

GLOBAL CYBER RISK PERCEPTION SURVEY

FEBRUARY 2018

By the Numbers: Global Cyber Risk Perception Survey



By the Numbers: Global Cyber Risk Perception Survey

CONTENTS

- 1 Introduction
- 2 As Technology Spreads, Cyber Risk Management Becomes a Top Priority
- 6 Executives Worry Most About Financially Motivated Attackers
- 8 Cyber Risk Management Requires a Comprehensive Approach
- 10 Recognizing the Threat, Organizations Invest in Cybersecurity Actions
- 12 Better Quantifying Cyber Exposure Will Help Determine Risk Finance Needs
- 14 Industry, Government, and Cybersecurity Effectiveness
- 16 Survey Demographics

Introduction



In the last four decades, the world has experienced an enormous shift in where value lies. Consider that in 1975, just 17% of the market value of S&P 500 companies was tied to intangible assets, including data, intellectual property, and other technologies¹. The bulk of their value was in physical assets. Today, the numbers have reversed: Just 16% of value is in physical assets; the rest comes from intangibles. That shift has been facilitated by, among other things, advances in computer processing, cloud computing, sensors, software, and ever-smarter devices.

This broad reliance on data and information extends to all companies — from automakers and aerospace giants to financial institutions and retail chains. As a result, organizations of all sizes and across all industries are vulnerable to cyber-attacks. And the threats are increasing not only in frequency, but are becoming more severe, diverse and complex, with significant consequences.

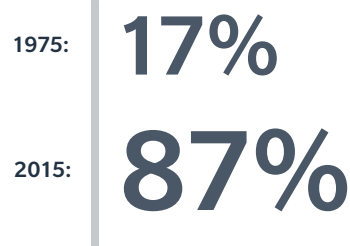
As leaders in our respective industries, Marsh and Microsoft collaborated on this project out of mutual concern regarding

the state of cybersecurity in the global economy, and the knowledge that cyber risk cannot be compartmentalized by industry, company size, or similar measures. We have a shared interest in protecting our customers from these threats, and in identifying, developing, and implementing best practices to help them manage their cyber risk.

This report provides a lens into the current state of cyber risk management at organizations around the world. Our survey captured the views of more than 1,300 risk professionals and other senior executives globally, representing 26 industry sectors. We gathered replies from some of the world's largest companies, small- and medium-sized enterprises, and even a few startups. We heard from CEOs, CFOs, chief technology officers, chief risk officers, corporate directors and others — in fact, more than half of our respondents worked at the C-suite level or board level.

What unites them is their concern about how to navigate their companies in the rapidly changing environment of cyber risk. And if our survey is any indication, it is probably one that you share.

We hope you use this report as a lens into your own organization and its experiences. We encourage organizations to develop resilience as they strive to resolve and mitigate emerging cyber risks in a challenging and evolving technology and threat landscape. We extend our thanks to the many people who answered the survey and shared their perspectives on this important topic.



Percent of S&P 500 companies' market value tied to intangible assets*

*Intangible Asset Market Value Study, 2017, Ocean Tomo, LLC

¹Intangible Asset Market Value Study, 2017, Ocean Tomo, LLC

As Technology Spreads, Cyber Risk Management Becomes a Top Priority

Ubiquitous internet connectivity, massive quantities of digital data, advanced analytical capabilities, and disruptive technologies continue to dramatically change the way business is conducted globally. As digital technologies impact business models — and the rate of change grows unabated — the technological transformation means that all organizations are increasingly vulnerable to cyber threats, and a single incident can inflict serious damage.

The significance of the concern about cybersecurity was reflected in the World Economic Forum's *2018 Global Risks Report*, which places cyber-attacks and massive data fraud among the year's top five risks — the first time two technological risks have been in the top five. The ubiquity of the cyber threat has led to a common mantra among cyber professionals: It's not *if* your organization's systems will be breached, it's *when*. In the *Marsh-Microsoft Cyber Perception Survey*, nearly 20% of respondents said that their organization has been a victim of a successful cyber-attack within the past 12 months. And according to a recent study by Kroll², 85% of executives reported at least one cyber incident in the last 12 months. Notably,

these two surveys report very different assessments of how pervasive cyber-attacks are in the enterprise, and there are a number of potential reasons behind this. Organizations often face challenges in determining whether an attack has occurred, and the evaluation process can take months. In addition to concerns about regulatory or legal action when discussing an attack, organizations also face a certain stigma around incident disclosure.

A successful cyber incident has the potential to disrupt supply chains, shut down core operations, and cause other losses. The financial impact can be severe. Among respondents to the *Marsh-Microsoft Cyber Perception Survey*, nearly one-third of those who said their organization estimates the potential financial costs of a cyber event projected that losses from a worst-case incident could reach into the tens of millions of dollars (see Figure 1). Among companies with over US\$1 billion in revenue, more than 40% of respondents estimated their worst-case financial impact would exceed US\$50 million.



²Kroll Annual Global Fraud and Risk Report 2016/2017

FIGURE
1

Companies of all sizes have started to estimate the financial impact of a cyber event.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

If your organization has estimated the financial impact of a cyber incident, what is the worst potential loss value in US dollars?

■ Losses up to US\$10 million
 ■ Losses US\$10 million to US\$50 million
 ■ Losses US\$50 million to US\$100 million
 ■ Losses above US\$100 million

COMPANY SIZE (REVENUE)

More than US\$1 billion



US\$500 million – US\$1 billion



US\$50 million – US\$500 million



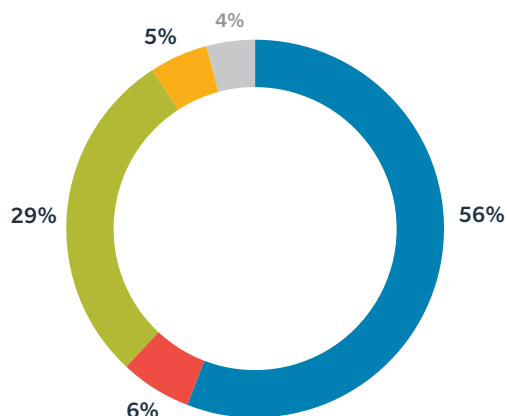
Less than US\$50 million



Most organizations now rank cybersecurity among their highest risk management priorities.

Among my organization's risk management priorities, cyber risk is:

■ A top five risk
 ■ The No. 1 risk
 ■ A risk, but not in the top five
 ■ Low priority
 ■ Don't know



Given the escalation of cyber events and their costs, it is understandable that nearly two-thirds of survey respondents said that cyber risk is among their organization's top five risk management priorities. That is roughly double the percentage who rated cyber that high in a survey Marsh conducted in 2016.

Those respondents whose organizations had been successfully attacked were slightly more likely to prioritize cyber risk than those who had not. Other reasons for the shift include media attention to attacks and corporate losses, an increase in available benchmarking data regarding peers' losses, and pressure from regulators, including those with global implications such as the EU General Data Protection Regulation (GDPR).



