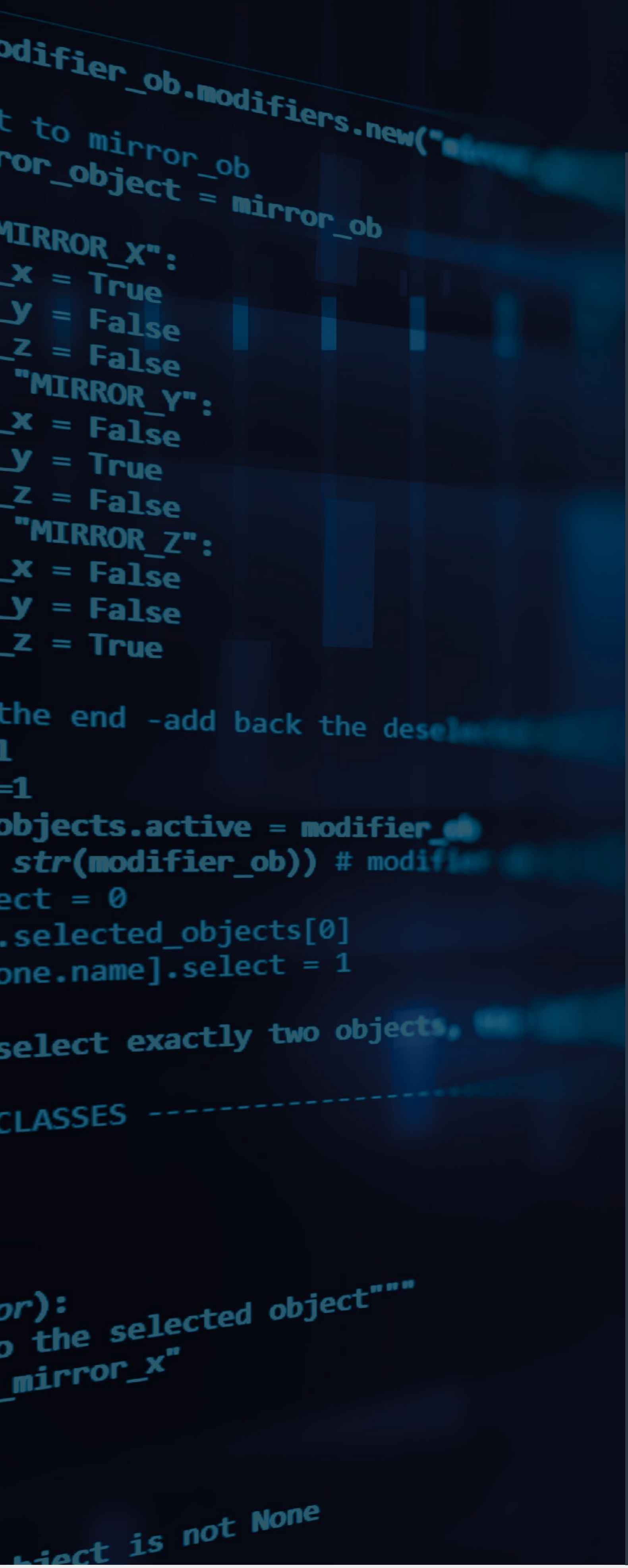
MARSH | Microsoft

INSIGHTS | SEPTEMBER 2019

2019 Global Cyber Risk Perception Survey

MARSH & McLENNAN COMPANIES



INSIGHTS | SEPTEMBER 2019

2019 Global Cyber Risk Perception Survey

CONTENTS

Introduction

Technology is dramatically transforming the global business environment, with continual advances in areas ranging from artificial intelligence and the Internet of Things (IoT) to data availability and blockchain. The speed at which digital technologies evolve and disrupt traditional business models keeps increasing. At the same time, cyber risks seem to evolve even faster.

Cyber risk has moved beyond data breaches and privacy concerns to sophisticated schemes that can disrupt entire businesses, industries, supply chains, and nations, costing the economy billions of dollars and affecting companies in every sector. The hard truth organizations must face is that cyber risk can be mitigated, managed, and recovered from, but it cannot be eliminated.

