Cyber catalyst report: Guiding priorities in cyber investments

The report stems from our Marsh Global Cyber Buyers' Study, which was fielded from January to July 2025, gathering insights across eight regions from 2,200+ cyber risk leaders — including both cybersecurity and risk management specialists.

2200+
Cyber Risk Buyers

8
Regions

20
Countries

A broad spectrum of company sizes and industries responded

We started with a simple question: What keeps you, as a cyber risk leader, awake at night?

The leaders provided a wide range of answers:

- Is my organization prepared for a ransomware attack? A privacy breach? Any of the dozens of other ever changing cyber threats?
- How should I direct my organization's cybersecurity investments?
- Is our confidence level in our cyber defenses justified?
- Does the decision-making structure for all things cybersecurity make sense?

And more.

Cybersecurity requires enterprise-wide engagement and collaboration, and we hope the insights contained within this report reduce the complexity when making difficult decisions.

The study follows similar surveys we conducted in 2019 and 2021, and combines quantitative and qualitative research, offering a snapshot of rapidly evolving trends in cyber risk management. By exploring both current pain points and future investment strategies, the report can provide valuable guidance as you look to enhance your cyber risk management strategy and resilience.

While the survey was global in scope, regional responses varied considerably, particularly around confidence levels and plans for cyber investments. This report highlights a few of those differences; we'll bring you additional regional analysis in the coming months.

Finally, we'd like to thank all those who participated.

Download Report

Executive Summary
Key Findings

Prioritizing cybersecurity investments

Nearly two-thirds of organizations globally plan to increase investments in cybersecurity in the coming year.

- The top three areas cited for investments were cybersecurity technology/mitigation, cybersecurity incident planning and preparation, and cybersecurity personnel and talent hires.
- Regionally, organizations in Asia were least likely to say they would increase spending; those in the UK were most likely.

- It's important not to overplay the significance of any one threat; there are many incident types and scenarios.
- Incident planning that emphasizes scenarios and tabletop exercises can help organizations respond to a range of event types. Incident planning that emphasizes scenarios and tabletop exercises can help organizations respond to a range of event types.

Diverse threats

Organizations cited a range of concerns, with ransomware and privacy breaches continuing to top the list, as they did in 2021.

These threats are highly visible and impactful, often causing significant operational disruption, financial loss, and reputational damage.

Increasing confidence

Nearly three-quarters of organizations expressed a high level of confidence in their overall cyber risk management strategy.

- Drilling down, many organizations expressed a lower level of certainty regarding specific cyber risk management strategies and capabilities, such as incident response planning and employee training.
- Confidence levels varied widely by region and, to a lesser extent, company size, with larger entities expressing high confidence.

- Most organizations use a variety of approaches to inform their strategies and cyber risk decision-making — ranging from global or regional committees and risk collectives to solo decision-making by CISOs.
- This differs from our 2021 study, which found that typically two to three key functions were involved in cyber risk investment decisions.

Varied decision-making approaches

Differences in cyber risk governance emphasize the need for coordinated, enterprise-wide decision frameworks that balance risk priorities and involve multiple stakeholders.

What may these findings mean for you?

The key findings from our study reveal critical trends and challenges in the evolving cyber risk landscape, but organizations must translate them into actionable strategies.

By focusing on enterprise-wide engagement, foundational controls, incident preparedness, and third-party risk resilience, you can better align your efforts with the goal of improving the way you effectively and proactively address today's and tomorrow's cyber threats.

What may this mean for your organization overall?

Enterprise-wide engagement matters

Effective cybersecurity depends on collaboration across all levels and functions within your organization.

From IT and security teams to executives and business units, everyone plays a role in identifying, managing, and responding to cyber risks.

Fostering a culture of shared responsibility can strengthen your overall security posture and may lead to faster, more coordinated responses to threats.

Focus on the fundamentals

While the latest threats may grab headlines, foundational security controls remain critical to preventing and mitigating events.

Consistently applying the most effective security controls — including incident response planning and testing, endpoint detection and response, multi-factor authentication, logging and monitoring, employee training, and patching — can create a strong defense that may reduce vulnerabilities.

Maintaining focus on these basics can be key to building resilience.

Be ready: Incident preparedness

Being prepared for a cyber incident can be just as important as preventing one and is found to be directly tied to the cost of an incident.