Despite the evident concern, however, just one in five respondents said they are highly confident in their organization's ability to manage and mitigate cyber risk or respond and recover from an attack (see Figure 2). This dynamic was pronounced among corporate directors, who have an important role in efforts to protect their organization from cyber threats. Roughly 70% of respondents who identified as board members said they ranked cyber risk as a top five concern, yet only 14% reported that they were "highly confident" in their organization's ability to respond to a cyber-attack.

FIGURE
2

Executives are more confident of organizations' ability to understand and assess cyber risk than of mitigating or responding to it.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

Regarding cyber risk, for each of the following, please indicate your confidence in your organization's ability to:*

- Highly confident
- Fairly confident
- Not at all confident

Identify and assess cyber risk



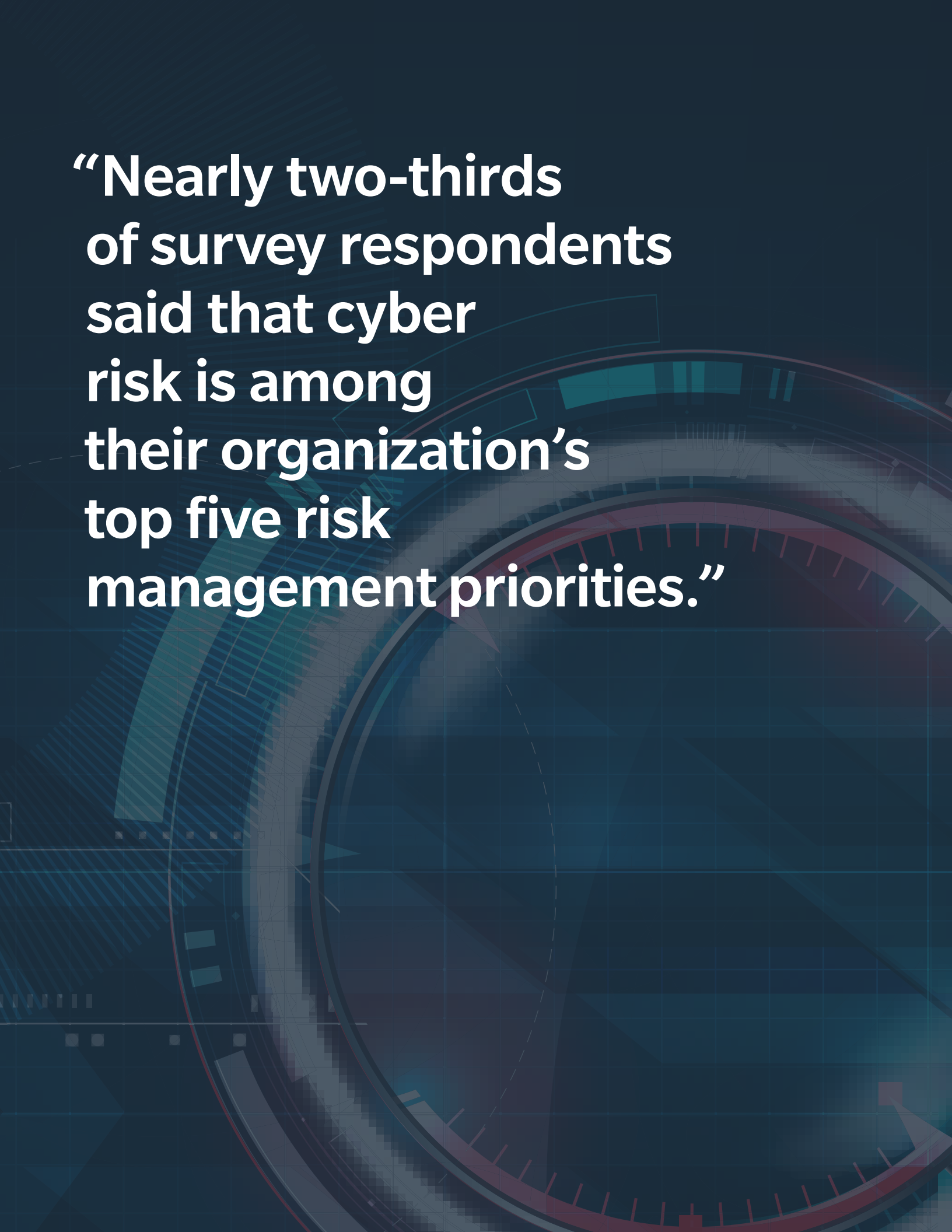
Mitigate and prevent



Respond and recover



*"Don't know" and "other" responses not shown

The background is a dark blue gradient with abstract, futuristic elements. It features several concentric circular arcs and a faint grid pattern, suggesting a digital or technological theme. The text is overlaid on the upper left portion of this background.

**“Nearly two-thirds
of survey respondents
said that cyber
risk is among
their organization’s
top five risk
management priorities.”**

Executives Worry Most About Financially Motivated Attackers

The term “cyber risk” covers a broad range of potential loss exposures. Some of the scenarios that most concern executives are among the hardest to quantify, in part because they require an understanding and analysis of cross-dependencies.

For example, three-quarters of respondents cited business interruption (BI) as one of the most worrisome consequences of a cyber-attack, and nearly 30% cited the potentially related disruption to their industrial systems or operational technology (see Figure 3). While the cost of a breach of personal information can be estimated based on historical data, cyber BI costs are more difficult to project because they depend on such factors as the sophistication of the attack, the organization’s business model, the level of planning and investment made before the attack, and its response. Additionally, the type of technology in use plays a role. New systems and legacy systems, for example, often present different security challenges because of different architectures and platforms, coding practices, and operational requirements.

The second-most cited concern — reputational damage — is also difficult to quantify. In an era in which increasingly sophisticated attacks are likely, how an organization responds is subject to intense public scrutiny. Companies that can manage events effectively will be better able to contain the reputational fallout.

Underpinning executives’ concerns about losses are the attackers and their motivations. Survey respondents were predominantly worried about financially motivated attackers (see Figure 4). That’s understandable, but in today’s world, cyber-attacks may be perpetrated by a broad range of actors, including those backed by nation-states with deep

resources and strong political motivations. An attack need not be solely financially motivated to trigger significant economic consequences.

