MARSH

MARSH REPORT | October 2015

International Business Resilience Survey 2015

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

CONTENTS

INTRODUCTION

Using its knowledge and information about business resilience, Marsh Risk Consulting has undertaken an in-depth study in collaboration with DRII (Disaster Recovery Institute International) about organizations' attitudes toward business risks and the processes they have in place. The benchmarking data in this report was collected from nearly 200 C-suite executives, risk professionals, and business continuity managers from large and medium-sized corporations internationally.

BOARDROOM DISCUSSION

79%

of respondents selected reputational damage from a sensitive data breach as the most likely and high-impact risk.

28%

of CEOs stated they have dedicated insurance coverage against cyber-attacks while only 6% of risk managers stated that they have.

73%

of respondents identified lack of crisis management planning as the area with the greatest potential impact on reputation.

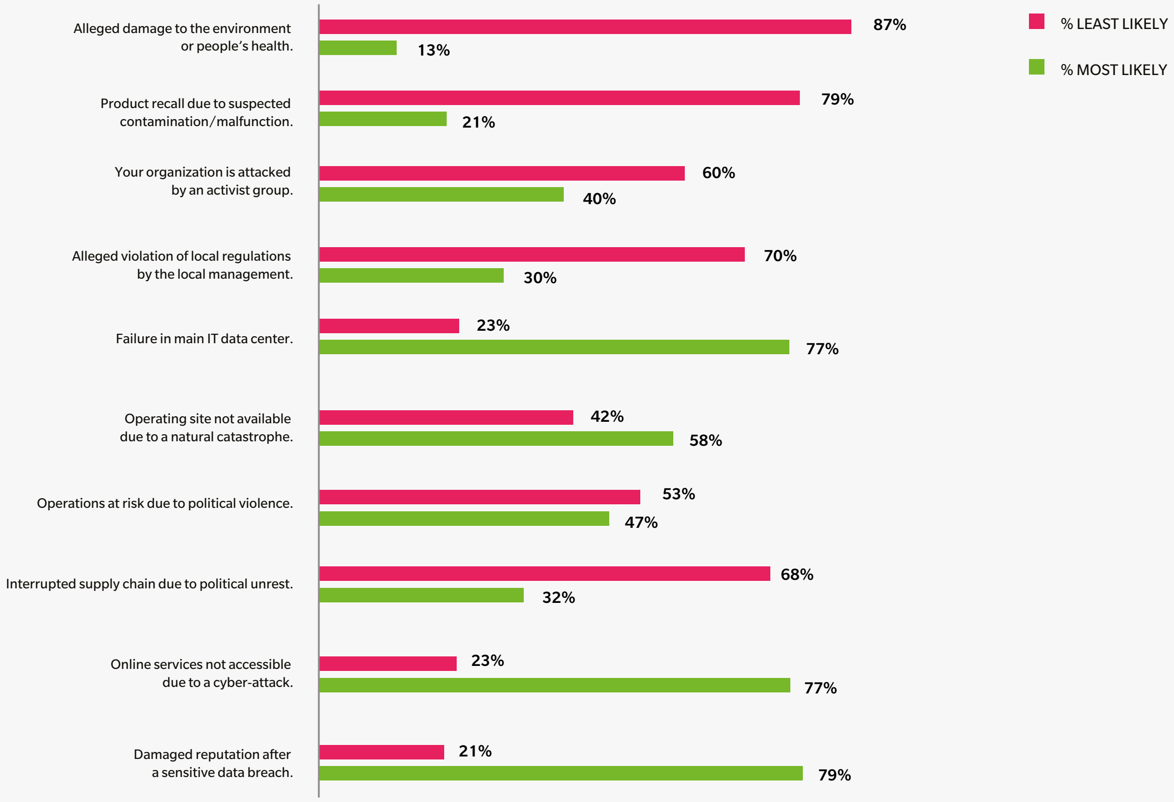
NON-TRADITIONAL RISKS TOP CONCERNS, BOTH IN TERMS OF LIKELIHOOD AND IMPACT

Considerable attention continues to be given to cyber risk – both in media rooms and boardrooms – across Europe, following a recent string of high-profile attacks on organizations.