The *2019 Global Cyber Risk Perception Survey* from Marsh and Microsoft investigates the state of cyber risk perceptions and risk management at organizations worldwide, especially in the context of a rapidly evolving business technology environment. It builds on a related survey conducted in 2017, and released in 2018. Our findings focus on five important concepts that underscore the state of enterprise cyber risk in today's 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.
2. Globally, organizations exhibit dissonance between their perception of cyber as a top-priority risk and their approach to managing it. In general, organizations are focusing more on technology and prevention than on prioritizing the time, resources, and activities needed to build cyber resilience.
3. Despite embracing technology and digital innovation, organizations have considerable uncertainty about the degree of cyber risk such new technologies bring.
4. The digitization of supply chains brings benefits, but many companies don't fully appreciate the interdependency of roles and their own responsibilities within the supply chain, especially larger enterprises.
5. There is ambivalence about the value of both government regulation and industry standards around cybersecurity. Most companies see both as having limited effectiveness, yet there is strong appetite for government leadership and support to help combat nation-state cyber threats.

The *2019 Global Cyber Risk Perception Survey* reveals many encouraging signs of improvement in the way that organizations view and manage cyber risk. Cyber risk is now clearly and firmly at the top of corporate risk agendas, and we see a positive shift towards the adoption of more rigorous, comprehensive cyber risk management in many areas. However, many organizations still struggle with how best to articulate, approach, and act upon cyber risk within their overall enterprise risk framework — even as the tide of technological change brings new and unanticipated cyber risk concerns.

We hope this report helps your company navigate the rapidly evolving cyber risk landscape. We encourage all companies to build cyber resilience, approaching 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.

Survey Highlights

The Marsh Microsoft *2019 Global Cyber Risk Perception Survey* looks at how organizations manage the escalating threat of cyber risk, particularly within a highly dynamic business environment that is being transformed by technological innovation and interdependence. Key survey findings show improvement since 2017 in several areas around organizations' awareness and tactics to address cyber risk, yet there is a striking dissonance between the high concern about cyber risk and the overall approach to managing it.

Priority and Confidence

Cyber risk became even more firmly entrenched as an organizational priority in the past two years. Yet at the same time, organizations' confidence in their ability to manage the risk declined.

- 79% of respondents ranked cyber risk as a top five concern for their organization, up from 62% in 2017.
- Firms' confidence declined in each of three critical areas of cyber resilience. Those saying they had "no confidence" increased:
  - From 9% to 18% for understanding and assessing cyber risks.
  - From 12% to 19% for preventing cyber threats.
  - From 15% to 22% for responding to and recovering from cyber events.

New Technology

Technology innovation is vital to most businesses, but often adds to the complexity of an organization's technology footprint, including its cyber risk.

- 77% of 2019 respondents cited at least one innovative operational technology that they have adopted or are considering.
- 50% said cyber risk is almost never a barrier to the adoption of new technology, but 23% — including many smaller firms — said that for most new technologies, the risk outweighs potential business benefits.
- 74% evaluate technology risks prior to adoption, but just 5% said they evaluate risk throughout the technology lifecycle — and 11% do not perform any evaluation.

Supply Chain

The increasing interdependence and digitization of supply chains brings increased cyber risk to all parties, but many firms perceive the risks as one-sided.

- There was a discrepancy in many organizations' view of the cyber risk they face from supply chain partners, compared to the level of risk their organization poses to counterparties.
  - 39% said the cyber risk posed by their supply chain partners and vendors to their organization was high or somewhat high.
  - But only 16% said the cyber risk they themselves pose to their supply chain was high or somewhat high.
- Respondents were more likely to set a higher bar for their own organization's cyber risk management actions than they do for their suppliers.

Government Role

Organizations generally see government regulation and industry standards as having limited effectiveness in helping manage cyber risk — with the notable exception of nation-state attacks.

- 28% of businesses regard government regulations or laws as being very effective in improving cybersecurity.
- 37% of businesses regard soft industry standards as being very effective in improving cybersecurity.
- A key area of difference relates to cyber-attacks by nation-state actors:
  - 54% of respondents said they are highly concerned about nation-state cyber-attacks.
  - 55% said government needs to do more to protect organizations against nation-state cyber-attacks.