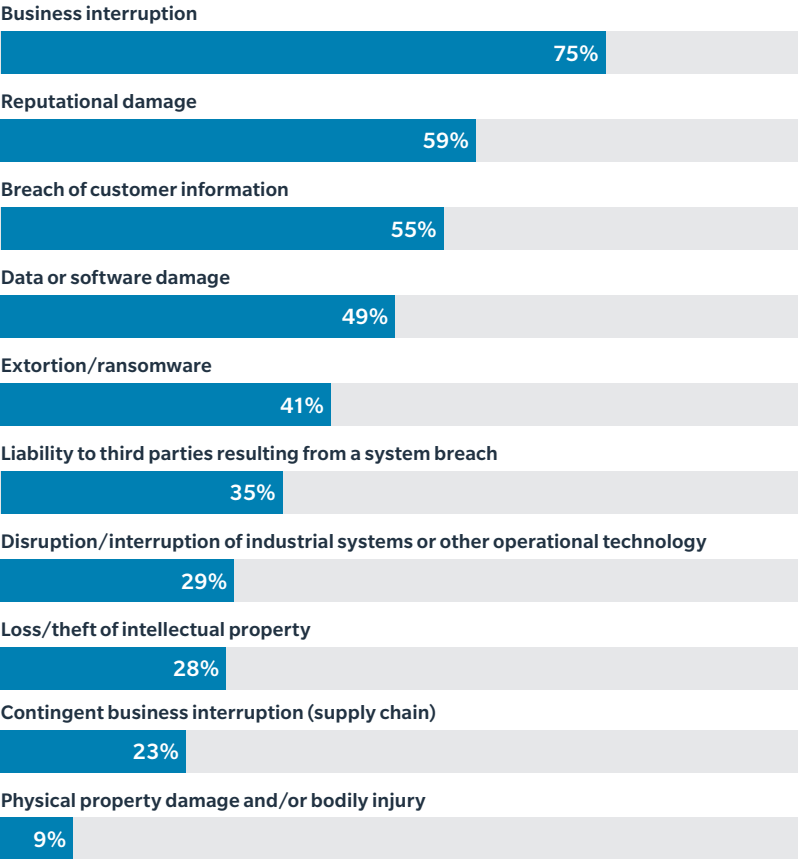
Barely 6% of survey respondents cited nation-state actions as a major source of concern. Distinguishing between nation-state attacks and financially

FIGURE
3

Business interruption seen as having the greatest potential impact from a cyber event.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

Which cyber loss scenarios present the greatest potential impact to your organization?*



*More than one response allowed

FIGURE
4

Financially motivated threat actors drive executives' concerns.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

With regard to a cyber-attack that delivers destructive malware, which threat actor concerns you the most?

Financially motivated threat such as organized crime and/or hacktivist groups

41%

Human error, such as employee loss of mobile device

16%

A malicious, rogue employee and/or contractor

15%

A third party with authorized access to your IT resources

11%

Operational error

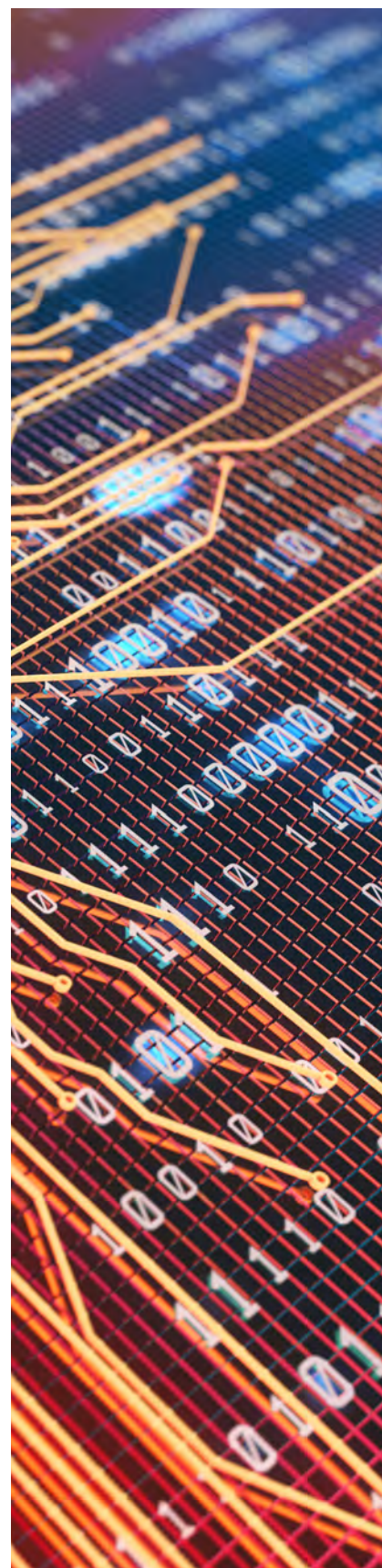
11%

Politically motivated threat, such as state-sponsored attacks or their proxies

6%

motivated ones can be difficult as the observable results may be the same. WannaCry and NotPetya are examples of what organizations now face: nation-state malware — or pieces of it — used by malicious actors to perpetrate attacks that can interrupt enterprise operations globally and cost companies millions. These two ransomware attacks affected organizations in more than 150 countries, prompting BI and other losses estimated at well over US\$200 million by some companies, brought reputational damage, and resulted in loss of customer data.

One actionable lesson from these ransomware attacks is that basic cyber hygiene measures can truly improve cyber risk management. Both WannaCry and NotPetya relied upon vulnerabilities that had been remedied through software patches. As cybercriminals become ever-more sophisticated, there is simply no way for organizations to protect themselves against threats unless they update their systems. Without continuous cyber hygiene, organizations are fighting the problems of the present with tools from the past. Indeed, information technology basics, such as keeping computers current and patched, are a high responsibility for everyone, and should be supported by every top executive.



Cyber Risk Management Requires a Comprehensive Approach

Technology dependence, new types of attacks, and the potential for major financial loss mean the structure of cyber risk oversight and responsibility has grown in importance. In turn, this has challenged organizations to evolve their structures and practices for cyber risk management. The conventional view was that cyber risk was a technology concern, and as a result, most organizations relied primarily on IT staff to address threats, with prevention of attacks as the driving goal.