Perhaps in light of this, respondents to the International Business Resilience Survey 2015 believe that cyber and IT-related events are those most likely to affect their organizations (SEE FIGURE 1) and have the greatest impact (SEE FIGURE 2) on organizational resiliency. Respondents appear to be 'comfortable' with the more traditional risks, such as business interruption (BI) and political risk, for example, which received the lowest percentage of responses both in terms of likelihood and impact. This doesn't seem to be the case for non-traditional risks, with cyber in particular giving risk managers and CEOs the greatest cause for concern. In terms of preparedness, the majority of organizations believe themselves to be better positioned to deal with traditional as opposed to non-traditional risks (SEE FIGURE 3).

FIGURE 1 **Based on your experience, please select three of the following scenarios that are most likely to happen and the 3 scenarios that are least likely to happen in your organization.**

Source: International Business Resilience Survey 2015



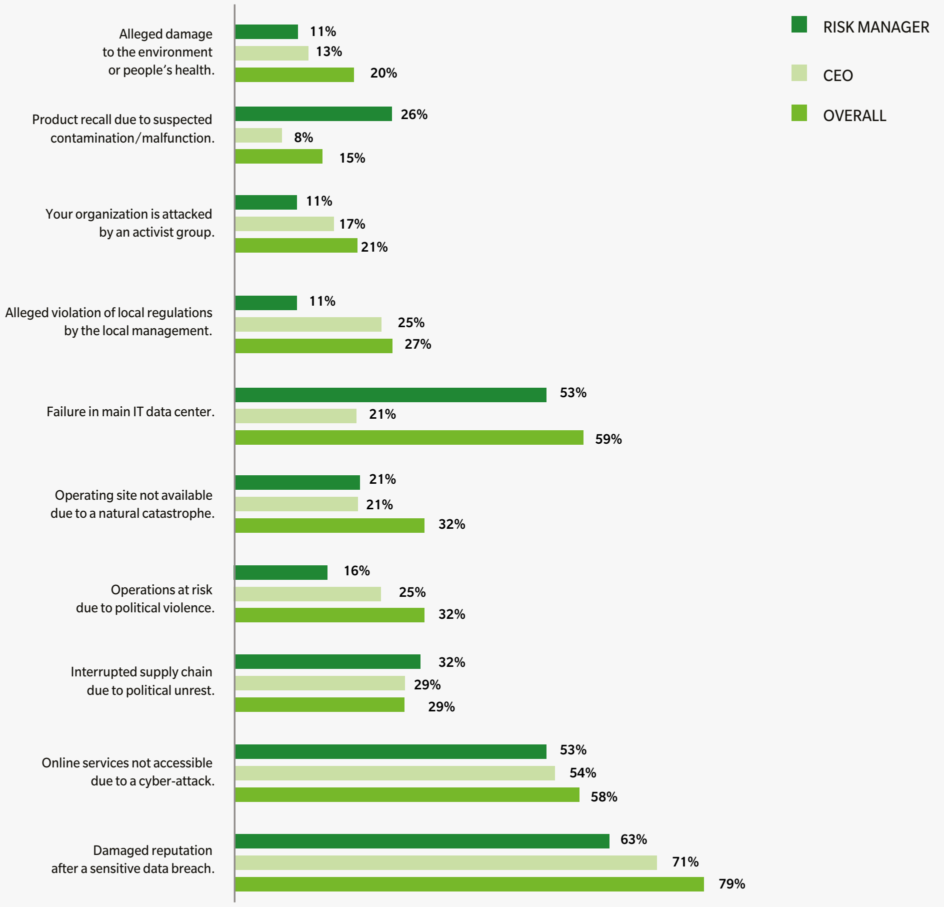
Organizations should review existing business continuity and crisis management frameworks to ensure they are properly addressing emerging, as well as traditional, risks.

Those companies that haven't already should undertake a comprehensive review of their cyber exposures to ensure that resilience is built into those areas that need it most.
In addition, firms should review the dependencies of critical services and processes from internal and third-party information systems and IT technologies.

Also worthy of note is that CEOs are more concerned than risk managers about reputational and regulatory risks, which is perhaps indicative of a different perception and/or concern about longer-term issues. In fact, when asked about events they consider least likely to happen, there is a disconnect between risk managers, who mention violation of local regulations, and CEOs, who say it is the one of the risks that is most likely to happen.

