

2019 Global Cyber Risk Perception Survey

Manufacturing Industry Report





PLANNED

Time in Planned Downtime

01:29:18

Time in Planned Downtime Job / Shift

01:29:18 / 01:29:18

DOWNTIME

Time in Downtime

01:29:18

Time in Downtime Job / Shift

01:29:18 / 01:29:18

SETUP

Time in Setup

01:29:18

Time in Setup Job / Shift

01:29:18 / 01:29:18

RUNNING

Time in Running

01:29:18

Time in Running Job / Shift

01:29:18 / 01:29:18



SLEEVES IN

245649/900000

SLEEVES OUT

245617/900000

SHIFT

JOB

OUT

EVENTS

STARTS

Wi-Fi, Settings, and other system icons

2019 Global Cyber Risk Perception Survey

CONTENTS

- 01 Introduction
- 02 Survey Highlights
- 04 Cyber Risk Dissonance: Priority Increases, Confidence Declines
- 10 New Technology Brings Increased Cyber Exposure
- 16 Supply Chain Risk: Moving to Technological Social Responsibility
- 20 Appetite for Government Role Draws Mixed Views
- 22 Cyber Risk Investments Focus on Prevention, Not Resilience
- 31 Conclusion

Introduction

As much as any industry, manufacturing is undergoing rapid transformation driven by continual advances in areas ranging from artificial intelligence and the Internet of Things (IoT) to autonomous technology and data availability. And while the speed of change keeps increasing, cyber risks seem to evolve even faster.

We've seen cyber risk move beyond data breaches and privacy concerns to complex schemes capable of disrupting entire businesses, industries, and supply chains. As risk professionals and other leaders in the manufacturing sector are learning, cyber risk can be mitigated, managed, and recovered from, but not eliminated.

The recently released *2019 Global Cyber Risk Perception Survey* from Marsh and Microsoft builds on a related survey conducted in 2017, and released in 2018. It explores cyber risk perceptions and risk management at organizations worldwide, especially in the context of a rapidly evolving business technology environment. In this industry-focused report of 2019 data, we look at how respondents from manufacturing organizations perceive and manage cyber risk.

Overall, manufacturers' perception of cyber threats mirrored other industries: The concern level has increased since 2017, but belief in their ability to manage cyber risk — their cyber confidence — declined.

One key difference between manufacturers' perceptions of cyber risk compared to other industries is in the level of concern regarding supply chain risk — manufacturers rank supply chain risk third in their list of concerns, after cyber threats and economic uncertainty, whereas other industries rank it seventh.

There are some interesting nuances to how manufacturers see the interplay between cyber threats and supply chain risk; for example, while supply chain risk ranks higher on the concern list for manufacturers than for other industries, perceptions of risk posed by supply chain partners are significantly lower among manufacturers than in other industries — a somewhat counterintuitive finding.

We also found that our manufacturing based respondents were less likely than those companies in other industries to employ an economic approach to measuring or expressing their cyber risk and a larger number had no method at all to do so. Likewise, fewer manufacturers have implemented key cyber risk resilience actions such as training, loss modelling, supply chain risk assessment, or updating cyber event response plans, focusing instead on technical, preventive actions.

We hope you find the manufacturing-focused *2019 Global Cyber Risk Perception Survey Report* to be a useful tool in generating discussion in your organization and with your external advisors as you navigate the rapidly evolving cyber risk landscape.

We encourage all companies to build cyber resilience, and to approach cyber risk as a critical threat that, with vigilance and application of best practices, can be managed confidently. Finally, we thank the many clients and others who shared their perspectives on this important topic.

Manufacturers See Cyber Risk as a Top Concern

Manufacturers globally reported a sharp rise in concern between 2017 and 2019 regarding cyber-attacks and cyber threats.

More than three-quarters (76%) of manufacturing organizations responding to the Marsh Microsoft *2019 Cyber Risk Perception Survey* ranked cyber risks in the top five concerns for their organization — similar to the 80% of organizations in other industries that said the same (see Figure 1).

There was also a sizable spike since 2017 — to 22% in 2019 — in the number of manufacturers and others citing cyber risks as their organizations’ number one risk concern.

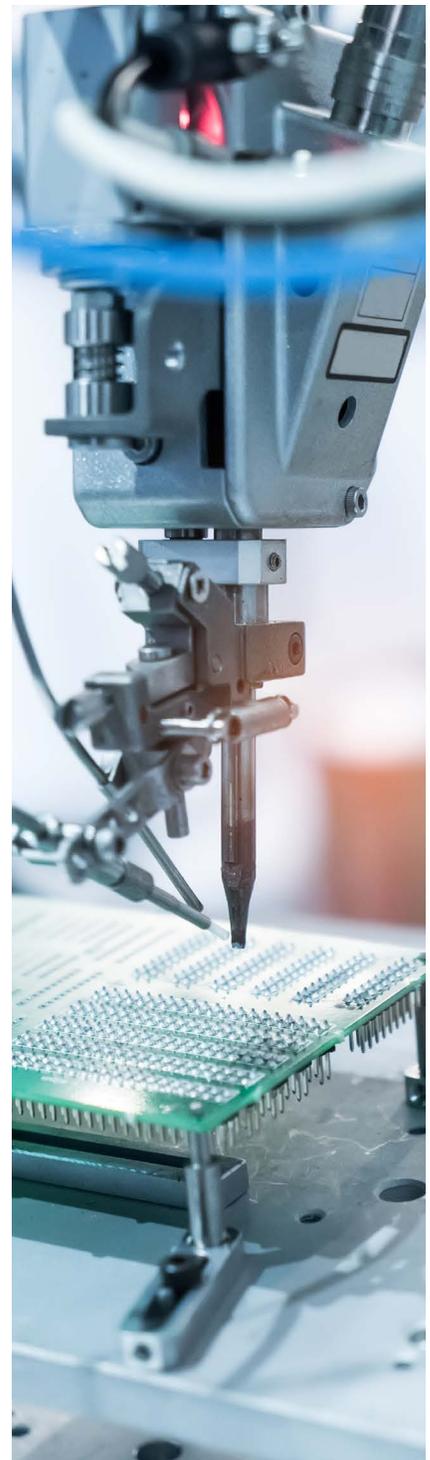


FIGURE 1
1

Cyber risk is a top-five concern for manufacturing organizations, with 22% ranking it #1.

