MARSH | Microsoft

INSIGHTS | FEBRUARY 2020

2020 Global Cyber Risk Perception Survey

Retail/Wholesale, Food, and Beverage Industry Report

MARSH & McLENNAN COMPANIES

INSIGHTS | FEBRUARY 2020

2020 Global Cyber Risk Perception Survey

Retail, Wholesale, Food, and Beverage Industry

CONTENTS

Introduction

The *2019 Global Cyber Risk Perception Survey* from Marsh and Microsoft investigated the state of cyber risk perceptions and risk management at organizations worldwide, especially in the context of a rapidly evolving business technology environment. We present here the findings related to retail, wholesale, food, and beverage (RWFB) companies.

Overall, RWFB companies aligned with the aggregate views from organizations across all industries in the global survey regarding cyber risks. But digging a bit deeper, we found that company size, as determined by revenue bands, was a significant differentiator in the views expressed by RWFB respondents.

Smaller companies, particularly those with less than $100 million in annual revenue, appear to be generally less prepared for managing and mitigating cyber risk than their larger industry peers. For example, and perhaps most importantly, smaller companies generally are not as confident as larger ones in their cyber risk management capabilities.

Whether that is due to perceptions around available resources and/or expertise, it is an important point to address and one that RWFB organizations and their cyber risk management advisors should be looking at closely.

The 2019 survey findings focused on five important concepts that underscore the state of enterprise cyber risk in today's RWFB business context:

1. Overall, companies' concern about cyber risk increased since 2017, but belief in their ability to manage cyber risk — their cyber confidence — declined. As noted, this is particularly true for smaller RWFB companies.
2. Globally, organizations exhibit dissonance between their perception of cyber as a top-priority risk and their approach to managing it. RWFB organizations also saw supply chain and reputation as top risks.
3. RWFB organizations lag those in other industries in the use of economic quantification to measure cyber risk exposures. And, more critically, small and midsize RWFB organizations are much less likely to recognize their risks or to invest in cyber insurance.
4. Despite embracing technology and digital innovation, organizations have considerable uncertainty about the degree of cyber risk such new technologies bring. More than in most industries, RWFB firms tend to believe the benefits of technology adoption outweigh potential harms.
5. The digitization of supply chains brings benefits, but many companies, RWFB and others, don't fully appreciate the interdependency of roles and their own responsibilities within the supply chain, especially larger enterprises.

We hope this look at how RWFB companies responded to the survey helps your company navigate the evolving cyber risk landscape.

Cyber Risks Rise as a Top Concern for Retail, Wholesale, Food, and Beverage Companies

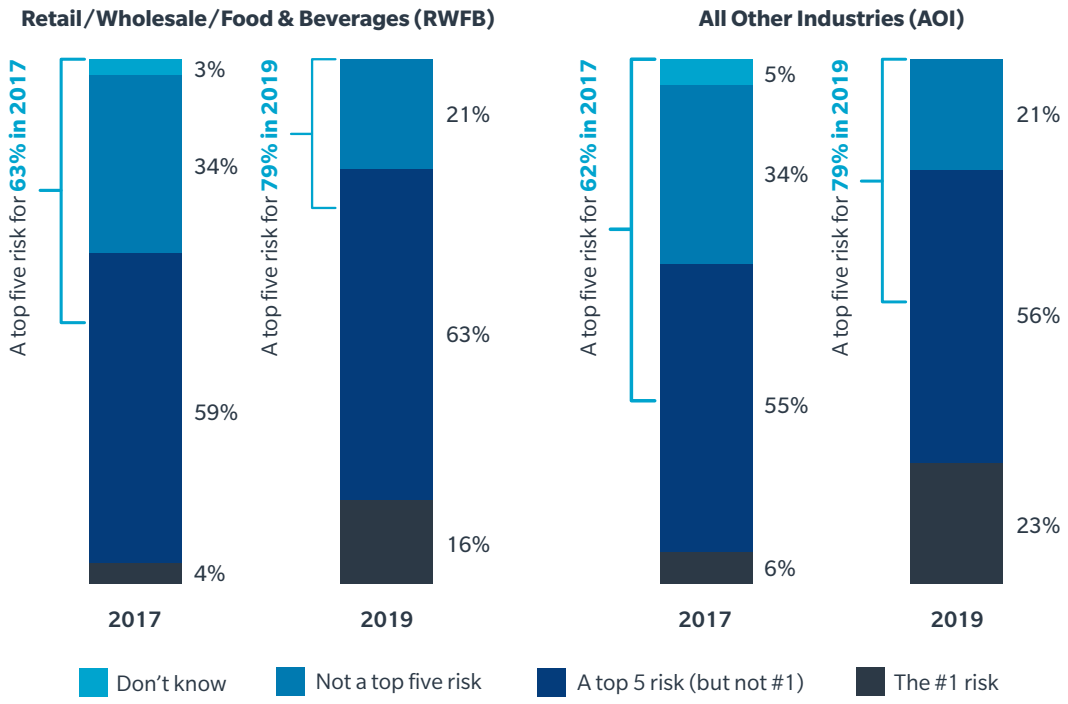
The past two years have seen a significant increase in the number of retail, wholesale, food, and beverage (RWFB) organizations that consider cyber risks to be a top threat.

In the *2019 Cyber Risk Perception Survey,* 79% of RWFB respondents ranked cyber threats as a top five risk, up from 63% in 2017 (see Figure 1).

FIGURE 1

RWFB firms rank cyber risks as a top business concern.

Q: Of the following business threats, please rank the top 5 that are the biggest concerns to your organization? (Results for *"Cyber-attacks/Cyber Threats"* shown)



Base: All answering; n=140 (RWFB 2017) & n=166 (RWFB 2019); n=1,234 (AOI 2017) & n=1,346 (AOI 2019).