The majority of organizations believe they are better positioned to deal with traditional than non-traditional risks.

FIGURE 2 **Based on your experience, please select three of the following scenarios with the highest impact on your organization's resilience.***
Source: International Business Resilience Survey 2015



*RESULTS DISPLAYED ILLUSTRATE THE PERCENTAGE OF RESPONDENTS, NOT THE PERCENTAGE OF RESPONSES

FIGURE 3 Based on your experience, please rate your organization's resilience to the following risk scenarios.*
Source: International Business Resilience Survey 2015

	OVERALL			CEO			RISK MANAGER		
	High resilience	Medium resilience	Low resilience	High resilience	Medium resilience	Low resilience	High resilience	Medium resilience	Low resilience
DAMAGED REPUTATION AFTER A SENSITIVE DATA BREACH.	35%	53%	13%	25%	54%	21%	28%	61%	11%
ONLINE SERVICES NOT ACCESSIBLE DUE TO A CYBER- ATTACK .	39%	44%	17%	29%	67%	4%	44%	39%	17%
INTERRUPTED SUPPLY CHAIN DUE TO POLITICAL UNREST.	25%	50%	26%	29%	46%	25%	28%	56%	17%
OPERATIONS AT RISK DUE TO POLITICAL VIOLENCE.	33%	35%	32%	33%	33%	33%	33%	39%	28%
OPERATING SITE NOT AVAILABLE DUE TO A NATURAL CATASTROPHE.	40%	43%	17%	50%	29%	21%	39%	56%	6%
FAILURE IN A MAIN IT DATA CENTER.	44%	42%	15%	29%	46%	25%	50%	44%	6%
ALLEGED VIOLATION OF LOCAL REGULATIONS BY THE LOCAL MANAGEMENT.	29%	43%	28%	17%	42%	41%	28%	50%	22%
YOUR ORGANIZATION IS ATTACKED BY AN ACTIVIST GROUP.	27%	41%	32%	26%	30%	44%	28%	56%	17%
PRODUCT RECALL DUE TO SUSPECTED CONTAMINATION/ MALFUNCTION.	33%	37%	30%	41%	33%	25%	17%	67%	17%
ALLEGED DAMAGE TO THE ENVIRONMENT OR PEOPLE'S HEALTH.	39%	32%	29%	33%	33%	33%	39%	39%	22%

*RESULTS DISPLAYED ILLUSTRATE THE PERCENTAGE OF RESPONDENTS, NOT THE PERCENTAGE OF RESPONSES.

Risk managers believe the violation of local regulations is the least likely risk scenario to happen to their organizations (82%), while 77% of CEOs state that it is the most likely to occur.

INSURANCE TAKE-UP FOR NON-TRADITIONAL RISKS REMAINS LOW, BUT PRODUCT INNOVATION MEANS THAT NOW MAY BE THE TIME FOR MANY TO REVISIT EMERGING COVERAGES

In keeping with the theme of the first section of this report, respondents' organizations appear to be better prepared against traditional risks and have, or plan to have, greater levels of insurance cover in place to protect against these types of events.

Generally speaking, there appears to be a confidence rating of between 11% and 26% that there is cover against the scenarios identified in FIGURE 4.

This is relatively consistent with other insurance surveys conducted by Marsh and by insurers. However, for cyber risks in particular, the level of insurance take-up appears low when compared with the criticality with which the risk is viewed.

According to the survey results, CEOs overestimate their levels of protection for the risks they consider to be the most likely and high-impact: 28% say they have dedicated insurance coverage against cyber-attacks, and 21% state they have dedicated insurance protection for reputation damage after a data breach. However, only 6% of risk managers say they have dedicated coverage for these two risks.