Q. Of the following business threats, please rank the top 5 that are the biggest concerns to your organization (cyber-attacks/cyber threats shown).



Driven in part by the steady drumbeat of incidents in the news, cyber risks have risen above all other strategic business concerns for most organizations in manufacturing as well as all other industries (see Figure 2).

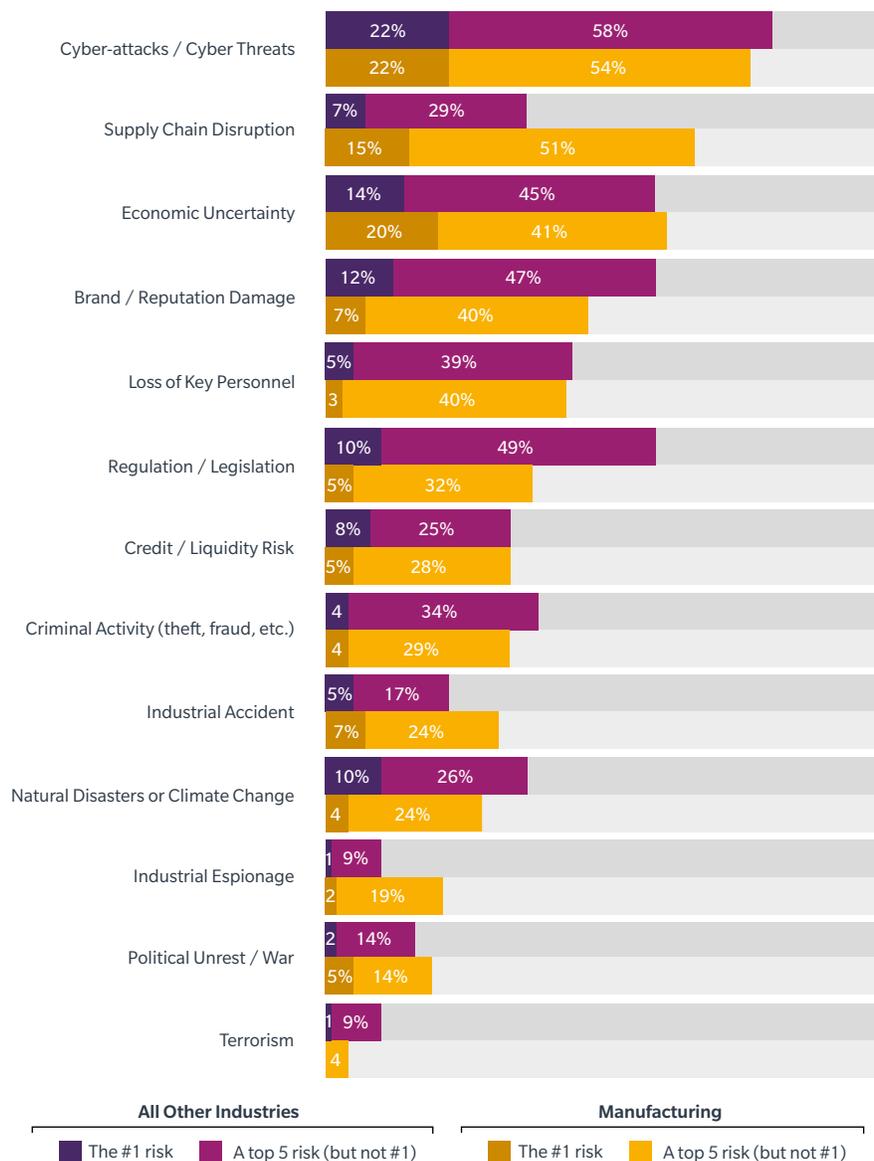
At the same time, manufacturers were significantly more likely than firms in other sectors to cite supply chain disruption as a top-five concern — 66% vs. 36%, respectively. In fact, 15% of manufacturing firms view supply chain disruption as the number one risk to their business, versus just 7% of organizations in other industries.

The main driver of this difference is likely to be the crucial role that supply chains, and supply chain partners, play in the core business operations of manufacturers relative to companies in other industries.

FIGURE 2

Cyber risks are the top concern for manufacturing organizations; supply chain disruptions are also high on the list.

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



Confidence in Cyber Resilience Falls for Manufacturers and Others

While organizational concern over cyber risks surged over the past two years, there was a simultaneous decline in organizations' confidence around overall cyber resilience.

We asked respondents to rate current confidence levels across three key areas of cyber resilience — understanding/assessing, mitigating/preventing, and managing/responding to cyber risks. Manufacturing organizations and firms in all other industries reported lower levels of confidence in all three areas in 2019 than in 2017.