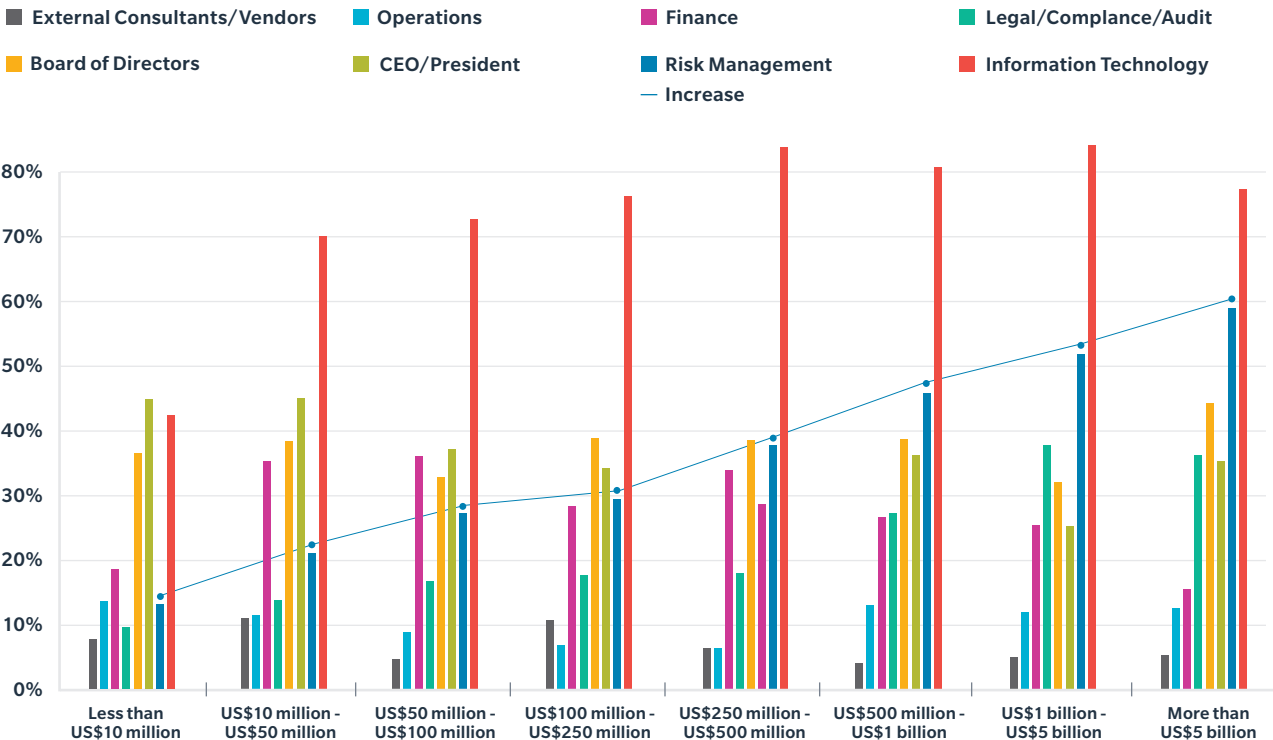
But the accelerating complexity and increasing financial impact of cyber attacks are leading sophisticated organizations to adopt a more comprehensive, economically driven approach to cyber risk management. This approach enlists stakeholders from across the enterprise focused on the entire life cycle — beyond only prevention — to include risk assessment, mitigation, and cyber resilience.

Asked about cybersecurity structure, 70% of survey respondents pointed to their IT department as a primary owner and decision-maker (see Figure 5). Much smaller numbers cited their CEO, board, risk management team, and/or legal and compliance staff.

However, there are variances based on company size: The larger the organization, the more dispersed the responsibility for cyber risk. For example, the involvement of

FIGURE 5 Responsibility for cybersecurity is spreading: the larger the firm, the more often risk managers are involved.
SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

Which functional areas are the primary owners and decision-makers for cyber risk management in your organization?*



*"Don't know" and "other" responses not shown / more than one choice allowed

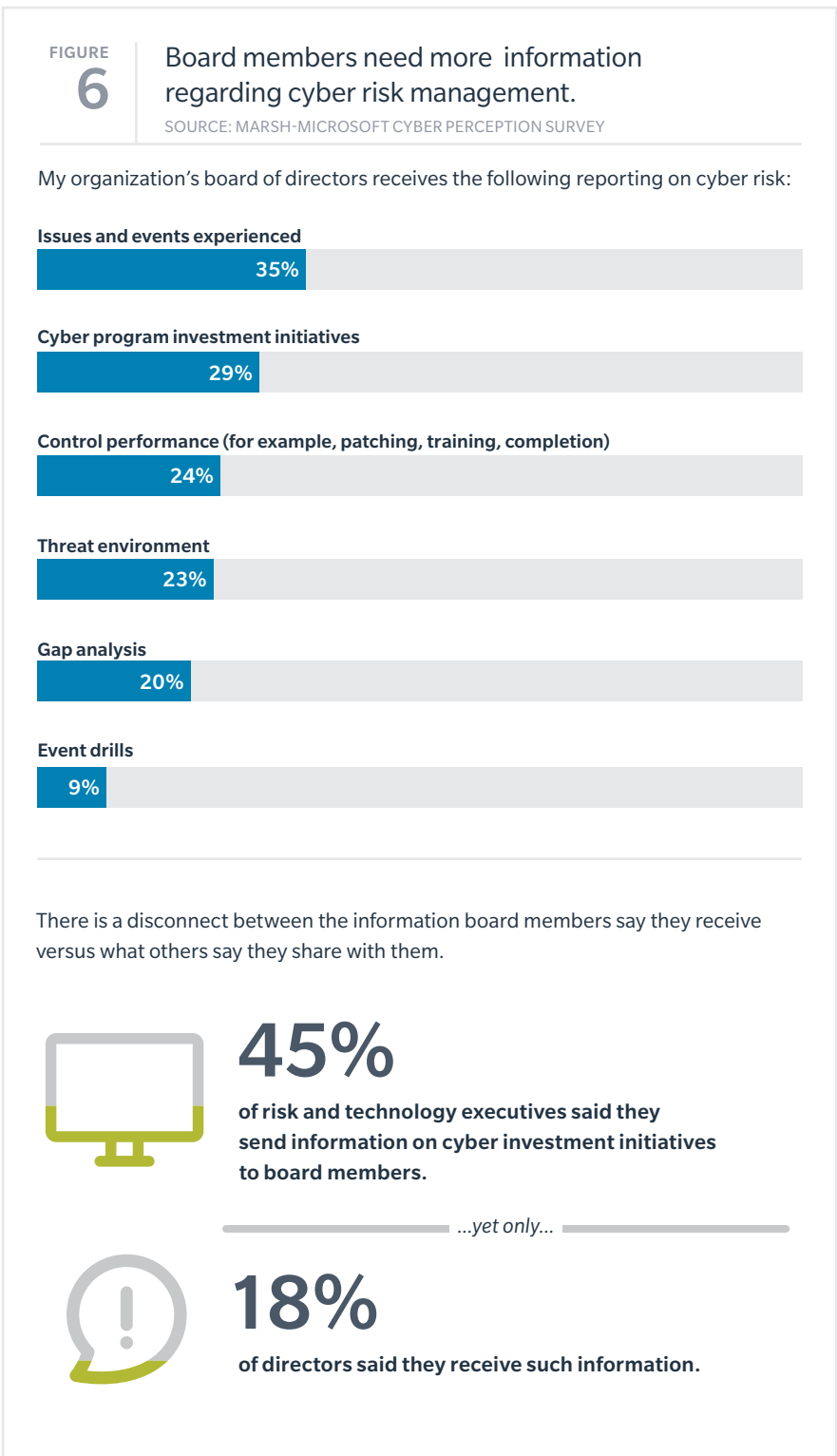
the risk management department climbed steadily with organization size, from a low of 13% in the smallest organizations (many of which may not have a separate risk management function) to 58% in the largest organizations — those with more than US\$5 billion in revenue.

The IT department remained a prominent player regardless of size, but other groups also took on leadership roles. For example, respondents saying their board was a primary cyber risk decision-maker held steady in the mid-30% range, climbing to 42% in the largest organizations.

Ideally, boards should view cyber risk management as part of their overall perspective on enterprise risk management. In organizations where the board is involved, however, we identified a disconnect: Corporate directors often appear to either not understand the information on cyber risk they receive, or to not be receiving it all (see Figure 6). For example, 53% of chief information security officers, 47% of chief risk officers, and 38% of chief technology/information officers said they provide reports to board members on cyber investment initiatives. Yet only 18% of board members said they receive such information.