FIGURE 4 **Please indicate if the following risk scenarios are covered by your organization's insurance program.**
Source: International Business Resilience Survey 2015

	YES	YES, AND WE HAVE A DEDICATED COVERAGE	NO, BUT WE PLAN TO HAVE IT IN THE NEXT 2 YEARS	NO	DON'T KNOW
DAMAGED REPUTATION AFTER A SENSITIVE DATA BREACH.	17,5 %	20%	3%	30,5%	29%
ONLINE SERVICES NOT ACCESSIBLE DUE TO A CYBER- ATTACK .	13%	23%	8%	30%	26%
INTERRUPTED SUPPLY CHAIN DUE TO POLITICAL UNREST.	15%	20%	4%	30%	31%
OPERATIONS AT RISK DUE TO POLITICAL VIOLENCE.	10%	16%	5%	41%	27%
OPERATING SITE NOT AVAILABLE DUE TO A NATURAL CATASTROPHE.	18%	25%	6%	21%	30%
FAILURE IN A MAIN IT DATA CENTER.	19%	26%	6%	23%	26%
ALLEGED VIOLATION OF LOCAL REGULATIONS BY THE LOCAL MANAGEMENT.	11%	16%	6%	36%	31%
YOUR ORGANIZATION IS ATTACKED BY AN ACTIVIST GROUP.	9%	11%	10%	39%	32%
PRODUCT RECALL DUE TO SUSPECTED CONTAMINATION/MALFUNCTION.	13%	19%	4%	41%	23%
ALLEGED DAMAGE TO THE ENVIRONMENT OR PEOPLE'S HEALTH.	15%	18%	5%	30%	32%

IT SYSTEMS CONSIDERED CRUCIAL TO OPERATIONS AND REPUTATION

The resiliency of IT systems is considered to be the most important factor in meeting business goals (SEE FIGURE 5). Additionally, respondents believe the failure of IT systems to be one of the two areas with potentially the greatest impact on reputation, along with lack of crisis management planning.

This is perhaps unsurprising in the modern age where the computers, email, and the internet are all so integral to organizations operating across virtually all industry sectors, and is backed up by the importance placed on the analysis and implementation of control procedures for the resiliency of IT systems (SEE FIGURE 6).

It is interesting to note that CEOs place less importance on the resiliency of IT systems in relation to reputation management, while giving greater attention to crisis management planning.
Firms should consider including a comprehensive review of the dependencies of critical IT services and processes in their crisis management plans, and the results of this should be relayed to the C-suite.

Safety at work also scored highly, along with business continuity management and crisis management planning.

FIGURE 5 **To meet business goals, the following are crucial for my organization (from 1 ‘totally disagree’ to 5 ‘totally agree’).***
Source: International Business Resilience Survey 2015

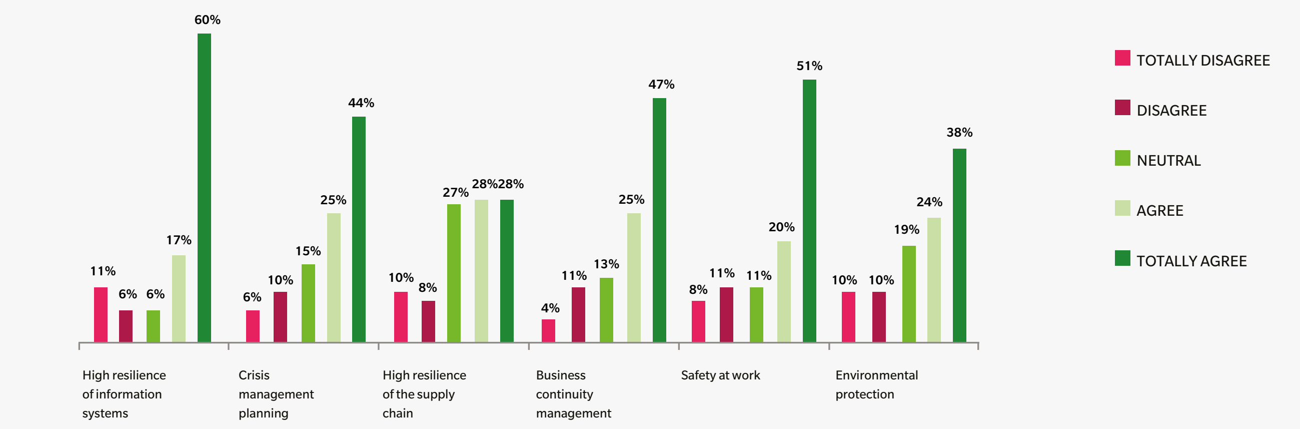
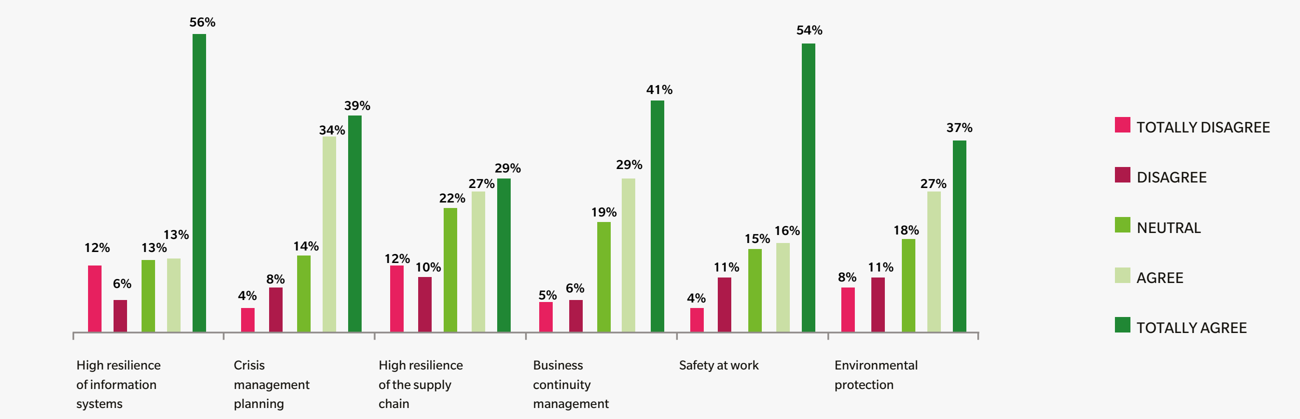