Developing and regularly testing incident response plans may enable your organization to more quickly contain and recover from attacks, minimizing damage and downtime.

A critical component of preparedness is having an out-of-band communications platform, which can allow secure, reliable communication channels to remain available even if primary networks are compromised.

Understand risk introduced by third parties

More than 70% of organizations experienced at least one material third-party cyber incident in the past year (SecurityScorecard).

Managing third-party risk requires thorough due diligence, regular monitoring, and clear contractual expectations with vendors and partners.

Addressing these risks proactively can help prevent prevent breaches originating from an organization's supply chain.

What may this mean for security professionals?

Enterprise-wide engagement matters

Integrating cyber risk considerations into broader enterprise risk management frameworks can align and streamline efforts.

Focus on the fundamentals

Prioritize and maintain a data-driven, rigorous implementation of the most effective controls in an effort to reduce the attack surface and help prevent cyberattacks.

Be ready: Incident preparedness

As the person or team on the front line of an attack, it is critical to have clear, practiced plans to detect, contain, and remediate attacks swiftly.

Understand risk introduced by third parties

Understand the technical and business risks that may be introduced by partners and vendors — and how to address them.

What may this mean for risk/insurance specialists?

Enterprise-wide engagement matters

Break down silos and engage with stakeholders across the enterprise to help enable comprehensive threat detection and response.

Focus on the fundamentals

Relying on foundational controls may help optimize insurance outcomes and reduce operational risk.

Be ready: Incident preparedness

Build incident preparedness into risk management and business continuity plans, with the goal of helping to minimize disruption and financial impact.

Understand risk introduced by third parties

Incorporate third-party cyber risk into enterprise risk assessments and vendor management programs.

Array of cyber threats on leaders' minds

Cyber risk management challenges continue to accelerate, driven by the speed and sophistication of attackers and the range of potential cyber threats. The range of threats underscores the critical need to deploy robust security controls and rapid incident response capabilities alongside proactive risk management and cyber insurance.

Ransomware and privacy risks persist amid a complex cyber threat landscape

We asked survey respondents to rank the main cyber threats to their organizations (see Figure 1).

The top two choices were ransomware and privacy breaches, each named as one of the top three cyber risks by 29% of respondents.

These were followed by denial of service (DOS) attacks, loss of non-personal private information, business interruption, and AI-related risks — highlighting the broad and varied nature of the threat landscape organizations must contend with.

Ransomware events may be top of mind in part because they tend to generate more news coverage than other incidents, leading many organizations to view it as the most catastrophic scenario for them.

On the plus side of their high-profile nature, ransomware incidents can be used to help focus an organization's attention on cybersecurity issues.

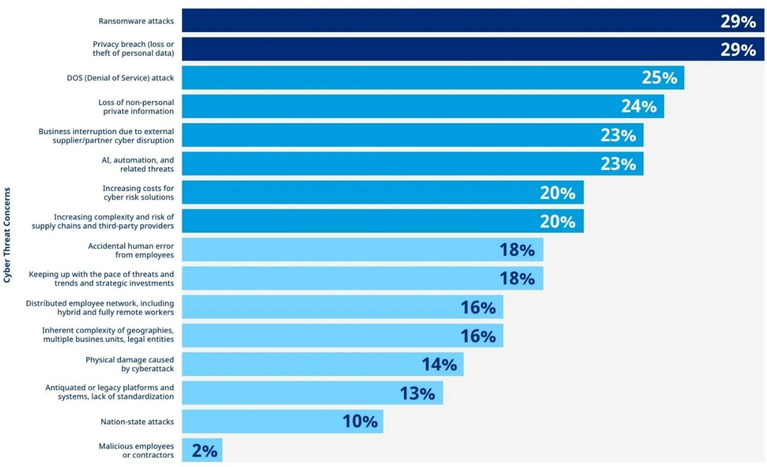
But on the flip side, care should be taken not to overplay their significance at the expense of other risks.

The cyber threat environment is muddled, with many incident types and scenarios that can potentially affect an organization.

No matter what the specific threat, effective cyber risk management should include *robust cybersecurity controls*, incident response capabilities, and insurance coverage. Together, these can form the foundation of a comprehensive cyber resilience strategy.

It can be difficult to determine which cyber controls are likely to have the most impact. The "right" controls for a particular organization will depend in large part on factors including company size, industry, its current state of cyber risk preparedness, and other unique circumstances.