Cybersecurity Culture and Resilience

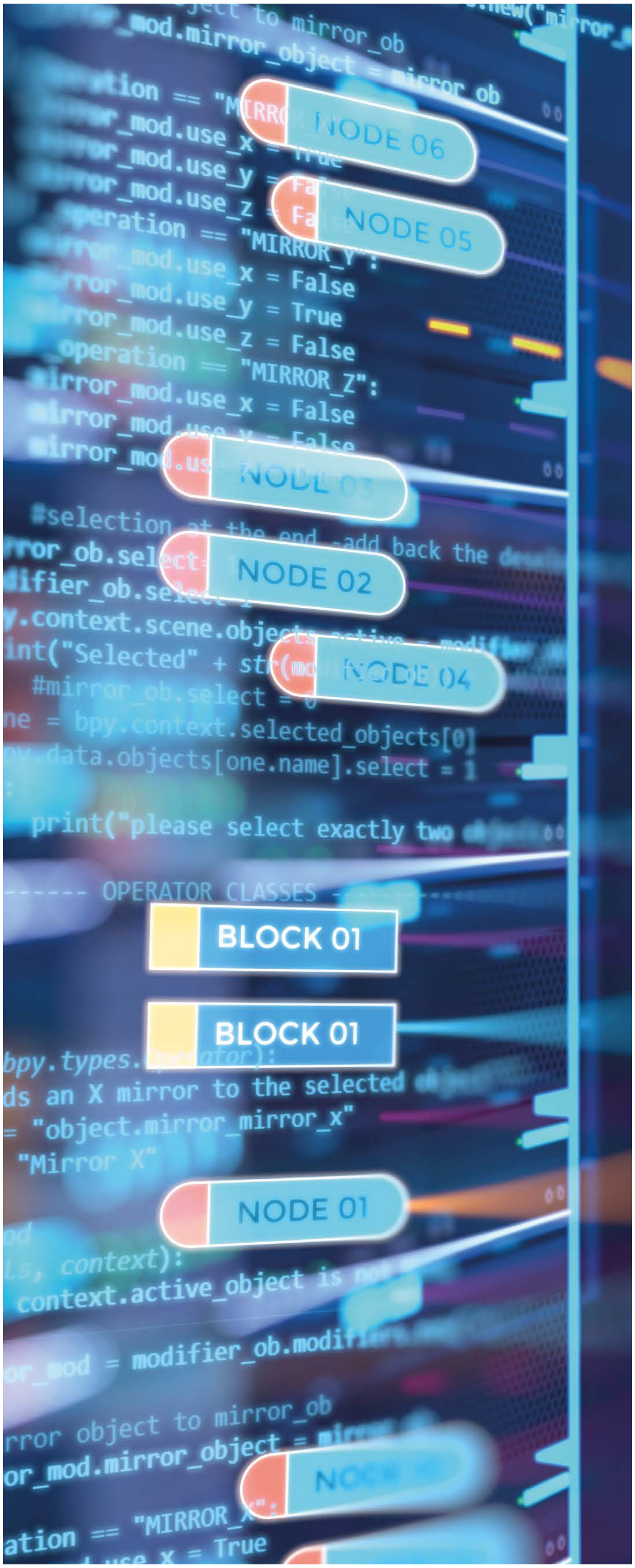
Many organizations focus on technology defenses and investments to prevent cyber risk, to the neglect of assessment, risk transfer, response planning, and other risk management areas that build cyber resilience.

- 88% said information technology/information security (IT/InfoSec) is one of the three main owners of cyber risk management, followed by executive leadership/board (65%) and risk management (49%).
- Only 17% of executives say they spent more than a few days on cyber risk over the past year.
- 64% said a cyber-attack on their organization would be the biggest driver of increased cyber risk spending.
- 30% of organizations reported using quantitative methods to express cyber risk exposures, up from 17% in 2017.
- 83% have strengthened computer and system security over the past two years, but less than 30% have conducted management training or modelled cyber loss scenarios.

Cyber Insurance

Cyber insurance coverage is expanding to meet evolving threats, and attitudes toward policies are also shifting.

- 47% of organizations said they have cyber insurance, up from 34% in 2017.
- Larger firms were more likely to have cyber insurance: 57% of those with annual revenues above $1 billion had a policy compared to 36% of those with revenue under $100 million.
- Uncertainty about whether available cyber insurance could meet their firm's needs dropped to 31%, down from 44% in 2017.
- 89% of those with cyber insurance were highly confident or fairly confident their policies would cover the cost of a cyber event.



Cyber Risk Dissonance: Priority Increases, Confidence Declines

While more companies see cyber risk as a top priority, confidence in cyber resilience is declining.