FIGURE 6 **Failure in managing the following can have a significant impact on the reputation of my organization (from 1 ‘totally disagree’ to 5 ‘totally agree’).***
Source: International Business Resilience Survey 2015



*RESULTS DISPLAYED ILLUSTRATE THE PERCENTAGE OF RESPONDENTS, NOT THE PERCENTAGE OF RESPONSES.

CURRENT AND PLANNED INVESTMENT IN IT SYSTEMS IS HIGH, BUT MORE WORK STILL TO BE DONE

The importance of IT resiliency is underlined by the responses to FIGURE 7, which reveal that 66% of respondents believe they are currently investing enough in IT, or plan to increase investment in the next three years. Just 18% say they are not currently investing enough, a figure which was only bettered by safety at work, which received 15% of the vote.

Perhaps even more interesting is the finding that 29% of respondents would chose to invest in IT system failure prevention if they could only invest in one particular area – nearly twice as much as the second-highest choice which is "Data breach prevention/mitigation".

It is clear then that systems failure is considered to be a much greater concern than external cyber threats. Bearing this in mind, organizations should perform periodic assessments of all operational risk scenarios that could affect their resilience in order to prioritize risk mitigation actions in accordance with their potential business impacts.

The protection of intellectual property was listed second by CEOs with 25%; however, it received far fewer votes from other respondents (just 10% overall), suggesting the risk is being underestimated by the majority of individuals.

FIGURE 7
Please indicate the correct amount of investment by your organization in the resilience of IT systems.
Source: International Business Resilience Survey 2015