Figure 1: Ransomware and privacy breaches top the list of cyber threat concerns



Across threats, scenarios and tabletop exercises are key to cyber resilience

Recent analysis of Marsh's comprehensive Cyber Self-Assessment data revealed that incident response planning that includes scenarios and tabletop exercises can be essential pieces of resilient cybersecurity.

Regularly conducting such exercises and incorporating new information on threats, trends, and ongoing changes in company control measures can lead to evolving, nimble plans.

As new threats emerge, these regularly scheduled active planning exercises, using real-life situations, can improve the response to an actual event, even if it is very different from what has been practiced.

For example, tabletop exercises can enable those who are involved in the response to think through details such as what technology will be available to use should the network be compromised.

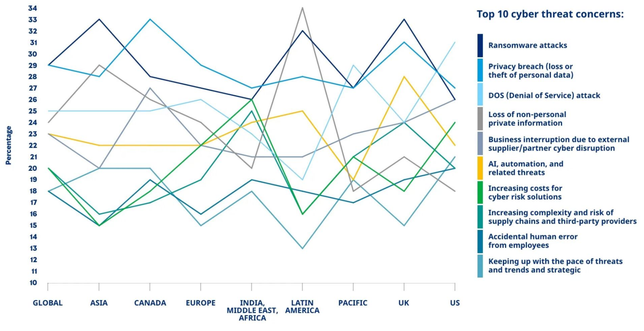
Tabletop exercises may be particularly valuable in addressing third-party and supply chain risks — an emerging concern across many regions with significant and widespread consequences.

By planning for and practicing responses to supply chain incidents, organizations can better prepare for the complexities introduced by external partners and vendors.

While nuances exist across regions, many cyber threats are similar worldwide.

This underscores the importance of maintaining foundational security controls and focusing on the basics, which can be critical to preventing and mitigating cyber events regardless of geography.

Figure 2: Ransomware attacks and privacy breaches are also the top concerns across regions



Confidence in cyber risk management increases

Respondents in 2025 expressed a high level of confidence in their cyber risk management and mitigation initiatives (see Figure 3), an increase in confidence levels from our 2021 study. But ascribing meaning to organizational confidence can be tricky as an organization can have high confidence in an area where they have invested much time and effort, but they don't know what they don't know. Cyber confidence can be shaken when real-life events play out in ways that a company had not anticipated, or if they arise in an area that has been overlooked.

Self-assurance in specific capabilities is often lower than overall confidence

Even among organizations with a high level of confidence in their overall cyber risk management and mitigation initiatives, many expressed a lower level of certainty regarding specific cyber risk management strategies and capabilities. For example:

72%
of respondents globally said they were confident overall

61%
confidence was highest in financing cybersecurity solutions

60%
followed by management of cyberattacks

58%
and lowest in mitigating and preventing cyberattacks

Figure 3: Majority of organizations are confident in their cyber risk management



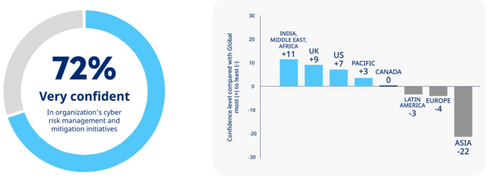
Showing percent 'confident' for all data points.
Q: For each of the following, please indicate your level of confidence in your organization's cyber risk management.

Confidence levels vary widely across regions

We also found confidence levels to vary widely by region (see Figure 4). For example, respondents in Asia were 22% less likely to say they were very confident than the global average; respondents in India, the Middle East, and Africa, on the other hand, were 11% more likely.

Regional and organizational differences in cyber risk confidence and capabilities should be addressed by adopting best practices and seeking guidance that are tailored to your organization.

Figure 4: Organizations in India, the Middle East, and Africa region most likely to express high confidence in cyber risk management



Showing differences in percent 'very confident' between global and regional responses.
Q: For each of the following, please indicate your level of confidence in your organization's cyber risk management.

What impacts confidence levels?

Compared to most risks facing an organization, cyber is relatively new. Over the past decade, as technology permeated nearly every aspect of global business, awareness of cyber risk increased tremendously.