This information gap points to the need to develop cyber risk economic/business models that facilitate a shared dialogue including common language among IT, the board, and other corporate departments. This disconnect further reinforces the need for a cross-functional approach to cyber risk governance.

An effective cross-functional approach must be backed up with strong organizational leadership, effective communications, and both formal and informal relationships across the enterprise to facilitate information sharing.



Recognizing the Threat, Organizations Invest in Cybersecurity Actions

The recognition of cyber risk as a top concern has led most organizations to boost investments in a range of assessment tools and resiliency measures. Nearly two-thirds of respondents said their organization will increase spending on cyber risk management practices, including risk mitigation and risk transfer (see Figure 7). This aligns with a recent Cybersecurity Ventures analysis that predicted global spending on cybersecurity products and services will exceed US\$1 trillion between 2017 and 2021.

And there is a wide range of potential actions in which to invest. When asked to select among 15 different cyber risk management activities, more than 60% of respondents reported their organization had adopted four or more of them over the

previous 12 to 24 months, and nearly 20% adopted 10 or more of them (see Figure 8).

More than half of respondents implemented enhanced phishing awareness training for employees — the highest engagement level of any activity we surveyed — and/or conducted a cybersecurity gap analysis. More than 40% had improved patch management, conducted penetration testing, required multi-factor authentication for remote access, or encrypted their organization's computers.

Among respondents who reported taking such actions, there was a higher level of confidence in their organization's ability to manage cyber risk. One of the drivers behind increased security measures is the spread of cloud computing and services,

which 68% of respondents say they use. As organizations shift more of their activities to the cloud, they can tap into the security resources and expertise of cloud providers to properly store and protect their data. In many cases, cloud providers may manage not only data security, but also network controls, identity and access controls, and patching. There is a strong correlation between organizations that report using cloud services and their use of other cyber risk management activities.

Despite identifying BI as a top risk, only about 30% of respondents said that they have developed a cyber incident response plan, a key outline of the protocols and processes that organizations should follow in the event of a cyber-attack.

Respondents cited a number of reasons for not having a plan, including a belief that their organizations' defenses were adequate, reflecting conventional overconfidence that attacks can be prevented. Respondents who did not have a plan cited a range of responses, from most common to least common:

1. Cybersecurity/firewalls are adequate for preventing cyber breaches.
2. Cyber incidents are covered in other crisis plans.
3. Organization lacks the expertise.
4. Not an organizational priority.
5. Cyber risk is too small to justify a plan.

FIGURE
7

As cybersecurity investment increases, more risk management options are on the table.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

Over the next 12 months, I expect my organization's level of investment in cyber risk management (including risk mitigation and risk transfer) to:

- Increase
- Remain flat
- Decrease
- Don't know

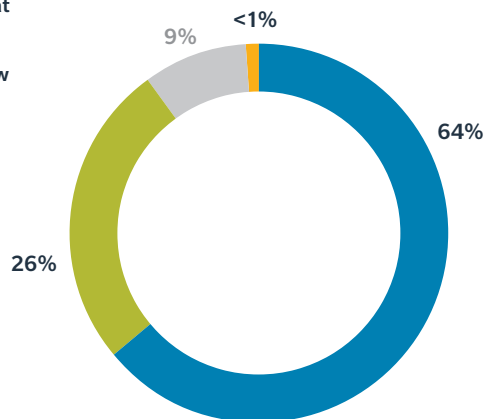


FIGURE
8

Organizations with high confidence in their cyber risk management conducted a wider range of cybersecurity activities.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

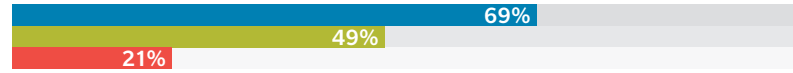
Which of these steps has your organization taken in the past 12 to 24 months?

Responses are segmented by the respondent's level of confidence in organization's ability to manage aspects of cyber risk:

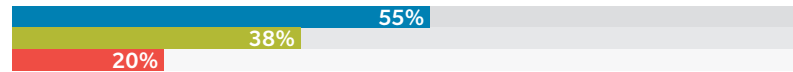
■ High ■ Fair ■ None

ACTIONS TO IDENTIFY AND ASSESS CYBER RISK

Conducted a cybersecurity assessment



Conducted penetration testing



Benchmarked cyber risks against peer organizations and/or our industry

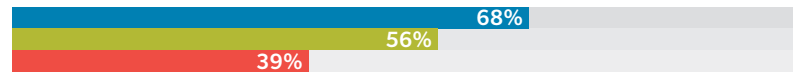


Modeled potential cyber loss scenarios

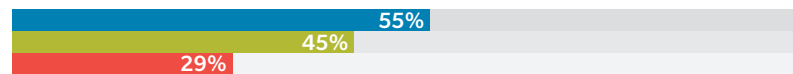


ACTIONS TO PREVENT AND MITIGATE CYBER RISK

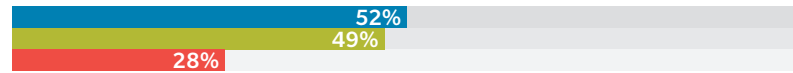
Implemented/enhanced phishing awareness training for employees



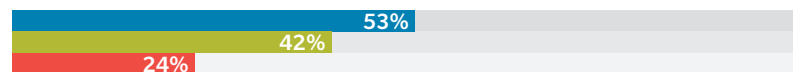
Encrypted organizational desktop and laptop computers



Improved vulnerability and patch management



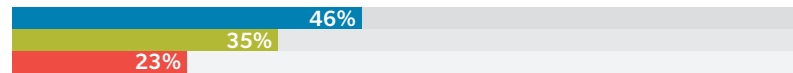
Required multi-factor authentication for remote access to our private network



Made tangible improvements to cyber event detection



Implemented a data loss prevention solution

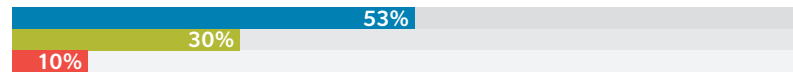


Reduced external system connectivity



ACTIONS TO RESPOND AND RECOVER

Developed a cyber incident response plan



Identified external support services during a cyber incident



Increased our cyber risk insurance limits of liability



Re-structured our cyber insurance and/or purchased different coverages



Better Quantifying Cyber Exposure Will Help Determine Risk Finance Needs

As evidenced by the millions of dollars potentially at stake in a cyber event, financing to help an organization recover from a cyber-attack is more important than ever, with serving insurance a key part of the equation. But before companies can effectively decide how much cyber insurance to purchase, they need to better understand their potential losses. And that is not yet the norm. Fewer than half of respondents said their organization estimates financial losses from a cyber event, and only 11% quantify their estimates in economic terms. Such estimations are a key step in helping boards and others as they

develop strategic plans and investment decisions, including those related to cyber insurance purchase.