TOTAL EUROPE

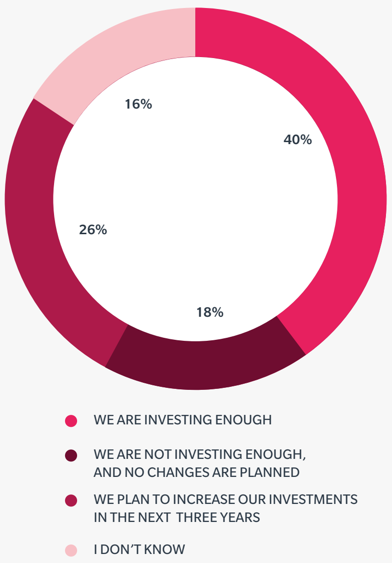
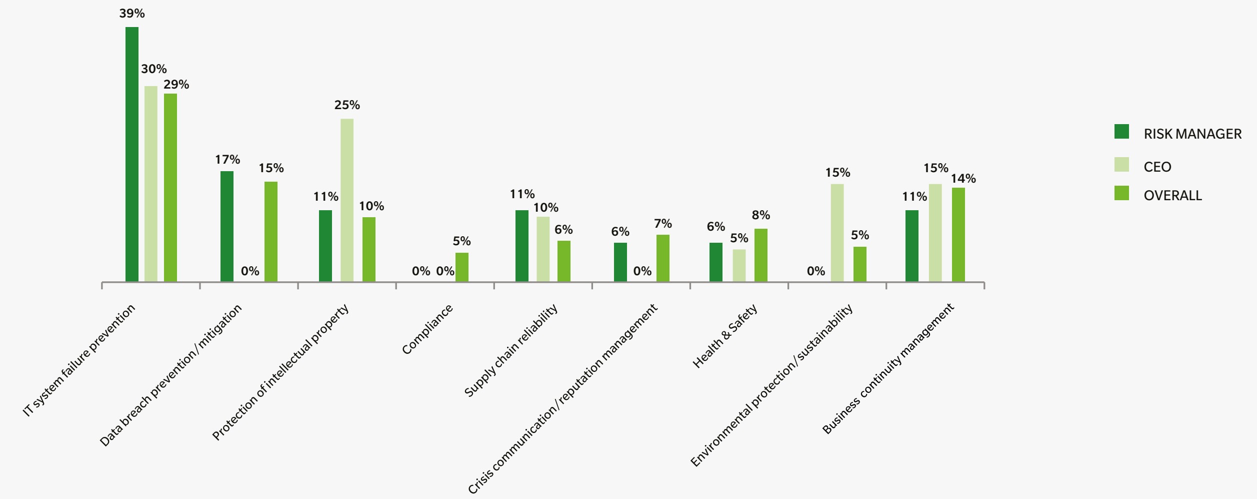


FIGURE 8 **If you could invest in only one of the following areas, which one would you choose?***
Source: International Business Resilience Survey 2015



*RESULTS DISPLAYED ILLUSTRATE THE PERCENTAGE OF RESPONDENTS, NOT THE PERCENTAGE OF RESPONSES.

CONCLUSION

The following are highlights of the key findings from the International Business Resilience Survey Report 2015, along with recommendations from Marsh Risk Consulting:

CYBER AND IT-RELATED RISKS

Cyber and other IT-related risks are considered to be the most likely to occur and those with the potential to cause the greatest impact. The two are also acknowledged for their importance in meeting business goals and reputation management.

Firms should undertake a comprehensive review of their cyber exposures to ensure that resilience is built into those areas where the most benefit can be extracted from each Euro. An enterprise-wide cyber risk control strategy should be designed, headed by a cross-functional cyber risk committee. In addition, firms should undertake a comprehensive review of the dependencies of critical services and processes from information systems and IT technologies. The assessment and the resulting risk mitigation plan should address equally on-premises systems and outsourced ones.

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

The majority of respondents consider business continuity and crisis management to be critical elements of their resilience that need to be adequately established and maintained.

Risk managers should work to identify all cyber and IT-related risk scenarios that could affect their organizations and share the resulting risk registers with senior management.

Those organizations that don't already should review existing business continuity and crisis management frameworks to ensure they are properly addressing emerging risks; in particular, data breach scenarios and the resilience of IT systems. The availability of a cyber crisis management plan is of paramount importance to secure organizations' reputations.

PERCEPTION VERSUS REALITY

Some in the C-suite take it for granted that their organizations have specific insurance cover for cyber and IT-related risks. On the contrary, despite an increase in the take-up of new specific cyber policies globally, overall penetration remains low. Additionally, risk managers, risk owners, and CEOs all have different perceptions about the severity of the risk scenarios affecting their organizations and the adequacy of the control measures in place.

Organizations should perform periodic assessments of all operational risk scenarios that could affect their resilience in order to prioritize risk mitigation actions in accordance with their potential business impacts.

About Marsh

Marsh is a global leader in insurance broking and risk management. We help clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 27,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global team of professional services companies offering clients advice and solutions in the areas of risk, strategy, and people. With 57,000 employees worldwide and annual revenue exceeding $13 billion, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting.

MARSH IS ONE OF THE MARSH & McLENNAN COMPANIES, TOGETHER WITH
GUY CARPENTER, MERCER, AND OLIVER WYMAN.

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. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority. Marsh Ltd, trading as Marsh Ireland is authorised by the Financial Conduct Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.