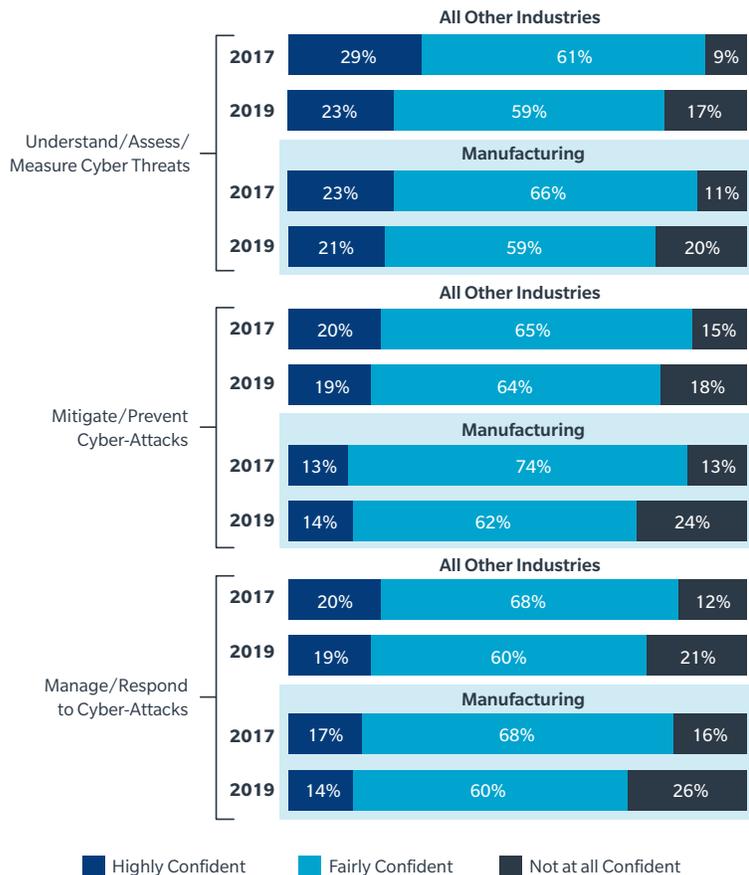
Moreover, manufacturers now consistently rate their confidence levels lower across all three areas of cyber resilience than do organizations in other industries. Almost twice as many manufacturing firms claim they are “not at all confident” in their capabilities to mitigate/prevent or manage/respond to cyber-attacks than said they are “highly confident” around these two areas.

Almost twice as many manufacturing firms claim they are “not at all confident” in their capabilities to mitigate/prevent or manage/respond to cyber-attacks than said they are “highly confident” around these two areas.

FIGURE 3

Confidence in cyber resilience measures slipped from 2017 to 2019.

Q: For each of the following, please indicate your level of confidence in your organization's ability to...



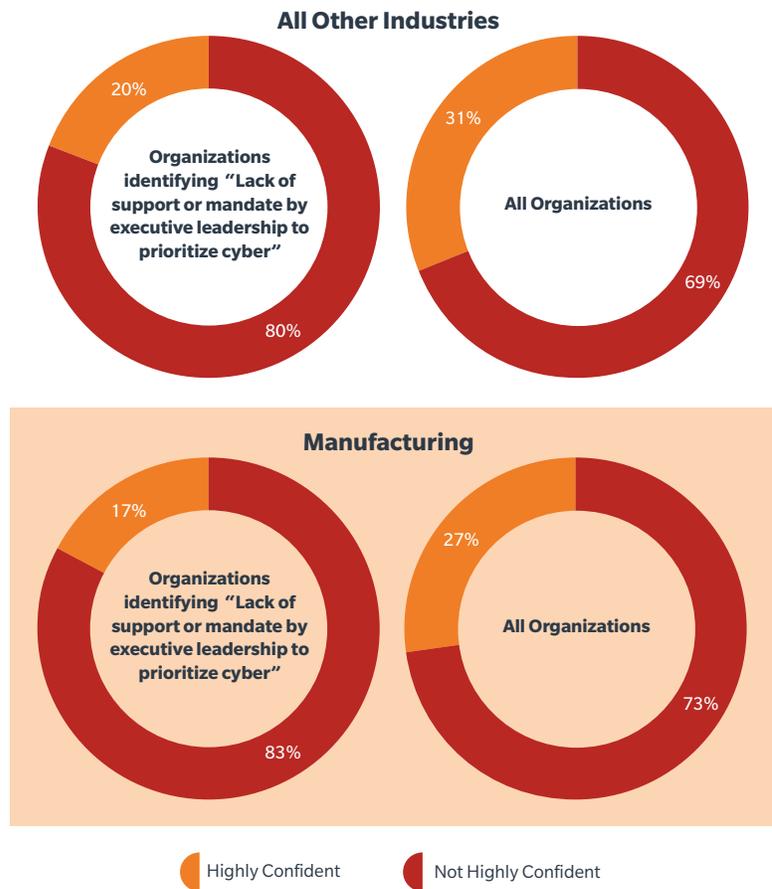


The decline in organizational confidence in cyber resilience capabilities may be partly driven by a lack of executive leadership on issues and initiatives related to cyber risk.

Organizations that cited “lack of support or mandate from executive leadership to prioritize cyber” as a major barrier to effective risk management were significantly less confident in their overall cyber resilience compared to those that did not cite lack of management support (see Figure 4).

FIGURE 4 Confidence in cyber resilience is low where senior leaders don’t prioritize cyber.

Q: Which of the following do you consider major challenges or barriers to effective cyber risk management for your organization?