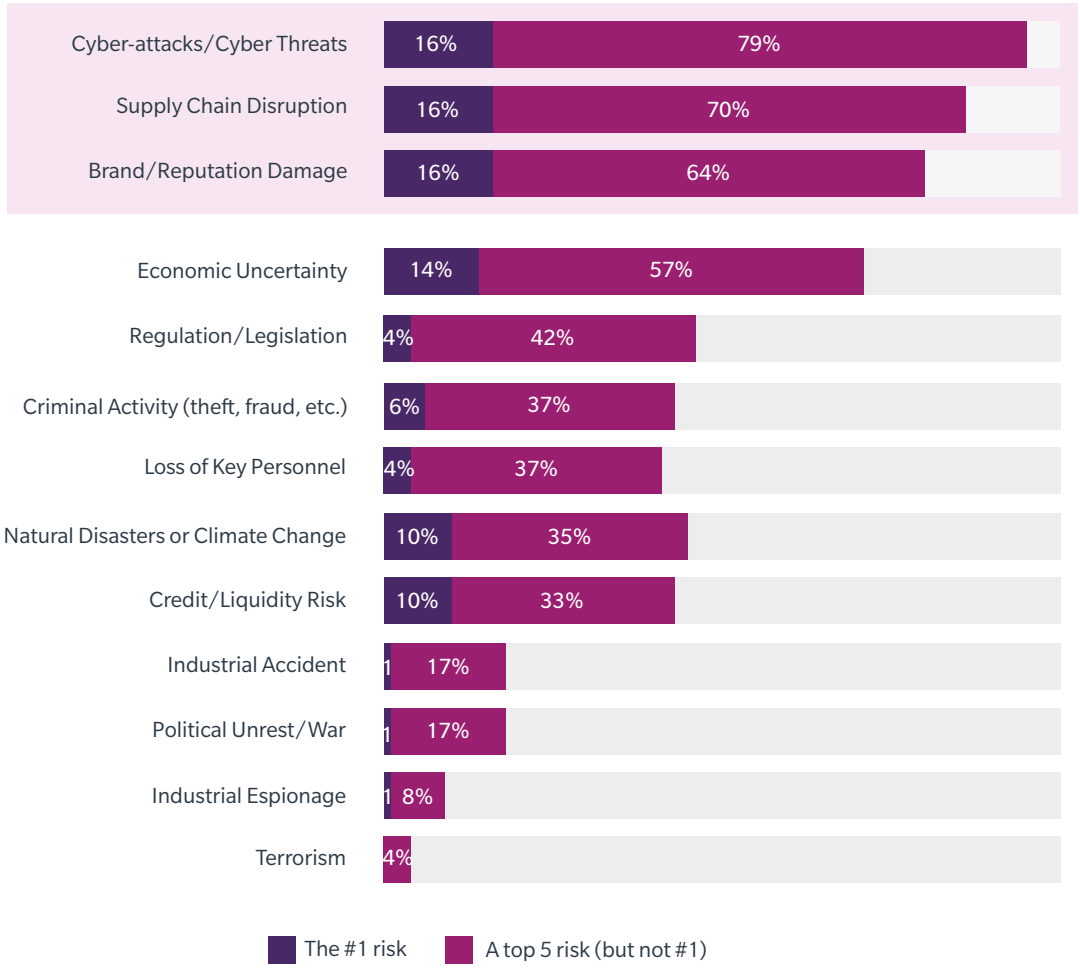
At the same time, the percentage of RWFB companies ranking cyber threats as their number one concern quadrupled, from 4% to 16%, closely aligning with the view in other industries.

Nearly 80% of RWFB companies in 2019 viewed cyber-attacks and threats as a top 5 risk, with supply chain disruption and brand/reputation damage ranking equally as high (see Figure 2).

FIGURE 2

No. 1 business threats for RWFB: cyber, supply chain, and reputation.

Q. Of the following business threats, please rank the top 5 that are the biggest concerns to your organization.



Base: All answering; n=166 (RWFB 2019); n=1,234 (AOI 2019).

Cyber Confidence Aligns with Other Industries

The 2019 survey measured confidence in three critical areas that collectively contribute to a company's overall cyber resilience:

1. **Understanding, assessing, and measuring potential cyber risks.** Insights, tools, and capabilities that allow companies to accurately gauge, compare, and calculate the types and levels of cyber risks faced, along with sources, drivers, and potential mitigating actions.

2. **Preventing and/or mitigating cyber risks.** A mix of technical and non-technical safeguards that help to lower cyber risks, deter potential cyber threats, and reduce or minimize any harms or losses suffered from a given cyber risk incident.

3. **Managing, responding to, and recovering from cyber events.** Well-rehearsed contingency plans, internal resources, and external experts who can help companies minimize the negative consequences and recovery time after an incident.

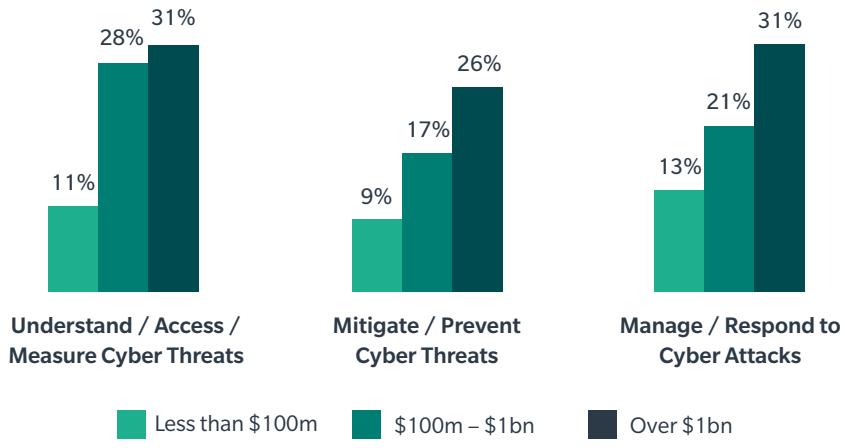
RWFB companies are generally aligned with other industries as to their confidence in each of the three areas of cyber resilience. For each criterion, from 20% to 25% of all organizations are highly confident and about 60% are fairly confident, with the remainder being not at all confident.

Confidence in cyber resilience capabilities varies significantly among RWFB companies based on organization size (measured by annual revenue), with confidence generally higher among larger companies (Figure 3). The confidence/size correlation may be attributable to the presumably greater resources and expertise that larger companies can devote to cyber risk. Small companies thus present an opportunity for cyber risk mitigation professionals to deliver cost-effective tools.

FIGURE 3

Confidence in cyber resilience increases with organization size.

Q: For each of the following, please indicate your level of confidence in your organization's ability to... (Percentage of RWFB organizations "Highly Confident" in each area, by annual revenue.)



Base: All RWFB companies answering (2019); n=52 (less than $100m); n=44 ($100m to $1bn); n=57 ($1bn or more).

Challenges to Managing Cyber Risk

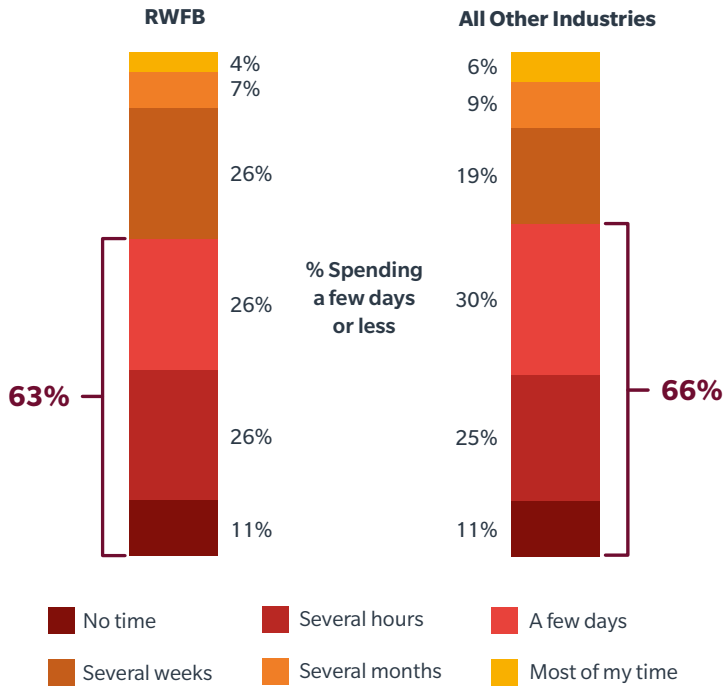
Across industry sectors, the main challenges to effective cyber risk management center on keeping pace with new risks and having adequate staff time, internal expertise, and budget for cyber resilience and risk management.

