detection and response (XDR) superseding earlier EDR tools such as advanced endpoint security (AES)

02| Broad implementation of MFA positively impacts cybersecurity outcomes

Question*	Question signal strength	Group signal strength
We require multifactor authentication (including smart cards, certificates, one time password (OTP) tokens, or biometrics) for all remote login access to the corporate network (for example, virtual private network (VPN), remote desktop protocol (RDP), and other secure remote access).	1.25	1.44
Irrespective of a user's location, we require multifactor authentication and encrypted channels for all administrative account access.	0.85	
In addition to the capabilities listed above, irrespective of a user's location, we require multifactor authentication for access to our most critical or sensitive data or systems.	0.84	

* Questions are drawn from the Marsh CSA.

Implementation rates allow for peer comparisons

We identified controls that are important to a company in maintaining a good cybersecurity posture. However, insurers often want to understand how a company compares to its peers before taking on a risk. Knowing which controls are either widely adopted by industry peers, or conversely which have not been widely adopted, can help a company identify controls that could potentially make them a more attractive risk to insurers.

Figure 3 shows the implementation rates for the top 10 cyber controls for their impact on an organization's probability of experiencing a cyber event. It's encouraging to see the high implementation rate for hardening techniques that enforce and redeploy configuration settings.

Failing to implement controls that are widely adopted by industry peers could make a company less attractive to insurers, especially for those measures with a large impact on the success of a cyberattack. Conversely, adopting a control that has not been adopted by peers could make a company a more attractive risk to insurers.

Consider that patching high severity vulnerabilities within a week of release — which decreases an organization's probability of a cyber event by a factor of two — is implemented by less than a quarter of organizations. By implementing this control, an organization both increases its cybersecurity posture and compares favorably against other companies.

03| Implementation rate of the highest impact Marsh Cyber Self-Assessment controls

Marsh key control category	Question*	Implementation rate
Hardening techniques	Our system configuration management tools (such as, active directory group policy) enforce and redeploy configuration settings to systems.	96%
Cybersecurity training	The organization conducts internal phishing campaigns at least annually.	89%
Endpoint detection and response	The organization operates the following IT and information/cybersecurity tools and capabilities: Network intrusion detection/prevention systems (IDPS).	88%
Logging and monitoring	The organization operates its own security operations center (SOC) and/or has an outsourced managed security service provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds b) Security incident and event management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software	88%
Logging and monitoring	In addition to the capabilities above, the SOC/MSSP capabilities include, but are not limited to, the following: a) 24x7 operations b) Mix of signature and heuristic-based detection c) Incident response, containment, and remediation capabilities d) Active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures e) Processes are continuously improved	85%
Endpoint detection and response	The organization operates the following information technology (IT) and information/cybersecurity tools and capabilities: Advanced endpoint security.[1]	82%
Email filtering	The organization implements the following malware protections: Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.	75%
Patched systems	The organization's target timeframe to patch common vulnerability scoring System (CVSS) v3 critical severity 9.0-10.0 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	53%
Privileged access management	The organization manages desktop/local administrator privileges via endpoint privilege management (EPM).	35%
Patched systems	The organization's target timeframe to patch common vulnerability scoring system (CVSS) v3 high severity 7.0-8.9 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	24%

* Questions are drawn from the Marsh CSA.

[1] Cybersecurity best practices have evolved since the time period of the cyber incidents, with managed detection and response (MDR) and extended detection and response (XDR) superseding earlier EDR tools such as advanced endpoint security (AES)

Comparing implementation rates by industry

While the overall implementation rate is a helpful metric when identifying which controls your company should prioritize, it can also be useful to understand how your company compares to industry peers (see Figure 4).

Some of the most effective controls are widely implemented across industries — such as using network intrusion detection/prevention systems and ensuring system configuration management tools enforce and redeploy configuration settings. However, we did find significant differences between industries.

For example, the education industry tends to lag behind organizations in other industries with the wide implementation of some of the individual controls. This results in the average incident rate within the education industry being significantly higher than it is in the other industries we looked at (see Figure 5).

While controls are, of course, deployed at the organizational level, understanding an industry’s overall implementation and incident rates can help flag areas of potential concern for decision makers.

04| Implementation rate of the highest impact Marsh Cyber Self-Assessment controls, for select industries

Marsh key control category	Question*	Industry response rate			
		Manufacturing	Education	Retail and wholesale trade	Professional, scientific, and technical services
Hardening techniques	Our system configuration management tools (such as, active directory group policy) enforce and redeploy configuration settings to systems.	99%	95%	93%	93%
Cybersecurity training	The organization conducts internal phishing campaigns at least annually.	91%	74%	85%	88%
Endpoint detection and response	The organization operates the following IT and information/cybersecurity tools and capabilities: Network intrusion detection/prevention systems (IDPS).	87%	93%	83%	79%
Logging and monitoring	The organization operates its own security operations center (SOC) and/or has an outsourced managed security service provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds b) Security incident and event management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software	87%	80%	89%	87%
Logging and monitoring	In addition to the capabilities above, the SOC/MSSP capabilities include, but are not limited to, the following: a) 24x7 operations b) Mix of signature and heuristic-based detection c) Incident response, containment, and remediation capabilities d) Active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures e) Processes are continuously improved	84%	75%	85%	82%

Marsh key control category	Question*	Industry response rate			
Endpoint detection and response	The organization operates the following information technology (IT) and information/cybersecurity tools and capabilities: Advanced endpoint security.	83%	63%	79%	78%
Email filtering	The organization implements the following malware protections: Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.	78%	68%	80%	66%
Patched systems	The organization's target timeframe to patch common vulnerability scoring System (CVSS) v3 critical severity 9.0-10.0 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	54%	47%	44%	57%
Privileged access management	The organization manages desktop/local administrator privileges via endpoint privilege management (EPM).	35%	16%	43%	33%
Patched systems	The organization's target timeframe to patch common vulnerability scoring system (CVSS) v3 high severity 7.0-8.9 vulnerabilities across your enterprise is: Minimum of within 7 calendar days of release.	22%	25%	26%	24%

* Questions are drawn from the Marsh CSA.