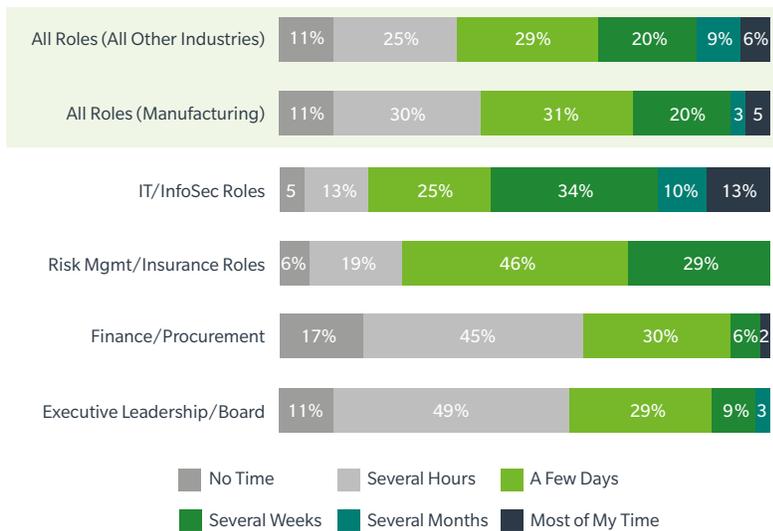
Lack of senior leadership involvement in championing cyber risk management for the organization is a problem in all industries. This is illustrated by the average amount of time spent on cyber risk and cybersecurity by people in different roles and functions (see Figure 5).

At manufacturing firms, a clear majority (60%) of executive leaders and board members reported spending just hours each year focused on cyber risk and/or cybersecurity. No manufacturer's risk management/insurance professionals reported spending more than a few weeks focused on these issues, despite the prominence of cyber risk as a top strategic threat for manufacturing organizations.

Worldwide, there seems to be a clear need for more time and focus on cyber risk by risk managers and senior leaders risk at manufacturers — a finding that applies to organizations across all industries.

FIGURE 5 Most executive leaders at manufacturers spend just a few hours per year focused on cyber risk and/or cybersecurity.

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



Another notable challenge for manufacturers in managing cyber risk is the low appreciation for external standards and guidelines.

Manufacturing firms responding to the survey are significantly more likely than firms in other industries to view both governmental laws and regulations and “soft” industry standards as having little effect on improving their cybersecurity and reducing overall cyber risk (see Figure 6).

Only 27% of manufacturers agree that government regulations are “very effective” in helping them improve their cybersecurity postures, and only 20% say the same about industry standards, such as NIST and ISO.

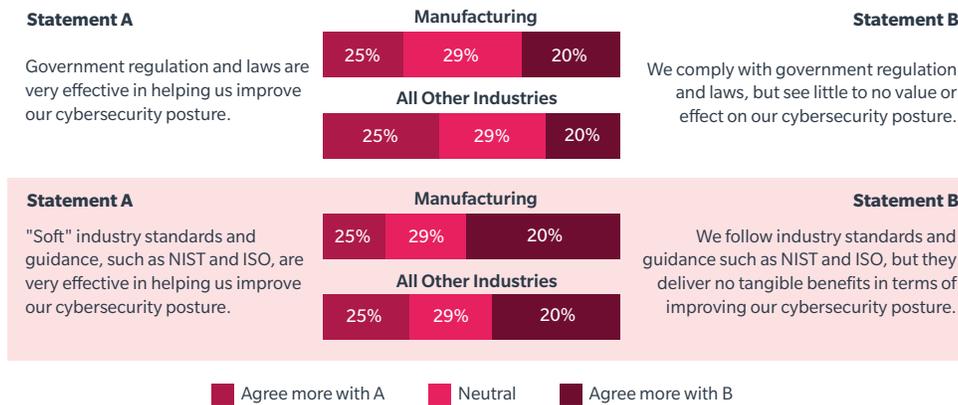
In fact, 34% of manufacturing organizations see statutory regulations as being of “little to no value” and a majority (52%) say the same about industry standards — both significantly higher responses than in other industries.

This variance may point to an opportunity for the manufacturing sector to ramp up its engagement and dialogue with public sector entities to identify ways to strengthen the perceived effectiveness of cyber regulation and industry standards.

FIGURE 6

Manufacturing organizations are likely to view government regulations and industry standards as having little impact on cybersecurity posture.

Q: For each of the following pairs of statements, please indicate which choice most closely reflects your organization’s views



Manufacturers Don't See Suppliers as Posing Major Cyber Risk

Manufacturers in our 2019 survey expressed much higher levels of concern about supply chain disruption compared to companies in all other industries.

Two-thirds (66%) of manufacturers ranked supply chain disruption as their third-greatest concern, after cyber risks and economic uncertainty. This is significantly higher than the 36% of firms in other sectors that cited supply chain disruption in their top five concerns, ranking it seventh.

One might assume that manufacturers perceive greater levels of cyber risk from their supply chain partners than do organizations in other industries, because manufacturing core operations tend to rely more heavily on supply chain integrity and security.

But our survey results indicate otherwise. For example, when asked to rate the level of cyber risk posed to their organization by their supply chain partners, manufacturers report significantly lower levels of concern than organizations in other industries.

Only 30% of manufacturers rate their level of concern about supply chain risk from their partners as “somewhat” or “very high,” compared to 40% in other industries (see Figure 7).

This disconnect between high concern over supply chain risk generally, and lower concern over risk from supply chain partners, is a bit of a conundrum.

On the other hand, manufacturers reacted in about the same low proportion as did other industries regarding the level of cyber risk their organization poses to their supply chain partners. Only 17% of manufacturers — and 16% in other industries — said that their concern about risk they themselves pose was “somewhat” or “very high.”



For all organizations, including manufacturers, the gap between perceptions of risk posed by the supply chain versus the risk posed to the supply chain increases when we look at the results based on company size (see Figure 8).

Firms with the largest revenues are more likely than smaller ones to perceive a higher level of cyber risk posed to their organizations by their supply chains, rather than vice versa.