While some organizations have attempted to assess their potential losses in economic terms, most use other means, if any at all (see Figure 9). About half of respondents said their organization either already purchases cyber insurance or plans to do so within 12 months (see Figure 10). Among organizations that currently have cyber insurance, nearly 30% said they will likely broaden the number and types of risks covered. This reflects a desire to prepare for evolutions in technology such as the

Internet of Things and artificial intelligence, as well as regulatory developments, including the EU GDPR.

Among all respondents, just 16% said the cyber insurance available today meets all of their organization's needs. It's worth noting that 44% of respondents said they "don't know" whether cyber insurance meets their organization's needs. This reflects the rapid evolution and expansion of cyber coverage, coupled with a lack of understanding in many companies about how much it has changed. It also points to the necessity to deploy more advanced risk quantification tools, which enable clearer decision making about the role of insurance in cyber risk management — for example, helping to determine limits and retention levels. Sophisticated economic models exist that allow organizations to better assess the likelihood they will be attacked, and their potential losses. However, few firms currently take advantage of them.

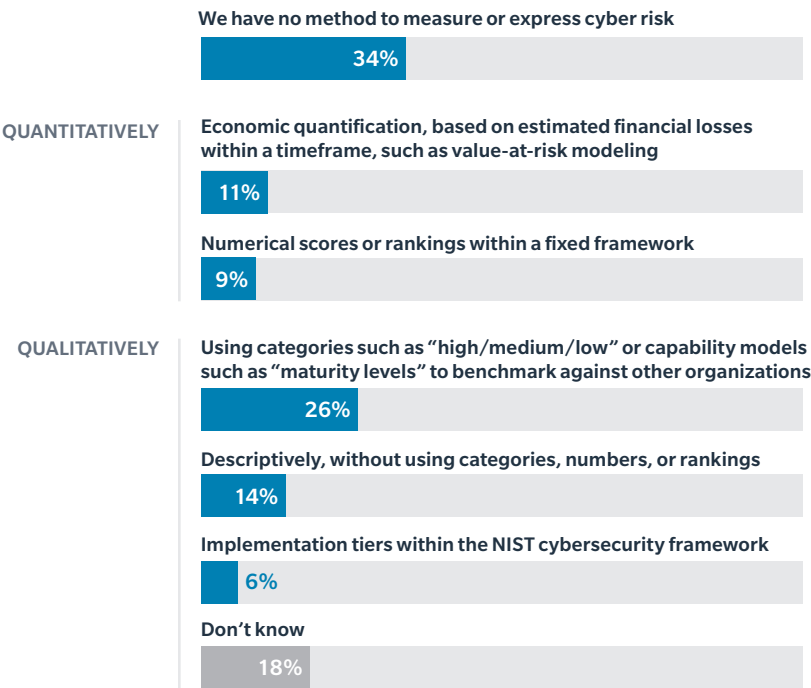
Among organizations that do measure or express cyber risk in economic terms, there is a greater likelihood that they are planning to purchase or increase their cyber coverage over the next year. They were also more than twice as likely to raise their cyber coverage limits.

FIGURE
9

Most organizations that have a means to express their cyber risk do so qualitatively.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

How does your organization measure or express its cyber risk exposure?



45%
of organizations
estimate the
financial impact of
a cyber incident.

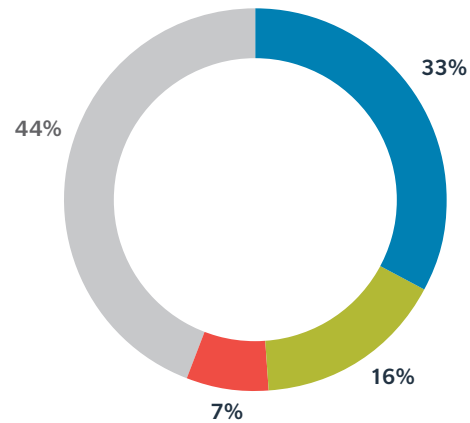
FIGURE
10

Cyber insurance market continues to develop as organizations balance their needs against available coverage.

SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY

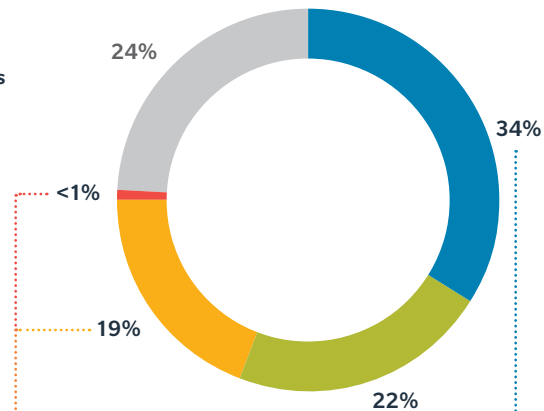
The cyber insurance available in today's market:

- Meets some of my organization's needs
- Meets all of my organization's needs
- Does not meet my organization's needs
- Don't know



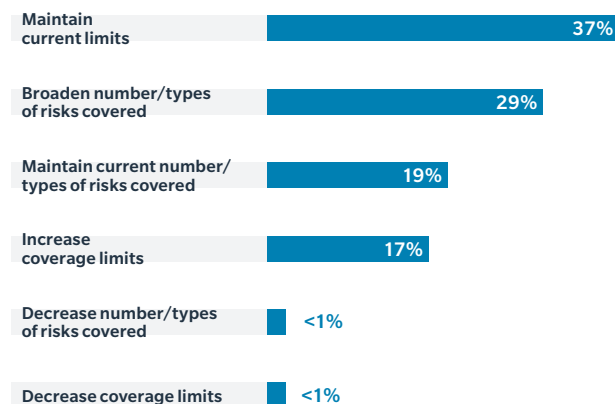
What is your organization's status with regard to cyber insurance?:

- Currently has cyber insurance
- Plans to purchase or increase cyber insurance in the next 12 months
- Does not have cyber insurance and does not plan to purchase it
- Plans to discontinue its cyber insurance coverage
- Don't know

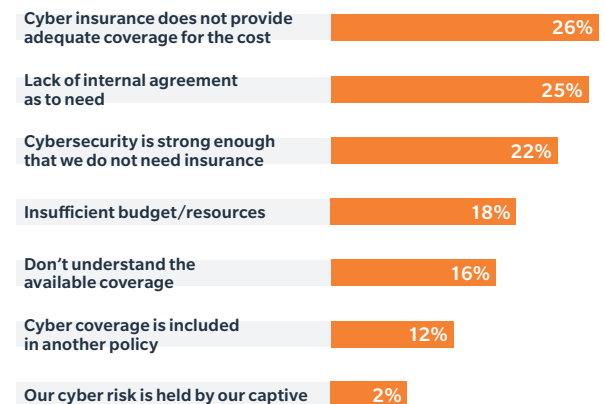


Among those with cyber insurance currently:

What plans does your organization have to change its cyber insurance in the next 12 months?*



Why does your organization not purchase cyber insurance or plan to drop it?*



*Remaining share responded "don't know"

Industry, Government, and Cybersecurity Effectiveness

As cyber risk has grown for companies in all sectors, so has the complexity of managing it. This is accelerated in part by the increased use of emerging technologies, including artificial intelligence, robotics, the Internet of Things, and more. At the same time, attacks evolve, sponsored increasingly by nation-states and organized crime.