Larger companies are more confident than smaller ones

Size also matters in confidence levels. Among the largest companies in our survey, 79% said they were very confident in their cyber risk management and mitigation capabilities, compared to 67% of small to medium size organizations. This aligns with findings about size in other studies we have conducted.

For example, a 2025 Cyber Risk Intelligence Center *(CRIC) study* of event likelihood found that the size, by revenue, of an organization can play a strong role in determining both the potential for an event and its impact on the organization.

Small companies tended to exhibit a wider variation in the frequency of cyber events, meaning that an improvement in cybersecurity measures could have a more significant impact on protecting them.

Larger companies typically showed a smaller variation in event frequency. However, the financial stakes for larger firms can be higher, meaning small improvements could have significant financial impacts.

Other size-related implications include the likelihood of being targeted by cybercriminals, potential room for improvement, financial impact, and insurance considerations.

Very confident in cyber risk mitigation

79%
of larger companies

67%
of smaller companies

Maturity and experience: how exposure builds cyber confidence

When it comes to cyber confidence, some regions demonstrate higher confidence levels, likely reflecting longer exposure and greater experience with cyber threats.

Regions such as India, the Middle East, and Africa (+11%), UK (+9%), and US (+7%) report confidence levels notably above the global average (72% very confident), which may indicate more mature cyber risk management practices.

Conversely, regions with lower confidence may reflect newer exposure to these threats or less mature cyber risk programs.

Those with higher confidence have likely been managing cyber risks for longer, allowing them to build experience and strengthen their security controls over time.

Deciding where to make cybersecurity investments

As part of this study, we conducted a series of in-depth interviews with senior cyber risk buyers and decision-makers from a diverse range of industries and regions (see the Methodology section for more details).

Their concerns ranged from being ready for specific cyber threats to balancing strategic investments and keeping up with the pace of evolving cyber trends (see Figure 5).

Although the details of what to invest in will vary by companies' unique situations, the general approach should include prioritizing proactive investments in cybersecurity technologies, incident response planning, and employee awareness training.

At the same time, balancing cyber risk budgets between cybersecurity investments and cyber insurance can help strengthen overall risk management.

Figure 5: Cyber risk buyers outline a range of issues "keeping them up at night"

Pain points:

- Balancing strategic investments in cyber insurance and cybersecurity as costs increase
- The rise of ransomware, phishing, and AI-related threats to business
- Sophistication of attackers and foreign and state-sponsored actors looking to disrupt business or create geopolitical instability
- Accidental human error and the increase of devices and access points
- The challenges of a distributed employee network, including hybrid and fully-remote workers
- Compliance with cyber policies and regulations, both of their enterprise and local government
- Malicious actors, either employees or suppliers
- Increasing complexity and risk of supply chains and third-party providers
- Limited regional expertise (outside the US) and lack of integrated decision-making between global and regional teams
- Antiquated or legacy platforms and systems; lack of standardization and integration across the enterprise
- Inherent complexities of multiple business units, legal entities, and geographies managed by large MNC's
- Borderless threats in a global economic system
- Keeping up with the pace of threats and trends

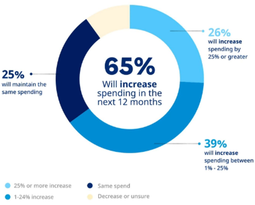
Most companies plan to increase cybersecurity investments

The range of cyber threats and concerns is leading companies to assess where and how they invest finite resources, including how to divide limited budget allocations between cyber insurance and cyber controls.

Globally, regardless of role or industry, companies are ramping up investments in cyber risk management, with over a quarter planning to increase spending by more than 25% (see Figure 6).

Figure 6: Most companies plan to increase cybersecurity spending

Average investment change in the next 12 months



As in other areas, plans for spending varied by region, with organizations in the UK most likely to increase cyber investments above the global average and those in Asia and Europe less likely to do so (see Figure 7). Interestingly, when comparing spending intentions and confidence levels by region, those that were least confident tended to also be the least likely to plan to increase spending.

Figure 7: Anticipated cybersecurity spending increases vary regionally





Technology, planning, and personnel top the list of investment priorities

70% Cybersecurity technology/ mitigation

68% Cybersecurity incident planning and preparation

67% Cybersecurity personnel and talent hires

66% Staff training

65% Cyber insurance

Over the next 12 months, these are the top five areas in which respondents said they would increase investments.