06| Cyber event incident rates for Nov 2020 – Nov 2021

Industry	Incident rate
All industries	9.6%
Manufacturing	7.0%
Education	18.8%
Retail and wholesale trade	8.5%
Professional, scientific, and technical services	7.7%

Conclusion

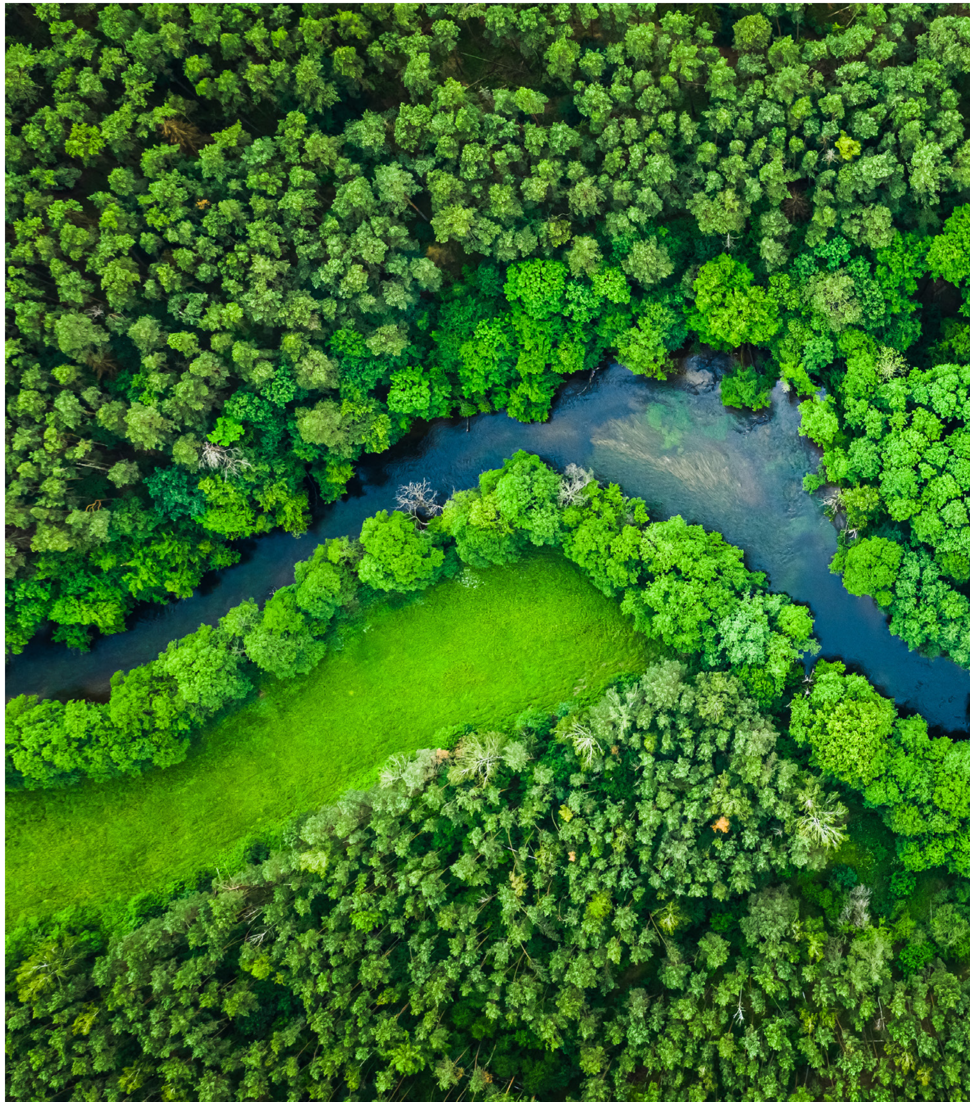
Ensuring a robust cybersecurity posture can seem daunting, especially as threats, best practices, and available solutions evolve. Identifying which controls to prioritize, and how best to implement them, can be confusing, as illustrated above with the use of MFA.

However, using the Marsh 12 key controls as an example, this study shows how data analysis can help to clarify the relative importance of various measures both in protecting a company and in cyber insurance underwriting and purchasing.

Results from studies like this one can help you model a return on investment for implementing various controls and prioritize which to implement. Underwriters can use such results to understand a potential insured's cybersecurity posture and risks.

At Marsh McLennan, these results are being used as part of a larger cyber event loss model, the forthcoming Marsh McLennan Cyber Attritional Loss Model (CALM™), informing the potential losses an organization could suffer and the potential savings benefit from increasing the insured's cybersecurity posture.

For more information, reach out to your Marsh, Guy Carpenter, or other Marsh McLennan representative.



About Marsh McLennan

Marsh McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's more than 85,000 colleagues advise clients in 130 countries. With annual revenue of over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit marshmclennan.com, follow us on LinkedIn and Twitter.

This report may not be sold, reproduced or redistributed, in whole or in part, without the prior written permission of Marsh McLennan, Inc. This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could bematerially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report.

We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.

MA23-16256 1042111188