The increasing number of attacks on consumer data held by RWFB companies has undoubtedly put cyber risk at the center of many board and C-suite agendas. However, for the majority of companies across industries, nearly two-thirds of decision-makers say they spent only a few days or less focused on cyber risk and cybersecurity over the prior year (see Figure 4). This shows a need for prioritization of cyber risk management. RWFB companies, and others, could benefit from increasing the amount of time senior leaders devote to addressing this critical risk issue.

FIGURE 4

Decision-makers spend only a few days per year focusing on cyber risk.

Q.Over the past 12 months, approximately how much of your total professional time has been spent on cyber risk and/or cybersecurity?



Base: All answering excluding "Don't Know" responses; n=156 (RWFB 2019); n=1,266 (AOI 2019).

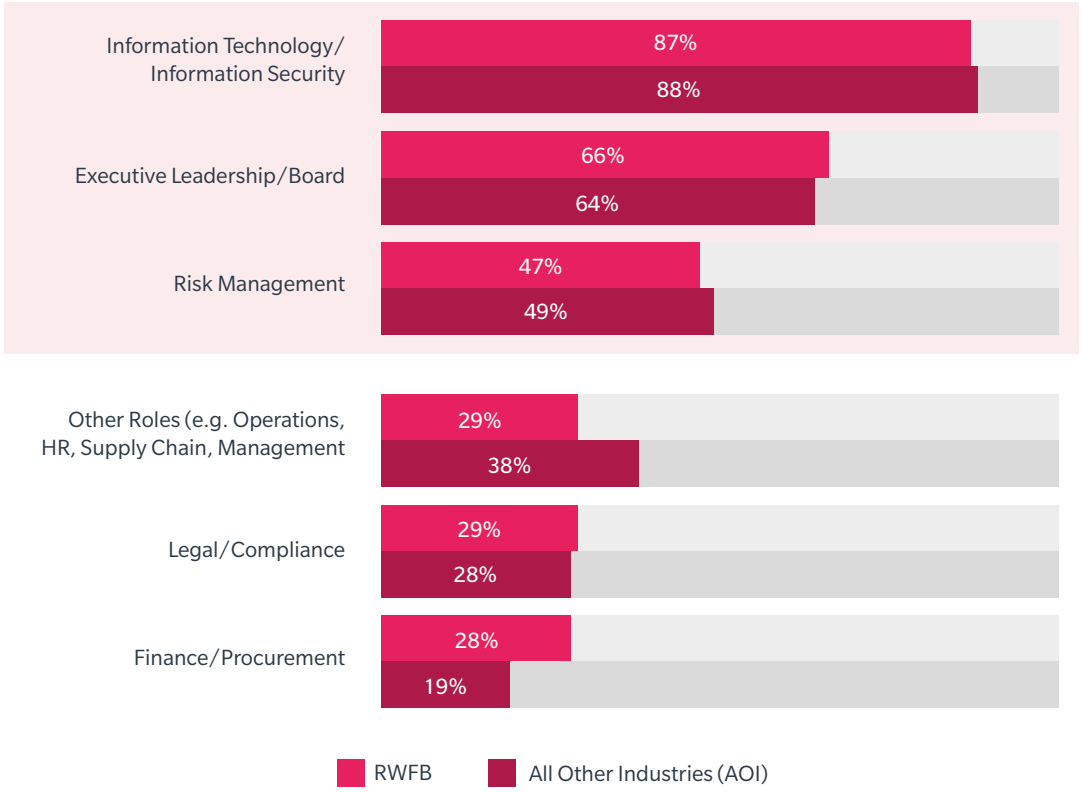
Stakeholder ownership of cyber risk is another area where RWFB companies align with other industries. The information technology (IT) function is named by more than 80% of respondents as a primary owner of cyber risk management.

Most companies cite substantial involvement from executive leadership/board members, but markedly less from risk management professionals (see Figure 5).

FIGURE 5

Cyber risk management at RWFB firms driven by IT/InfoSec, executive leadership, and risk management.

Q. Please rank the three functions that are the main owners or drivers of cyber risk management in your organization.



Base: All answering; n=166 (RWFB 2019); n=1,347 (AOI 2019).

About 30% of RWFB respondents report that legal/compliance, finance, and/or other functions have some ownership role in cyber risk management, which is a significant variation compared to non-RWFB organizations. Clearly, there is an opportunity for the risk management function to take greater ownership of cyber risk oversight.

Although senior leaders play a role in championing cyber risk management at most RWFB organizations, the fact that IT is listed by 87% as a primary owner reflects a misunderstanding held by many companies that cyber threats are primarily a technology issue.

Building a Case for Investment in Cyber Risk Mitigation

Without rigorous economic measurement of cyber risk exposures, companies may be challenged or prevented from clearly understanding the potential financial impact of a cyber incident. This, in turn, hampers the ability to develop adequate risk management strategies and allocate investments proportionate to the level of risk.

The 2019 survey shows that companies that have adopted quantitative methods of assessing or expressing their cyber risk exposures are:

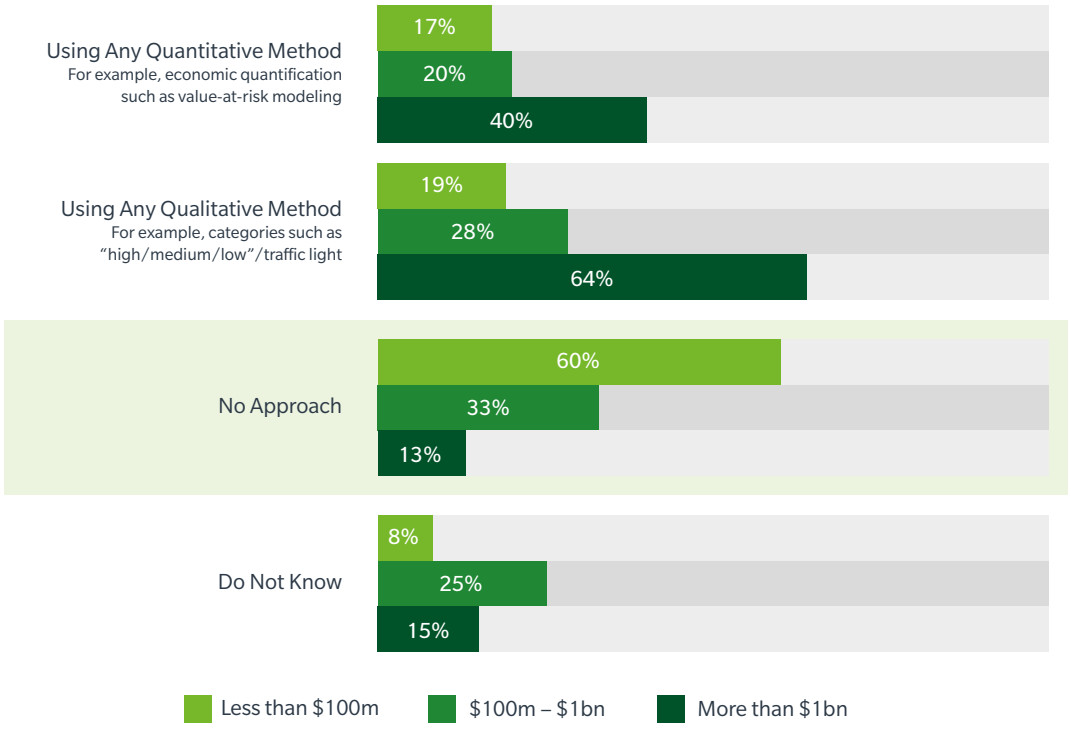
- More confident in their core capabilities to prevent and mitigate cyber risks.
- More certain that they are spending and staffing against cyber risks at levels appropriate to current and future exposures.