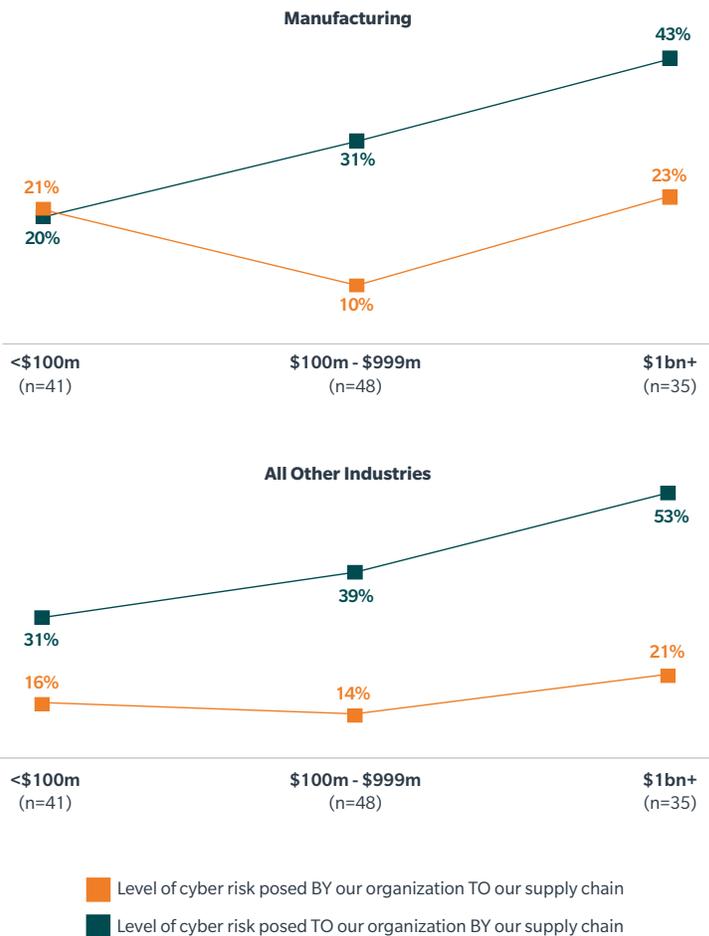
However, among manufacturers of every organizational size/revenue, fewer cited high cyber risks from their supply chains than did similar-sized organizations in other industries.

This is surprising given the significantly higher levels of concern expressed by manufacturers about “supply chain disruption” compared to those in other industries.

FIGURE 8

Large manufacturing firms are more likely than smaller manufacturers to perceive a high level of cyber risks posed to their organizations by their supply chain partners

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



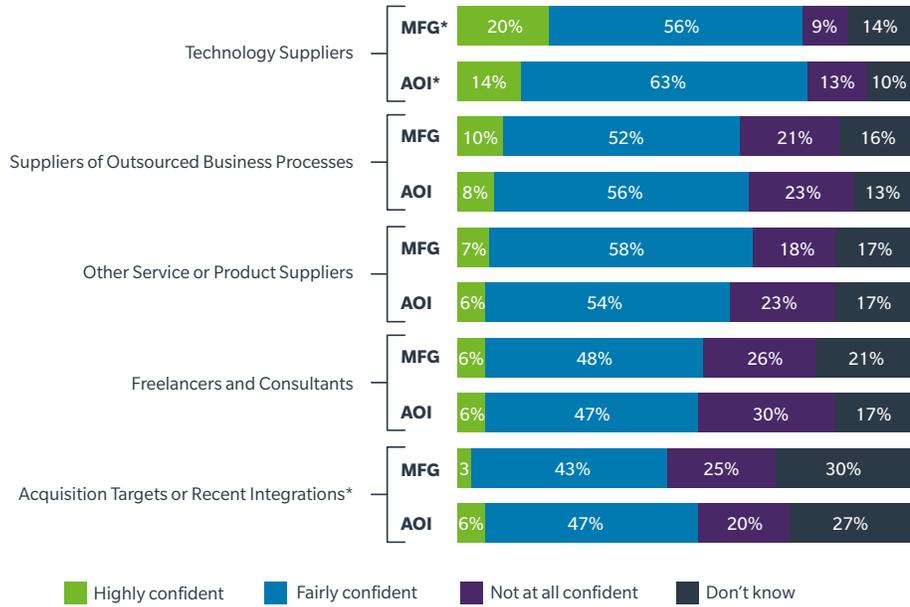
Firms engaged in manufacturing and other industries exhibit similar levels of confidence regarding their ability to mitigate cyber risks posed by suppliers (see Figure 9). In the case of cyber

risks presented by technology suppliers, manufacturers have significantly higher confidence that they can prevent or mitigate such risks compared to firms in all other industries.

FIGURE 9

Few manufacturing organizations are highly confident in their ability to mitigate cyber risks posed by various third parties.

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



* MFG = Manufacturing AOI = All Other Industries



Manufacturers Less Likely to Employ Economic Cyber Risk Assessment

What’s behind the disconnect between manufacturers’ high level of concern about supply chain disruption, and relatively lower level of concern about supply chain risk?

One possible explanation lies in the approach to assessing and expressing cyber risk exposures: Manufacturers appear to be significantly less likely to employ a rigorous economic approach to measuring or expressing their cyber risk exposures compared to other industries (see Figure 10).