Investing in foundational security

It's encouraging to see that most companies plan to increase investments in cyber risk management and mitigation. As they do so, focusing investments on cybersecurity fundamentals may be critical. For example, *additional research* we've conducted has shown that foundational practices — including endpoint detection and response (EDR), logging and monitoring, and cyber incident response planning and testing — correlated highly with a reduction in the likelihood of cyber incidents.

As organizations adopt more technology, the attack surface inevitably expands and increases the number of potential entry points for attackers. This expanded exposure makes foundational security controls even more essential, as they can serve as the first line of defense against increasingly sophisticated threats.

By prioritizing essential controls and adhering to best practices, organizations can minimize risk exposure and enhance cyber resilience in an environment where technology growth and third-party dependencies continue to evolve.

72%

of organizations prioritize addressing vulnerabilities introduced by complex supply chains, highlighting growing awareness that third-party cyber exposure can be a significant risk.

Measuring cyber risk exposure: Large increase in risk measurement; quantitative measures more than doubled

It's important to keep in mind that the "right" areas in which to increase investment will vary depending on such factors as an organization's size, industry, existing capabilities, and unique situation. One key to setting an investment strategy is to measure and understand these circumstances (see Figure 8).

Figure 8: Companies' measurement of cyber risk exposure has increased

	2025 Study	2021 Study
Financially based on estimated potential losses of a cyberattack within a specific timeframe (value-at-risk modeling)	66%	26%
Systematically via stages or implementation tiers within cybersecurity frameworks	66%	29%
Quantitatively via numerical scores or rankings within a fixed framework	56%	22%
Visually or categorically with colors and/or levels such as "high/medium/low" to benchmark against other organizations	55%	28%
Calibrating the likelihood and/or severity of potential cyber risks	54%	28%
We have no method to measure cyber risk	1%	18%

Cyber risk decision-making: an enterprise-wide exercise

The accelerating threat environment has made cyber risk a C-suite and board-level priority for many companies, meaning that more emphasis is being placed on enterprise-wide oversight and collaboration, including on investment decisions.

Cyber risk decision-making differs across organizations, with security leaders often supporting committees or acting as primary decision makers in shaping response and mitigation strategies.

Differences in cyber risk governance emphasize the need for coordinated, enterprise-wide decision frameworks that balance risk priorities and involve multiple stakeholders.

Establishing oversight

We found that organizations establish oversight in several ways, depending upon the level of integration and maturity of their cyber risk initiatives:

Cybersecurity decision maker

A sole decision maker is often supported by cybersecurity technical experts who conduct due diligence and provide investment recommendations to a CISO, COO, or CEO, depending on the size of the company.

Risk, cybersecurity, and insurance collective

This decision-making structure is a coordinated effort between cyber risk leaders, with greater deference to the leader who initially recommended the investment.

Regional or global oversight committee

These include representatives from operations, risk, IT, cybersecurity, finance, legal, and insurance who have strong influence in identifying and vetting investment decisions across cyber risk.

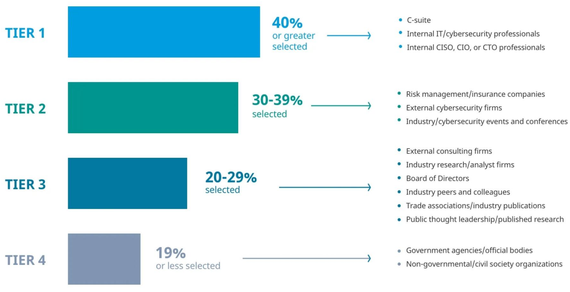
Informing the decision makers

Survey respondents said they use a variety of approaches to inform their strategies and cyber risk decision-making — from global or regional committees and risk collectives to solo (or ultimate) decision-making CISOs (see Figure 9).

This contrasts with our 2021 study, which found that two to three key functions typically were involved in cyber risk investment decisions. In general, today's decision makers are addressing challenges by purchasing solutions; leveraging, or "borrowing" external expertise; building in-house specialist teams and centers of excellence; and more.

Throughout the decision process, they are looking for market intelligence and insights, first from internal leaders, followed by risk management/insurance companies and cybersecurity firms.