The methods that organizations use to measure and express their cyber risk exposures is a foundation for strategy formation, smart budget planning, and effective cyber risk management. Although more RWFB companies implemented quantitative risk assessment methods in 2019 — 26% compared to 11% in 2017 — progress has not been consistent across the industry. Again, company size is a factor, with large enterprises more than twice as likely as others to use quantitative and/or qualitative risk assessment methods (see Figure 6).

FIGURE 6

Use of formal cyber risk assessment varies among RWFB organizations.

Q. In general, how does your organization measure or express its cyber risk exposure?



Base: All answering; n=166 (RWFB 2019); n=1,347 (AOI 2019).

Among small RWFB organizations, 60% use no formal approach to gauge their exposure to cyber risks. By comparison, only 33% of midsize companies and 13% of large enterprises have no method. The top five reasons cited by RWFB companies for not assessing cyber risk exposures are lack of internal expertise, internal consensus, necessary data, budget, and lack of justification by level of exposure.

Notably, both small and midsize RWFB companies are about 10 times more likely than large companies to say that their current level of risk exposure does not justify the cost and effort involved in implementing quantitative or economic measurement frameworks. This perception is likely a fundamental barrier stopping small and midsize RWFB organizations from improving their approach to cyber risk assessment. And it can become a vicious cycle: Without an accurate assessment of exposure, many companies will not recognize their vulnerabilities or the need for more resources.

The adoption of cyber insurance is closely linked to economic measurement of cyber risk exposure. The survey finds that, in all industries, organizations that use quantitative cyber risk assessment methods are significantly more likely to purchase cyber insurance than those that use only qualitative assessments or no formal assessment methods at all. Overall, 48% of RWFB companies currently have cyber insurance, and 18% plan to purchase it within the next year, close to the 45% and 19%, respectively, for organizations in all other industries (see Figure 7).

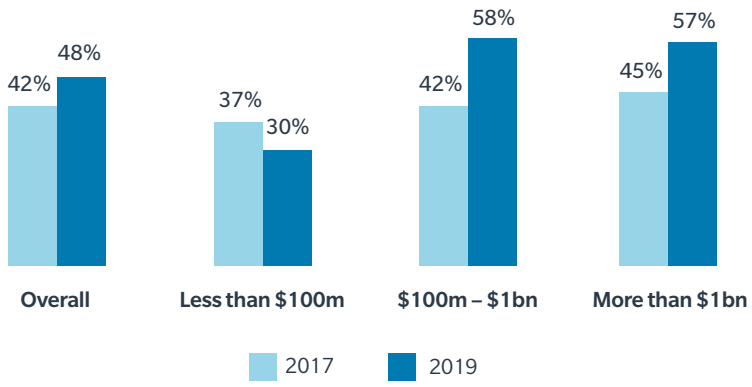
Survey responses by RWFB organizations show a clear divergence over the past two years in cyber insurance trends between smaller RWFB organizations and larger ones. In 2017, the share of small, midsize, and large RWFB companies with cyber insurance was similar, at 37%, 42%, and 45%, respectively. In 2019, the majority of midsize and large RWFB companies had cyber insurance, while the share of small companies with coverage decreased.

This decline in cyber insurance among smaller RWFB companies is concerning given that the volume, variety, and economic impact of cyber threats faced by businesses of all sizes increased over the same period.

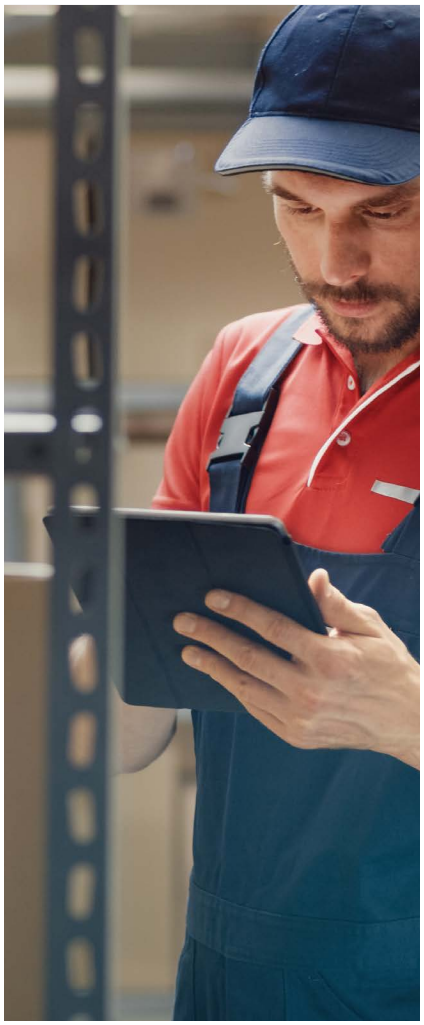
FIGURE 7

Smaller RWFB organizations less likely to have cyber insurance.

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



Base: All answering; n=100 (RWFB 2017); n=114 (RWFB 2019).



Cyber Risk Mitigation Activities and Investments

RWFB organizations generally kept pace with others in implementing various cyber risk mitigation actions. The majority of organizations shored up technical and cybersecurity defenses, and most improved or updated policies and procedures related to cyber risk mitigation and incident response planning within the past 24 months.

Fewer RWFB companies have undertaken activities to improve the assessment and understanding of cyber risks, which indicates a potential blind spot that these organizations would be well-advised to address.

The variance by RWFB organization size continues in additional areas of cyber risk management. Smaller RWFB companies significantly trail their midsize and large counterparts in nearly all risk assessment and resilience activities (see Figure 8). These include:

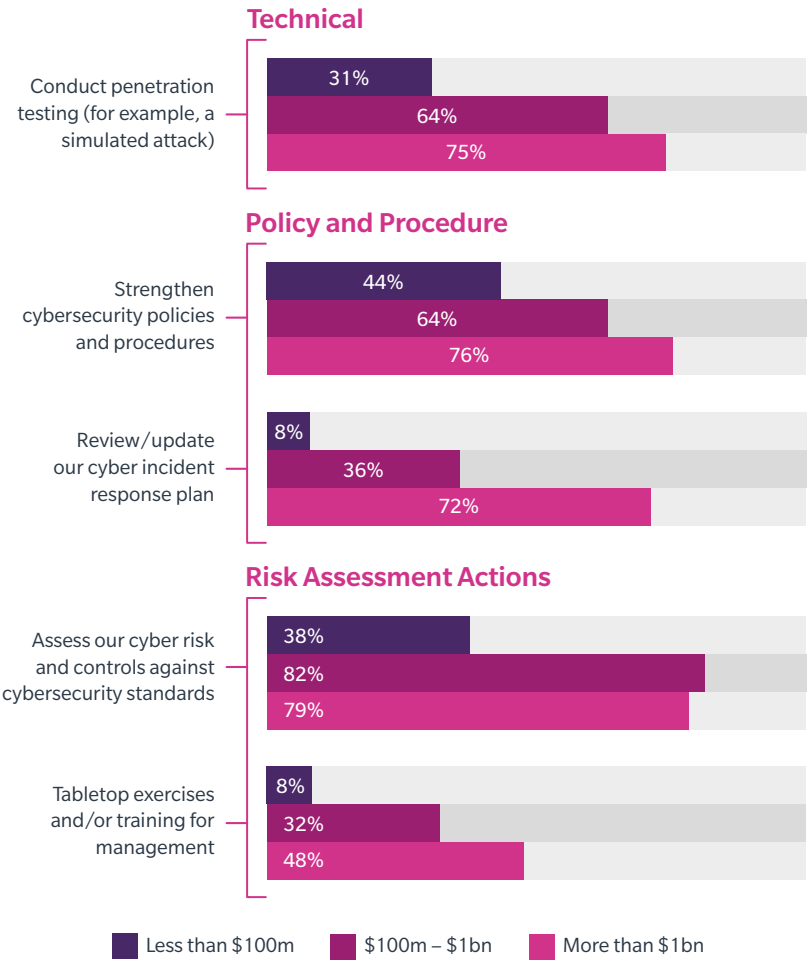
- Conducting penetration testing.
- Strengthening cybersecurity policies and procedures.
- Reviewing and updating cyber incident response plans.
- Assessing cyber risks and controls against cybersecurity standards.
- Engaging in tabletop exercises and/or management training related to cyber risks.

This signals a clear need for small RWFB companies to increase their activity and preparedness levels across all three areas of cyber risk resilience, not just technical prevention.

FIGURE 8

Small RWFB organizations less likely to take key risk mitigation steps.

Q: Please indicate whether your organization has taken the specific actions listed below within the past 12 to 24 months.



Base: All answering: n=76 (RWFB 2019); n=619 (AOI 2019).

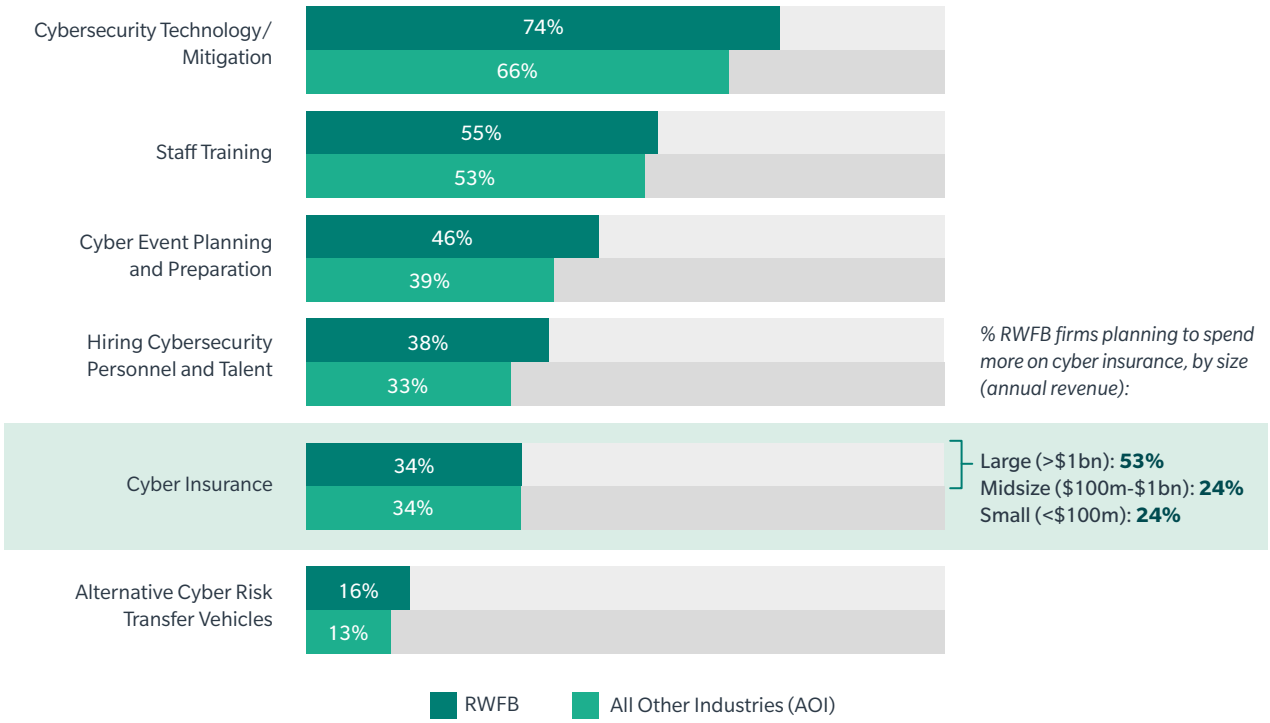
Many organizations cite risk audit or improvement actions suggested by external advisors and qualitative cyber risk assessments as influencing their investment decisions related to cybersecurity/technology and resilience-building initiatives. Regarding investments in cyber insurance, however, RWFB companies tend to cite the organization's overall risk tolerance and peer benchmarking as the main influences in determining spending.

RWFB companies' cyber risk investment plans over the next three years closely mirror those of other industries (see Figure 9). Many plan to increase investments in cybersecurity technology, mitigation, and staff training related to cyber risks. Some 46% of RWFB organizations plan to increase spending on cyber event planning and preparation, compared to 39% in other industries, while 38% plan to spend more on hiring cybersecurity staff and enhancing their talent and expertise.

FIGURE 9

Most RWFB firms plan to increase spending on cyber risk management.

Q: How do you expect your investment allocations in the following areas of risk management to evolve over the next three years?



Base: All answering; n=90 (RWFB 2019); n=759 (AOI 2019).

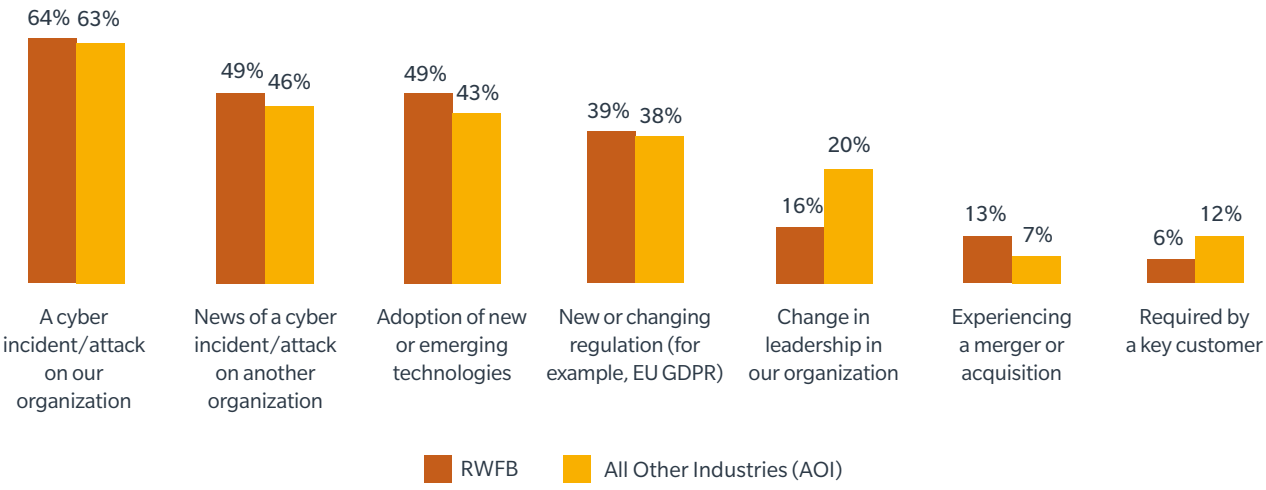
Planned investments generally appear to be focused on cybersecurity technology and prevention efforts as opposed to other preparation or resilience-building efforts. Most companies seem to give low priority to hiring cybersecurity personnel — a potential concern as lack of internal expertise can be a primary barrier in addressing cyber risk exposures quantitatively.