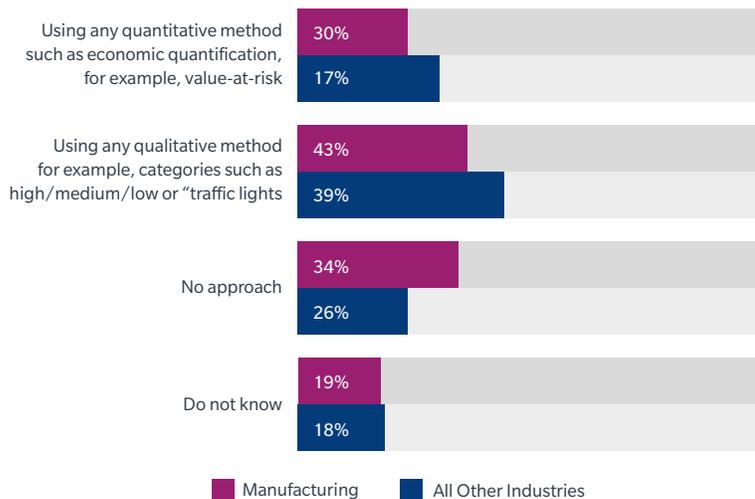
The relatively lower use of economic — or any — cyber risk assessment methods by manufacturers may make them less aware or knowledgeable about potential losses and liabilities in the event of a cyber incident.

This may help explain why manufacturers report lower levels of concern and/or higher levels of confidence regarding supply chain-related cyber risks compared to companies in other industries.

FIGURE 10

Over a third of manufacturing firms have no formal approach to quantifying cyber risk.

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



Mitigating Cyber Risks Requires Action and Investment in Multiple Areas

Many organizations are engaging in more — and a broader expanse of — measures to assess, mitigate, and manage their cyber risk exposures. Most, however, continue to focus on technical and preventive activities, such as improving security of digital devices and strengthening cybersecurity policies and procedures.

Manufacturing firms appear to lag slightly behind organizations in other industries when it comes to most actions taken to improve cyber risk resilience.

In particular, manufacturers were significantly less likely than other industries to have conducted penetration testing (45% vs. 54%, respectively), implemented awareness training for employees (58% vs. 67%), identified external resources for incident support (36% vs. 46%), and conducted tabletop exercises or management training (20% vs. 30%) within the past 12 to 24 months.



FIGURE 11

Fewer manufacturers have implemented key cyber risk resilience actions, focusing instead on technical actions.

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

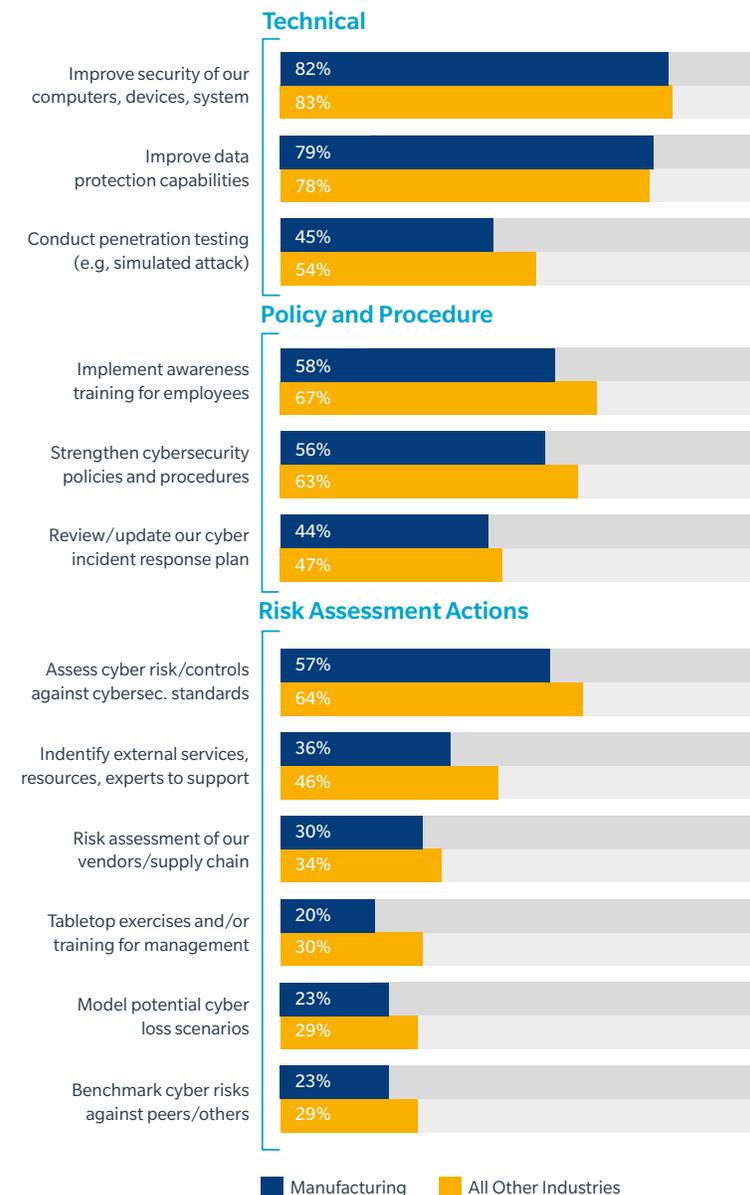


FIGURE
12

Manufacturers that quantify risks in economic terms are likely to implement a wider range of actions to understand and enhance cyber resilience.

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



Notably, the 2019 survey found a consistently higher level of sophistication regarding cyber risk resilience exhibited by organizations that measure or express current exposures in economic terms, vs. those that do not.

Organizations that express the risks in economic terms were clearly and consistently ahead of organizations that do not in terms of understanding, confidence, and actions taken around cyber risk.

This general finding is true for manufacturing firms. A relatively small number of manufacturers currently express their cyber risk exposures in economic terms, and those that do have, on average, engaged in a significantly wider range and number of resilience-building actions compared to manufacturers that do not quantify their cyber risk (see Figure 12).