Figure 9: People and organizations that inform investment decisions



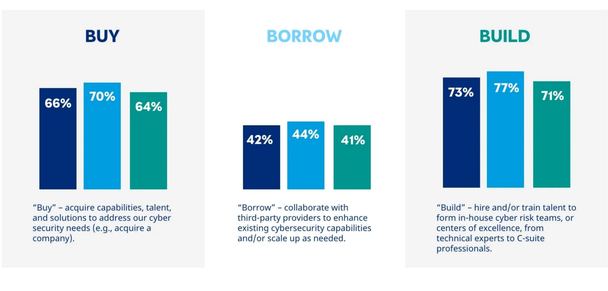
Investment approaches: Buy, borrow, or build

Among the three methods, the build method was preferred, particularly by larger organizations, although buying was a close second; many organizations said they use a combination of approaches (see Figure 10).

One advantage of the buy model is that third-party providers can scale rapidly and provide specialized expertise on demand. Importantly, third parties bring an objective perspective that may be helpful for making unbiased, data-driven risk decisions — something that can be challenging to achieve internally. This objectivity may help organizations accurately assess their cyber risk profile and develop tailored strategies to mitigate exposure effectively.

As a result, the desire to work with a third-party adviser jumped significantly (to 93%) when positioned specifically as an adviser capable of assessing cyber risk and recommending strategies, actions, and specialists to address organizational needs. Among those planning to increase cybersecurity investments in the next 12 months, 50% said they would turn to third parties.

Figure 10: Companies build, buy, and borrow to address cyber risk challenges



Conclusion: Building cyber resilience – your path forward

We hope that this report will help organizations translate insight into action.

By assessing your unique risk landscape and investing strategically in the right controls and capabilities, you can better take control of your cyber risk.

As the world's most trusted and innovative cyber risk advisor, we can help you navigate the complexity of cyber risk with clarity and confidence. To discuss the report findings as they relate to your organization, contact your Marsh representative or fill out the form to be contacted directly.

Stay tuned for upcoming reports that will offer deeper dives into regional survey findings.

Methodology

The Marsh Cyber Risk Buyers' Study 2025 employed a rigorous, multi-phased, mixed-methods research design combining qualitative and quantitative approaches.

This methodology provided a comprehensive understanding of cyber risk perceptions, confidence levels, investment priorities, and emerging trends across global industries and regions. A global branding and consultancy firm, Occula Group, fielded the study.

In the qualitative phase, 36 in-depth, double-blind executive interviews were conducted with cyber risk buyers from diverse industries and geographic regions. A double-blind protocol was strictly followed to minimize bias and ensure data integrity.

The quantitative phase involved administering a structured online survey to more than 2,200 cyber risk buyers representing a broad spectrum of company sizes, industries, and eight global regions. The survey instrument was pre-tested to ensure clarity, relevance, and reliability of questions.

2200+

Cyber risk buyers representing a broad spectrum of company sizes, industries, and eight global regions.

The study included respondents from

8

Regions

20

Countries

Participants were selected to represent diverse industries, company sizes — from small and medium enterprises to multinational corporations — and geographic regions. All participants held relevant cybersecurity, risk management, or insurance roles to ensure informed responses.

The study included respondents from the following 8 regions and 20 countries:

- **Asia**: Japan, South Korea, Singapore
- **Canada**
- **Europe**: France, Germany, Italy, Spain
- **India, the Middle East, and Africa**: India, Saudi Arabia, South Africa, United Arab Emirates
- **Latin America**: Brazil, Colombia, Mexico, Peru
- **Pacific**: Australia, New Zealand
- **UK**
- **US**

Quantitative data were analyzed using statistical methods to identify trends, regional and organizational disparities, and correlations between variables. Qualitative interview data were coded and thematically analyzed to contextualize survey findings and uncover deeper insights. Comparative analysis was conducted against prior studies, including the 2021 report, to assess changes over time.

Participation in the study was voluntary, with confidentiality and anonymity assured. The study complied with applicable data protection regulations and ethical research standards.

While the study covers a broad global sample, some regional nuances may require further localized research. Additionally, self-reported data may be subject to respondent bias despite measures taken to mitigate it.

Download Report

About Marsh

Marsh, a business of Marsh McLennan (NYSE: MMC), is the world's top insurance broker and risk advisor. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective. For more information, visit marsh.com, or follow on LinkedIn and X.

Marsh is a business of Marsh McLennan.

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.

1166 Avenue of the Americas, New York 10036

Copyright © 2025, Marsh LLC. All rights reserved.