Regarding impacts on future cyber risk management investment, the RWFB industry closely mirrors other industries: Most cite cyber incidents or attacks on their own organization, attacks on other organizations, and adoption of new technologies (see Figure 10).

FIGURE 10

Cyber-attacks are biggest triggers for increasing investment in cyber risk management.

Q: Which factor will have the biggest impact on your organization's planned increase in budget allocation for the following areas of cyber risk management?



Base: All answering; n=70 (RWFB 2019); n=545 (AOI 2019).

Cyber Risks Posed by New Technologies

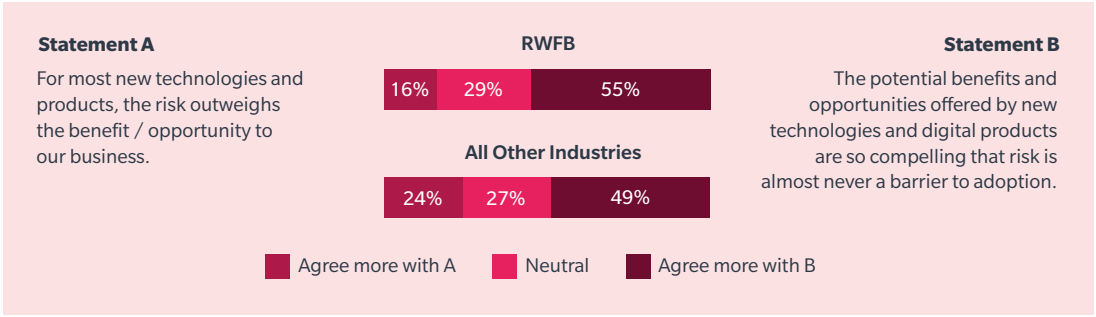
The potential cyber risk associated with new technologies generally does not inhibit RWFB organizations from adopting them.

Regarding the relative risk-reward around new technologies, RWFB organizations are more likely than others to say the benefits outweigh the potential harms (see Figure 11).

FIGURE 11

Most RWFB firms agree that benefits of new technologies outweigh the risks.

Q: For each of the following pairs of statements, please indicate which most strongly reflects your organization's attitude.



Base: All answering; n=89 (RWFB 2019); n=740 (AOI 2019).

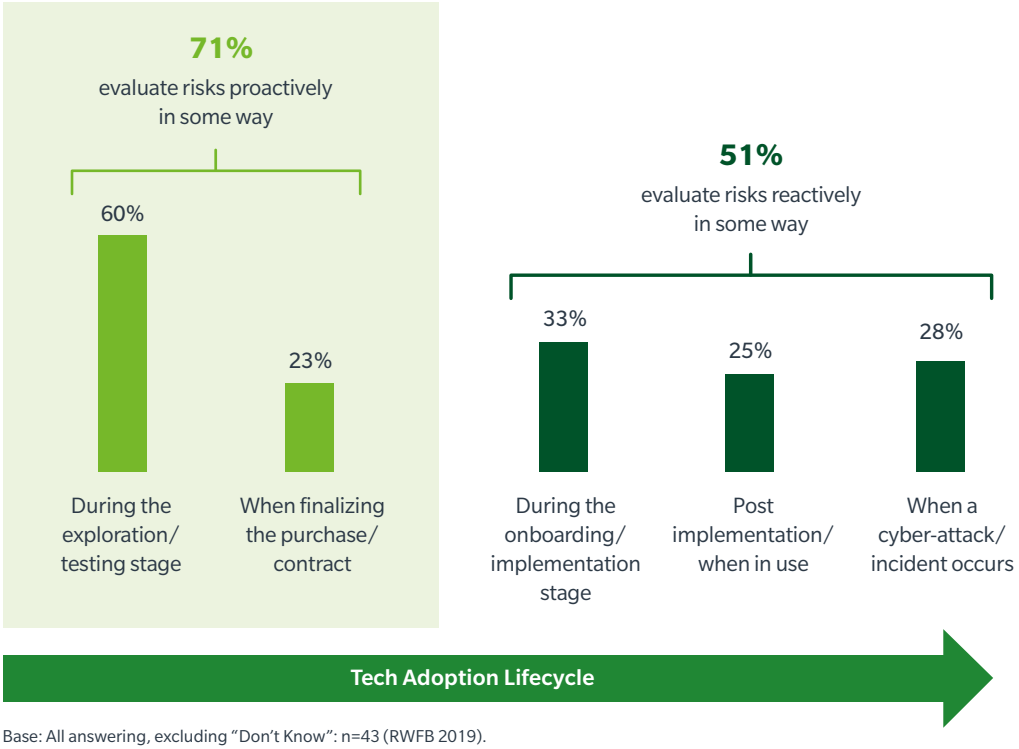
Assessing risk exposures both prior to and following the adoption of new technologies can help organizations understand the potential issues that can occur throughout the lifecycle of the technology, including cyber risks that may develop in the course of integration with other systems and tools.

Yet most RWFB companies evaluate cyber risk primarily during the exploration and testing stage of new technology implementation (see Figure 12). Significantly fewer companies continue to evaluate cyber risks at later stages, and only 5% say they evaluate risks at every stage. These results largely mirror those of all industries.

FIGURE 12

Only 5% of RWFB companies evaluate cyber risks throughout the lifecycle of new technologies.

Q: When adopting and implementing new technologies, at which of the following stages is cyber risk typically evaluated in your organization?



Base: All answering, excluding "Don't Know": n=43 (RWFB 2019).

Only 28%... *evaluate risks proactively and reactively*

Just 5%... *evaluate risks at all possible stages of the lifecycle*

And 8%... *don't evaluate risks at all*

Cyber Risks from Third-Party Suppliers

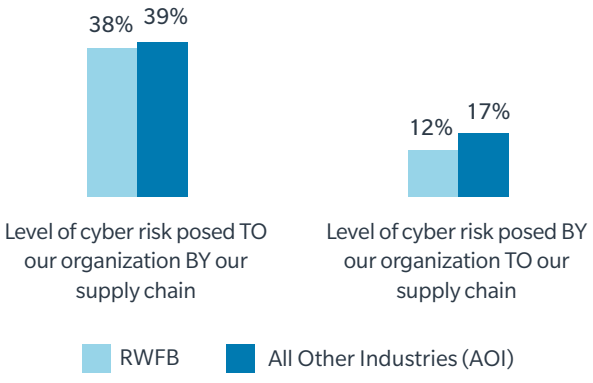
Another important cyber risk vector affecting most organizations is through the supply chain — vendors and commercial partners. This risk can "flow" both ways: Vendors can pose cyber risks to those they supply, but that organization, too, may present cyber risks to its suppliers.