Manufacturers Less Likely to Use Cyber Insurance

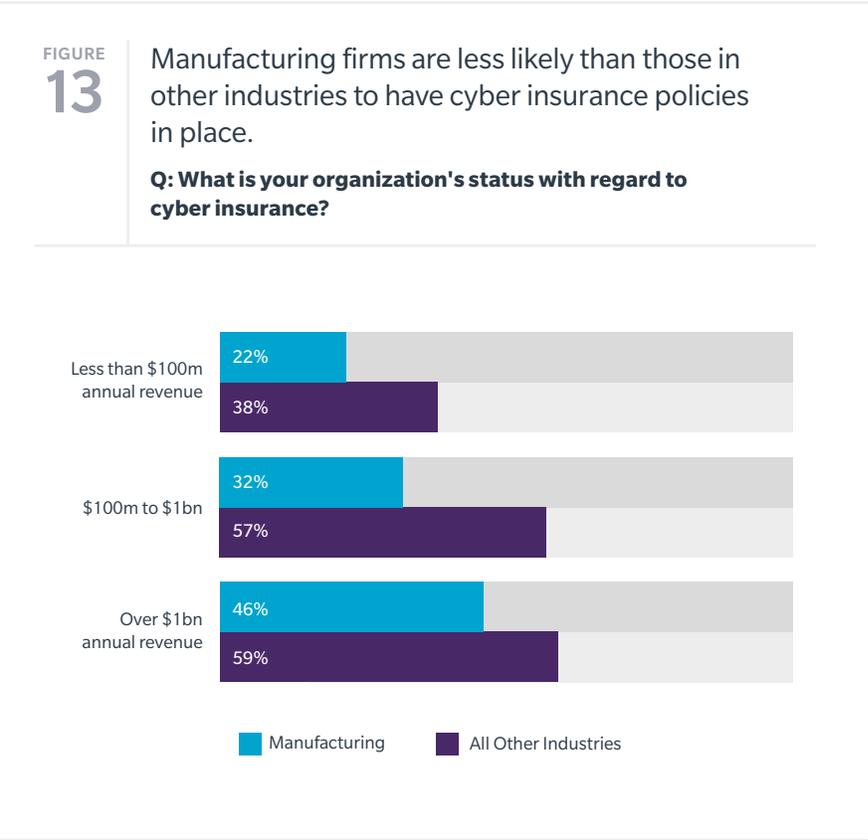
Best practice consensus holds that effective cyber risk management requires a holistic breadth of actions and tools, rather than a single emphasis on technology or other “silver bullets”.

Organizations should develop multi-pronged approaches that enhance and reinforce key capabilities, resources, and systems in order to reduce their overall level of cyber risk while simultaneously increasing the ability to assess, prevent, and recover from a potential incident or attack.

Cyber insurance and/or alternative risk transfer mechanisms can be key component(s) of a comprehensive cyber risk management strategy.

Risk transfer can help firms fill gaps in resilience capabilities and/or effectively cover potentially large costs and penalties arising from a cyber incident. In this area, too, our survey shows that manufacturers have significant ground to make up compared to other industries.

Less than one-third of manufacturing firms said they have cyber insurance policies in place, compared to half of those in other industries (see Figure 13). This disparity is even greater for firms with less than \$1 billion in annual revenue.

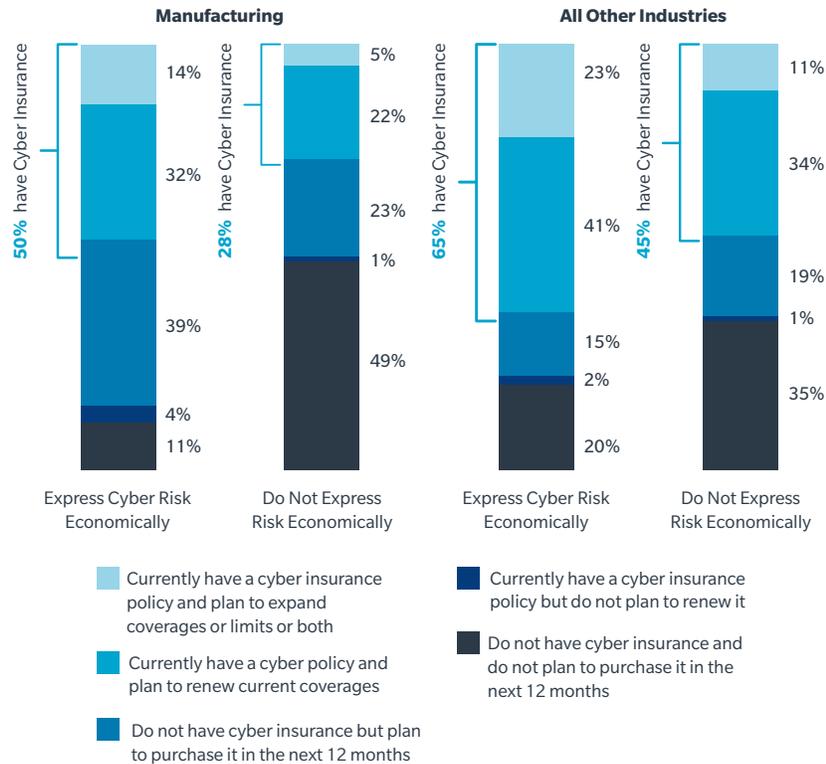


As with other cyber risk mitigation actions, adoption of cyber insurance is higher among organizations that have quantified their cyber risks economically (see Figure 14). Most manufacturers that quantify cyber risk (85%) currently have, will expand, or plan to purchase cyber insurance, compared to only 50% that do not quantify their cyber risk.

FIGURE
14

Manufacturing firms are less likely than those in all other industries to purchase cyber insurance.

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



Plans for the Future

The 2019 survey asked organizations about their recent cyber risk resilience actions and about areas in which they expect to ramp up risk-related activities and investments over the next three years.