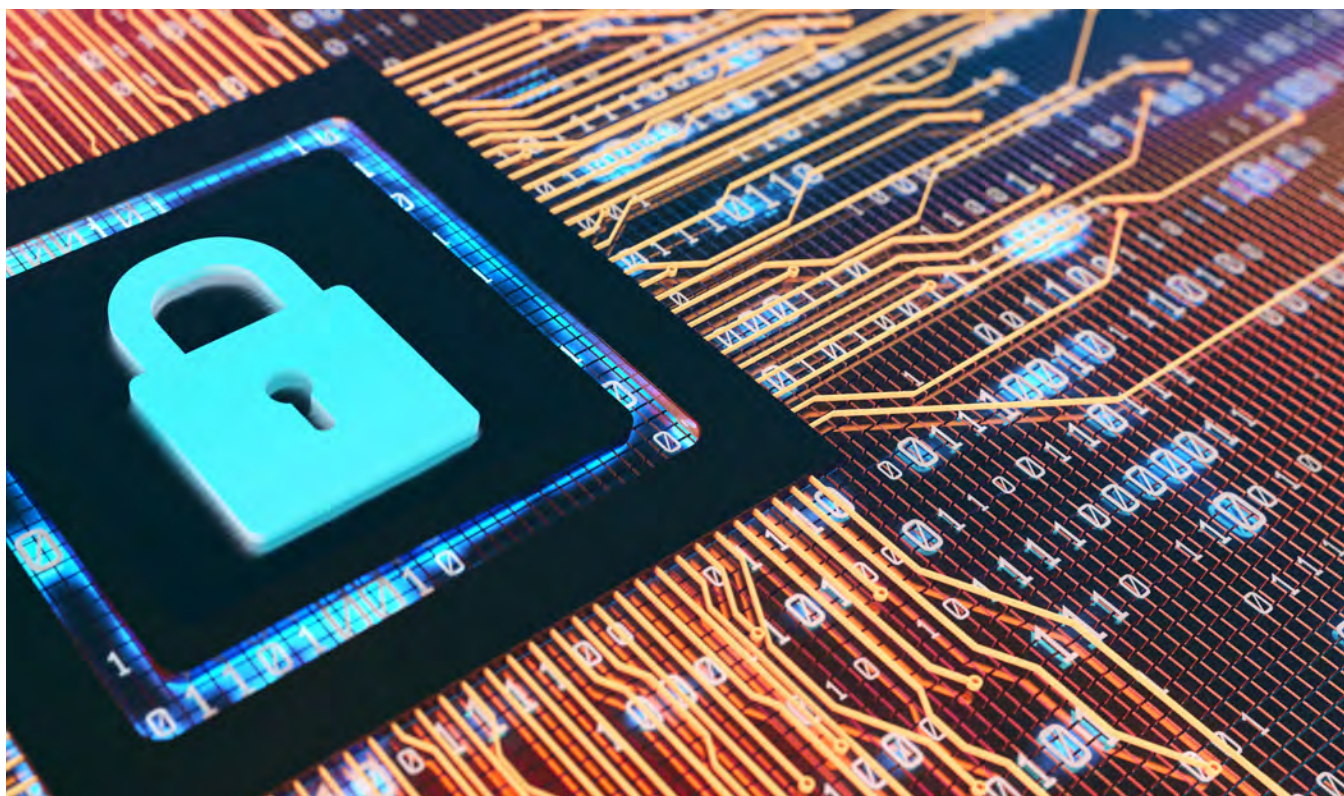
Organizations can more effectively manage cyber risk by applying a holistic, comprehensive approach that emphasizes proven security practices, such as updating systems regularly and other preventative measures. Overcoming the managerial and technological challenges this presents can be addressed more effectively when responsibility is shared among stakeholders, including corporate boards, C-suite executives, risk professionals, and technologists.

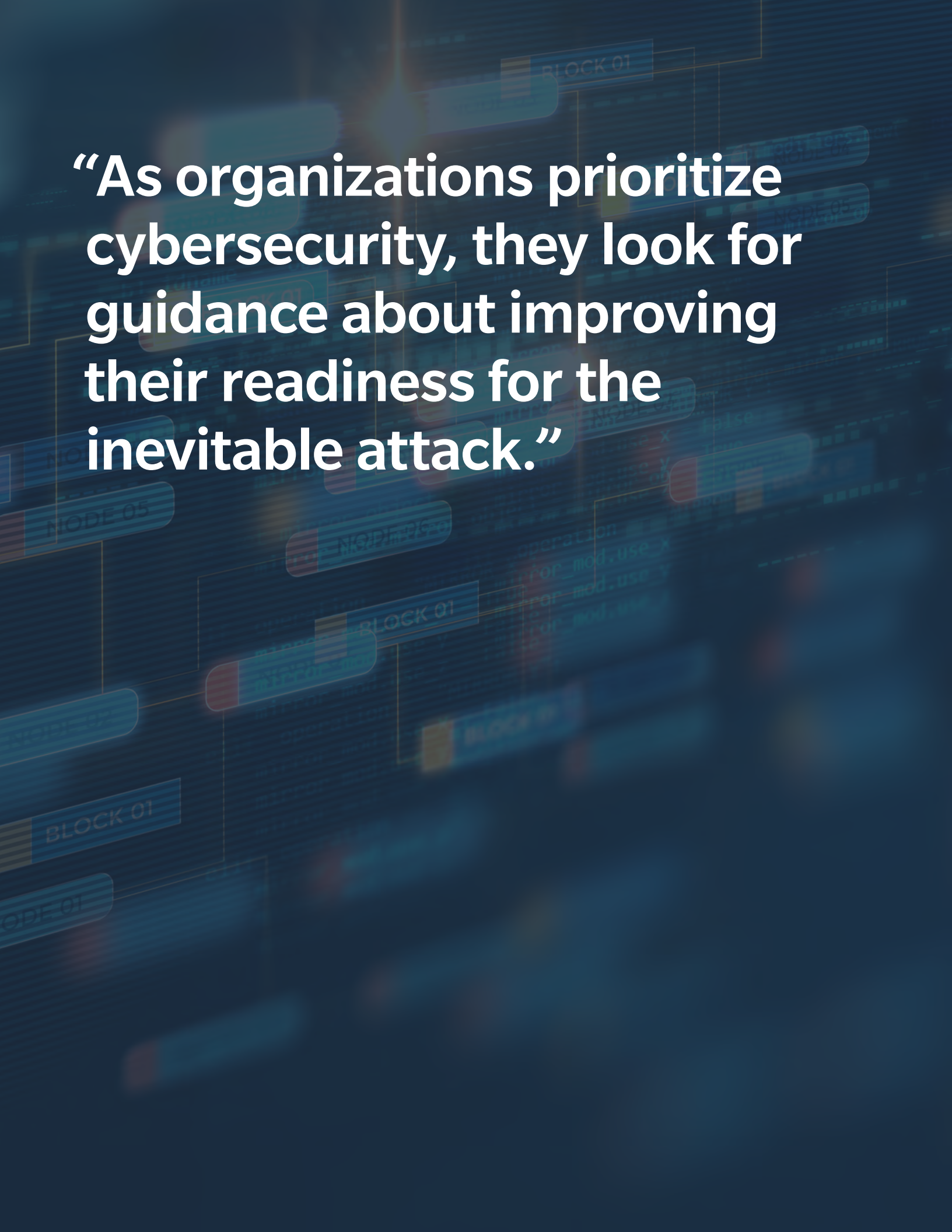
Governments have a critical role to play as well. Given the growth of state-sponsored and organized crime-sponsored attacks, more needs to be done by all instruments of government to work with industry. Government's unique capabilities can be leveraged to