The global survey showed that organizations generally tend to perceive the level of risk posed to their organization by their supply chain to be greater than the risk they pose back to third parties. RWFB companies are three times more likely to perceive somewhat high or very high cyber risk posed to their organization by their supply chains than vice versa (see Figure 13).

FIGURE 13

RWFB companies are apt to perceive greater cyber risk posed to their organization by supply chain partners than vice versa.

Q: What level of cyber risk is posed to your organization BY its supply chain/3rd parties? And the reverse: What level of cyber risk does your organization pose TO its supply chain/3rd parties?



Base: All answering: n=82 (RWFB 2019); n=711 (AOI 2019).

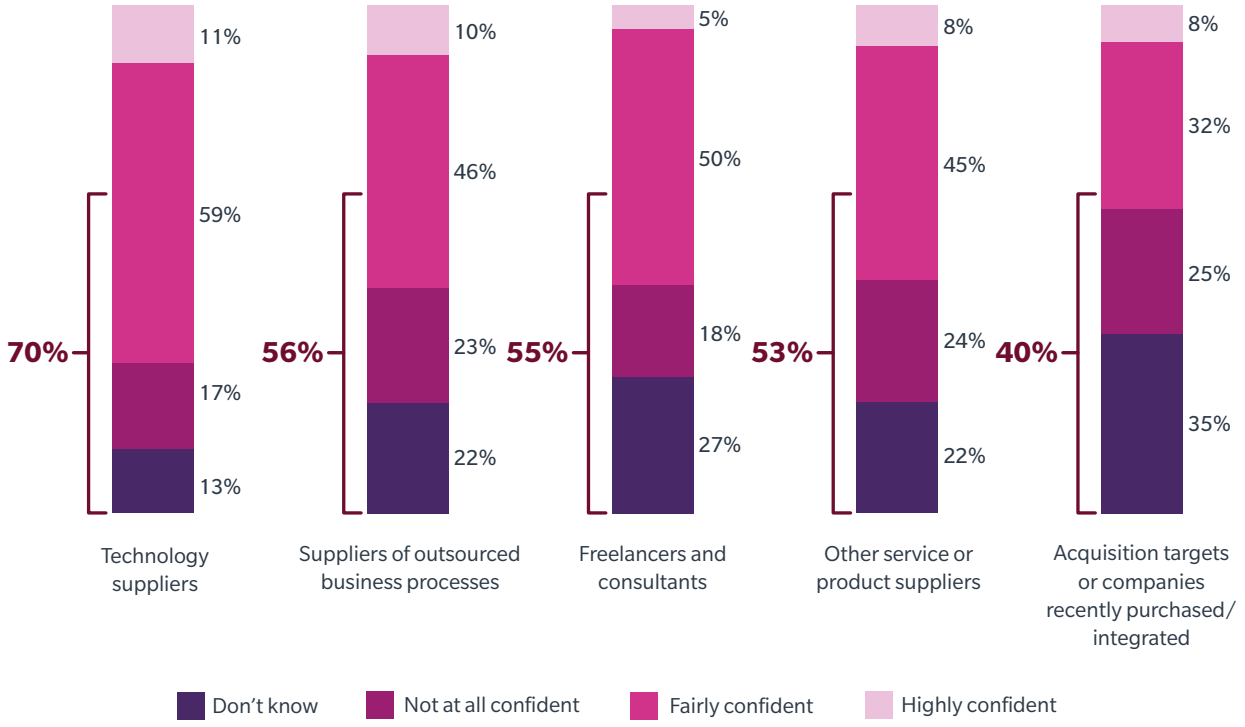
The majority of RWFB respondents say they have fair or high confidence in their ability to mitigate cyber risks from various third parties (see Figure 14).

Confidence levels are especially high around mitigating risks from technology suppliers, and lowest related to acquisition targets or companies recently integrated into their operations.

FIGURE 14

RWFB firms are confident in their ability to mitigate cyber risk from suppliers and other third parties.

Q: How confident are you in your organization's ability to prevent/mitigate cyber risk from the following...?



Base: All answering excluding "Don't Know" responses; n=156 (RWFB 2019); n=1,266 (AOI 2019).

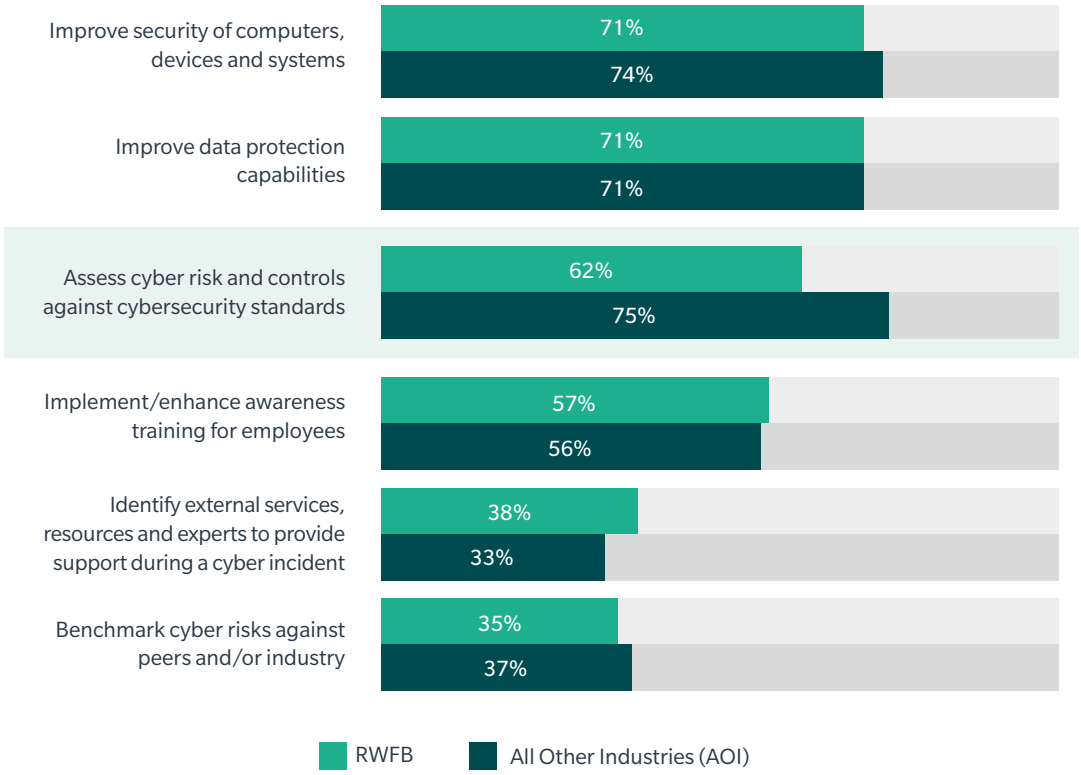
Most RWFB organizations expect their supply chain partners to implement cybersecurity initiatives and improvements similar to those they take themselves.