Across all industries, the majority of organizations said they expect to increase spending on cybersecurity technology/mitigation, as well as on staff training related to cyber risks (see Figure 15). This is no surprise given that these areas have been in focus for cyber risk initiatives and investments for most organizations over the past two years.

In contrast, just over one third expect to invest in planning and preparation for cyber event response, and slightly less expect to invest in insurance/risk transfer and staffing (see Figure 15).

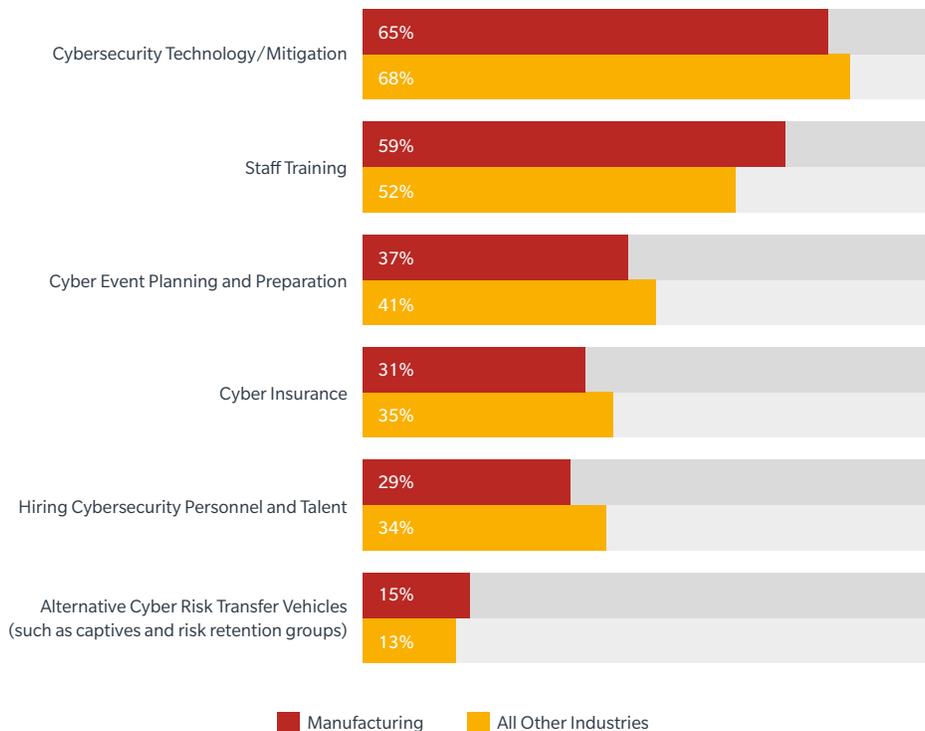
Investments in cyber resilience measures, generally, continue to take a back seat to preventive and technological tactics.

Organizations worldwide — including manufacturers — may want to re-examine their near-term action and investment plans and ensure they are implementing a comprehensive and balanced strategy to build resilience for the inevitable cyber incidents.

FIGURE
15

Cybersecurity technology and staff training top the list of future investment allocations for risk management.

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



Conclusion

As cyber risks become increasingly complex and challenging, there are encouraging signs in our 2019 *Global Cyber Risk Perception Survey* that enterprises are, slowly but surely, starting to implement best practices in cyber risk management. Nearly all recognize the magnitude of cyber risk, many are shifting aspects of their approach to match the threat, and most are doing a good job in traditional cybersecurity — protecting the perimeter.

The most savvy organizations are building cyber resilience through comprehensive, balanced cyber risk management strategies, rather than concentrating solely on prevention. These more complex approaches account for the need to build capabilities in understanding, assessing, and quantifying cyber risks in the first place, as well as adding the tools and the resources to respond to and recover from cyber incidents when they inevitably occur.

Nonetheless, this year's survey shows that there remains a considerable gap between where cyber sits on the corporate risk agenda and the overall level of rigor and maturity of organizational cyber risk management. Many enterprises globally could benefit by applying strategic risk management principles to their cyber risk approach, supported by more expertise, resources, and management attention as they build cyber resilience.

Especially in an "Internet of Everything" era with digitally dependent supply chains and innovative technology, yesterday's practices and mindsets are not enough, and may actually inhibit innovation. Optimizing security from the "castle" the self-enclosed organization — to the wider community is harder, but inevitable. It requires a shift from solely focusing on enterprise security to embracing responsibility for network security across the entire supply chain.

At a practical level, this year's survey points to a number of best practices that the most cyber resilient firms employ and which all firms should consider adopting:

- Create a strong organizational cybersecurity culture, with clear, shared standards for governance, accountability, resources, and actions.
- Quantify cyber risk to drive better informed capital allocation decisions, enable performance measurement, and frame cyber risk in the same economic terms as other enterprise risks.
- Evaluate the cyber risk implications of new technology as a continual and forward-looking process throughout the lifecycle of the technology.
- Manage supply chain risk as a collective issue, recognizing the need for trust and shared security standards across the entire network, including the organization's cyber impact on its partners.
- Pursue and support public-private partnerships around critical cyber risk issues that can deliver stronger protections and baseline best practice standards for all.

Despite the decline in organizational confidence in the ability to manage cyber risk, we are optimistic that more organizations are now clearly recognizing the critical nature of the threat, and beginning to seek out and embrace best practices. Effective cyber risk management requires a comprehensive approach employing risk assessment, measurement, mitigation, transfer, and planning, and the optimal program will depend on each company's unique risk profile and tolerance. Still, these recommendations address many of the common and most urgent aspects of cyber risk that organizations today are challenged with, and should be viewed as signposts along the path to building true cyber resilience.

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	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 business of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue approaching US\$17 billion and 76,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: 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.

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 © 2019 Marsh LLC. All rights reserved. 280497