improve cyber readiness across sectors, including the ability to convene stakeholders for development of standards and best practices to improve cyber risk management.

As organizations prioritize cybersecurity, they look for guidance about improving their readiness for the inevitable attack. Policymakers should continue to promote the development and coordination of frameworks and practices for enterprise cyber risk management, including guidance that is sectoral and cross-sector, while at the same time developing national strategies for cybersecurity. For example, the NIST Cybersecurity Framework is a primary reference for organizations managing cyber risk across functional domains, and it has informed emerging regulatory approaches to cybersecurity.

As the survey results underscore, cybersecurity risk can be managed, but not eliminated. The scale and complexity of the challenge is too great for a "silver bullet" solution. Effective adaptation and coordination is required to remain resilient against this significant and dynamic threat.





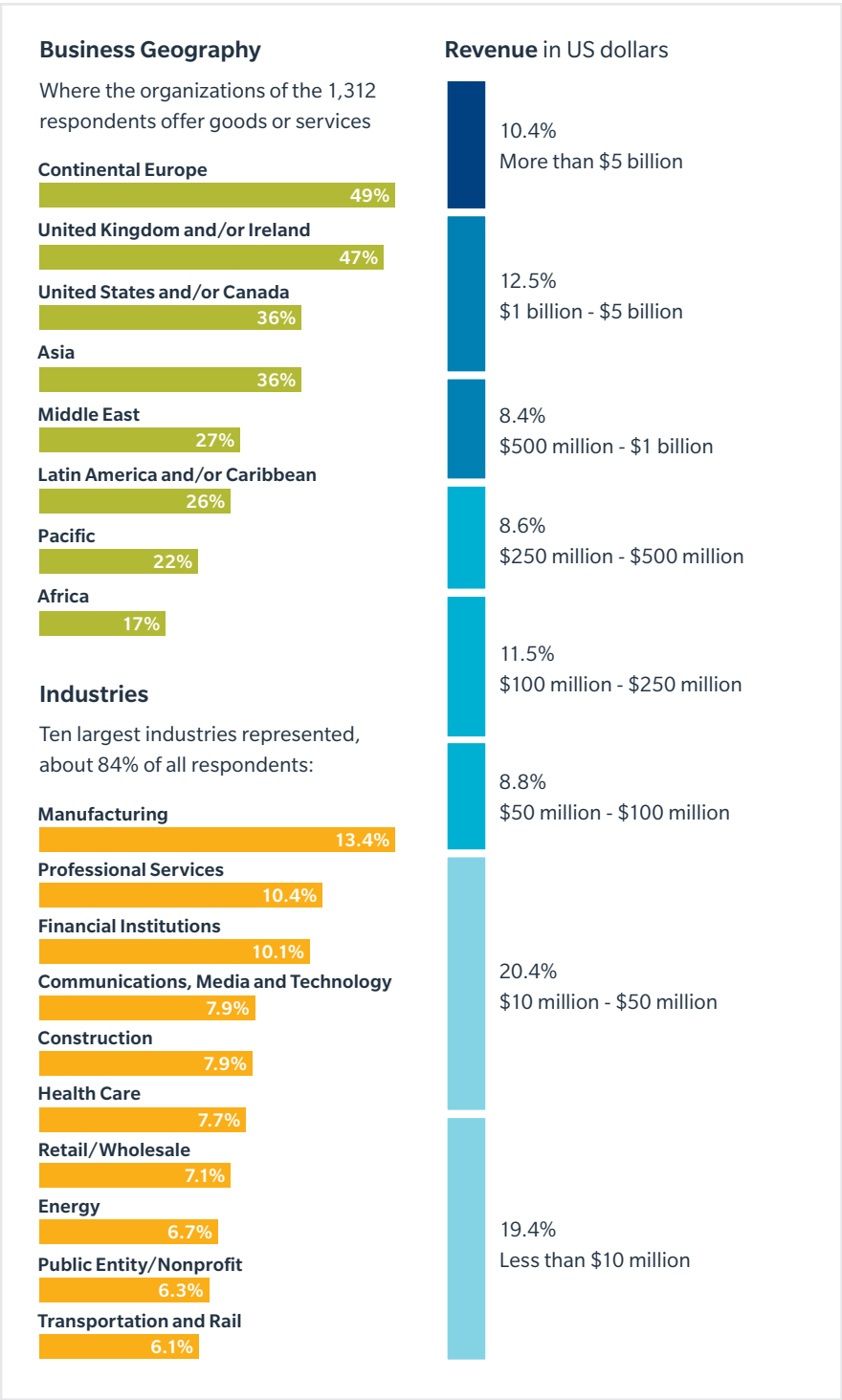
“As organizations prioritize cybersecurity, they look for guidance about improving their readiness for the inevitable attack.”

METHODOLOGY

This report is based on findings from the *Marsh-Microsoft Global Cyber Risk Perception Survey* administered between July 2017 and August 2017.

Overall, 1,312 senior executives participated in the global survey, representing a range of key functions, including information technology, risk management, finance, legal/compliance, senior management, and boards of directors.

SURVEY DEMOGRAPHICS





ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, Marsh's 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US\$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter [@MarshGlobal](#); [LinkedIn](#); [Facebook](#); and [YouTube](#), or subscribe to [BRINK](#).

ABOUT MICROSOFT

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

ACKNOWLEDGEMENTS

Marsh thanks Microsoft's Global Security Strategy and Diplomacy team for their collaboration in developing this report. The Global Security Strategy and Diplomacy team combines technical expertise and public policy acumen to develop public policies that improve security and stability of cyberspace, and enable digital transformation of societies around the world.

Marsh also thanks Marsh & McLennan Companies' Global Risk Center for its collaboration. The Global Risk Center brings together leaders from industry, government, non-governmental organizations, and academia to address critical challenges facing enterprise and societies around the world.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. 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.

Copyright © 2018 Marsh LLC. All rights reserved. MA18-15384 193971570