In particular, most RWFB organizations expect suppliers and third-party partners to improve the security of computers, platforms, and systems; to improve data protection capabilities; and to implement cyber risk awareness training for employees (see Figure 15).

FIGURE 15

RWFB companies are less likely to expect suppliers to assess cyber risks and controls against cybersecurity standards.

Q: What cybersecurity measures do you expect your supply chain partners/3rd parties to take?



Base: All answering; n=166 (RWFB 2019); n=1,347 (AOI 2019).

Conclusion

The 2019 survey shows that retail, wholesale, food, and beverage companies generally align with organizations in other industries when it comes to initiatives, plans, and perceptions of cyber risk. However, there are clear differences between companies of different sizes within the RWFB industry around various cyber risk perceptions. Smaller RWFB companies should make a concerted effort to match the risk management practices of their midsize and larger enterprise counterparts, particularly in the key areas of cyber resilience and risk assessment activities. These will become more critical as cyber risks grow in frequency and methods, and as smaller companies prove to be attractive and vulnerable targets for cyber-attackers.

Methodology

This report is based on findings from the *2019 Marsh Microsoft Global Cyber Risk Perception Survey* administered between February and March 2019.

Overall, 1,500 business leaders participated in the global survey, representing a range of key functions, including risk management, information technology/information security, finance, legal/compliance, C-suite officers, and boards of directors.

Survey Demographics

Geography

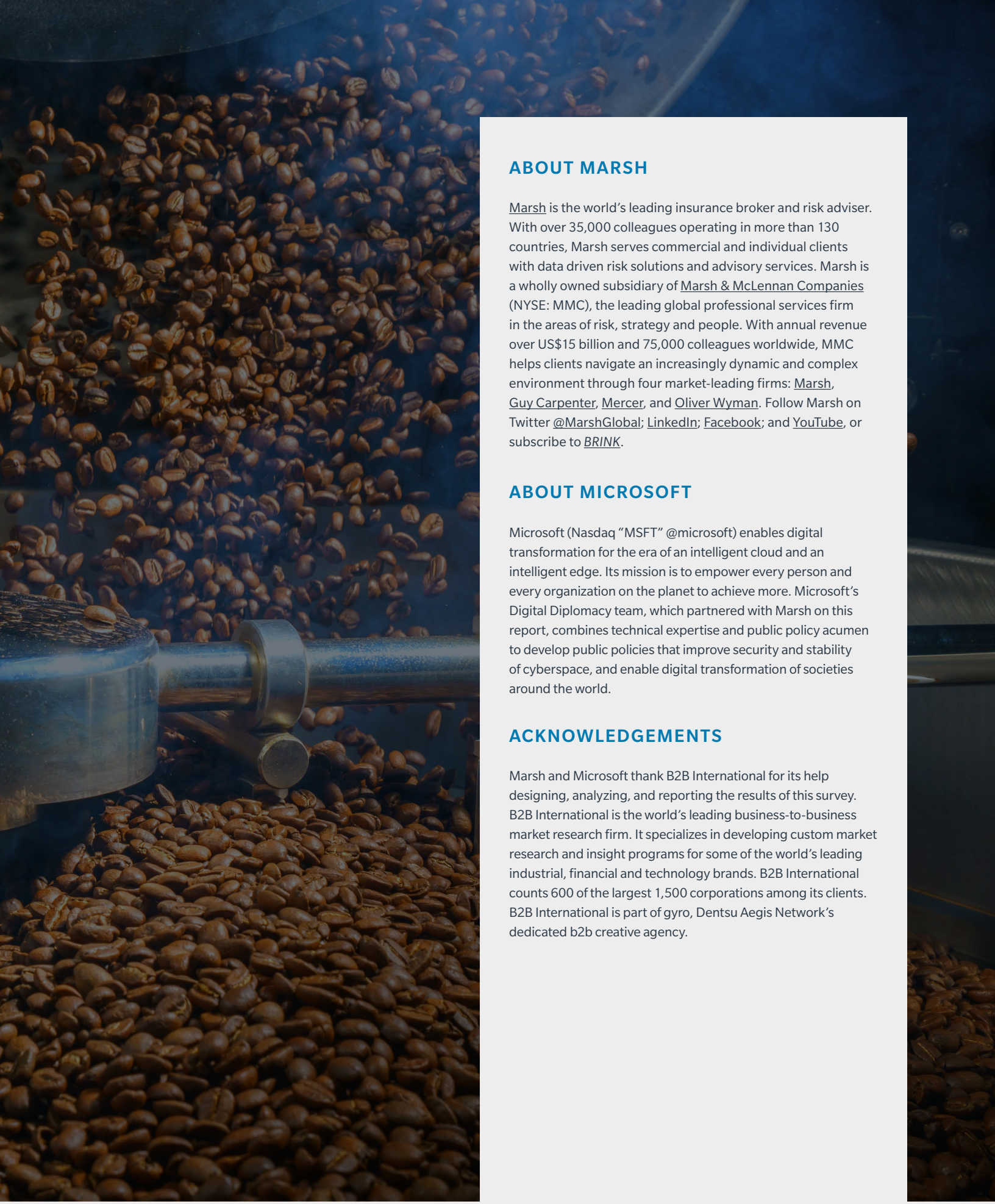
Where the 1,500+ survey respondents are based professionally	
Latin America and Caribbean	35%
Europe	35%
United States and Canada	22%
Asia and Pacific	6%
Middle East and Africa	2%

Revenue

Total annual revenue of survey respondents' business organizations, in US dollars	
More than $5 billion	10%
$1 billion - $5 billion	15%
$250 million - $1 billion	17%
$100 million - $250 million	14%
$25 million - $100 million	21%
Less than $25 million	23%

Industries

Industry sectors in which survey respondents' organizations primarily operate	
Manufacturing/Automotive	16%
Retail, Wholesale, Food, and Beverage	11%
Financial Institutions	9%
Energy/Power	8%
Health Care/Life Science	7%
Transportation/Rail/Marine	6%
Communications, Media and Technology	5%
Professional Services	5%
Real Estate	4%
Chemical	4%
Construction	4%
Education	4%
Public Entity/Nonprofit	4%
Mining/Metals/Minerals	2%
Aviation/Aerospace	1%



ABOUT MARSH

Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. 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$15 billion and 75,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms: Marsh, 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. Microsoft's Digital Diplomacy team, which partnered with Marsh on this report, 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.

ACKNOWLEDGEMENTS

Marsh and Microsoft thank B2B International for its help designing, analyzing, and reporting the results of this survey. B2B International is the world's leading business-to-business market research firm. It specializes in developing custom market research and insight programs for some of the world's leading industrial, financial and technology brands. B2B International counts 600 of the largest 1,500 corporations among its clients. B2B International is part of gyro, Dentsu Aegis Network's dedicated b2b creative agency.

For more information about Marsh's cyber risk management solutions, contact cyber.risk@marsh.com or your Marsh representative: www.Marsh.com.

To learn more about Microsoft's security offerings, visit www.Microsoft.com/security.