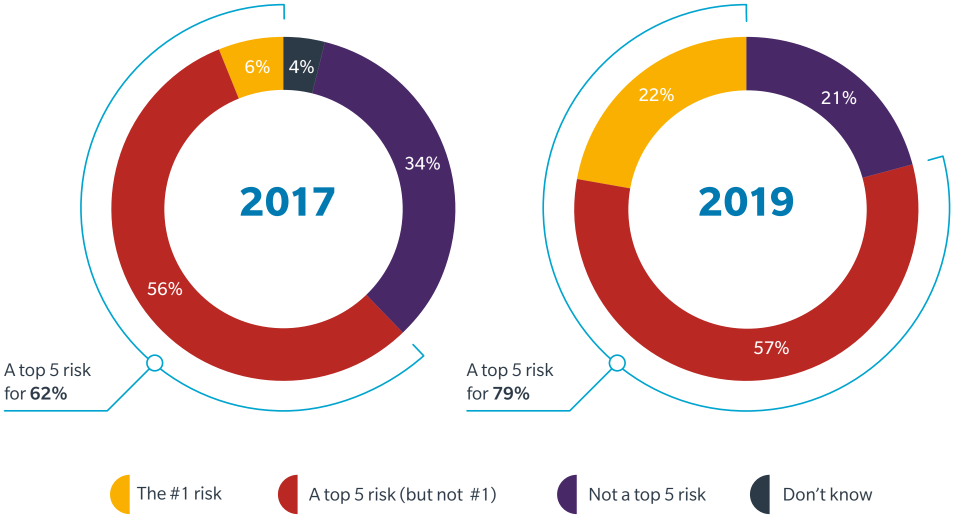
Cyber Risk Awareness Increases

Driven by the frequency and severity of high-profile incidents, such as the 2017 NotPetya attack, cyber risks and threats increased significantly among respondent organizations' top priorities in 2019 (see Figure 1). Globally, 79% of respondents ranked cyber risks as a top five concern for their organization, up from 62% in 2017. The number citing cyber risk as their #1 concern nearly quadrupled, from 6% to 22%.

FIGURE 1

Cyber risk has climbed sharply among organizations' risk priorities.

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



Base: All answering; n=1312 (2017); n=1512 (2019)

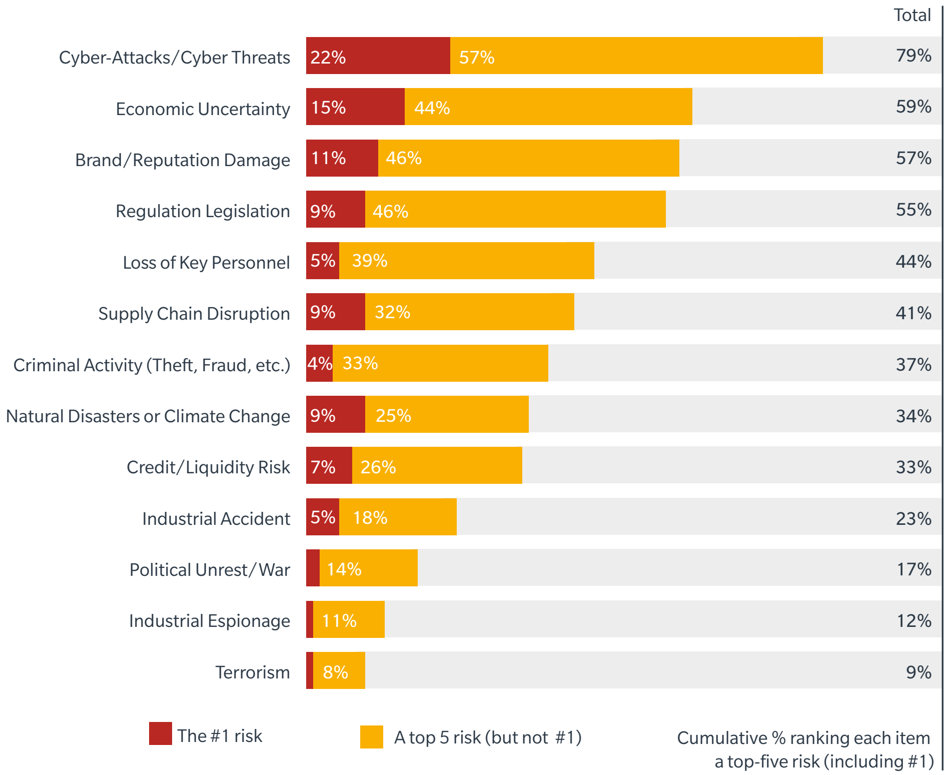
In 2019, more respondents ranked cyber risk as a top concern than any other major business risk (see Figure 2). Economic uncertainty was second, ranked as a top 5 risk by 59% of organizations — a full 20 percentage points below cyber-attacks and cyber threats.

These results suggest a sharp rise in the prominence of cyber risk, and correlate strongly with other recent studies. For example, the World Economic Forum (WEF) *2019 Global Risks Report* ranked data theft and cyber-attacks among the top five risks most likely to occur.

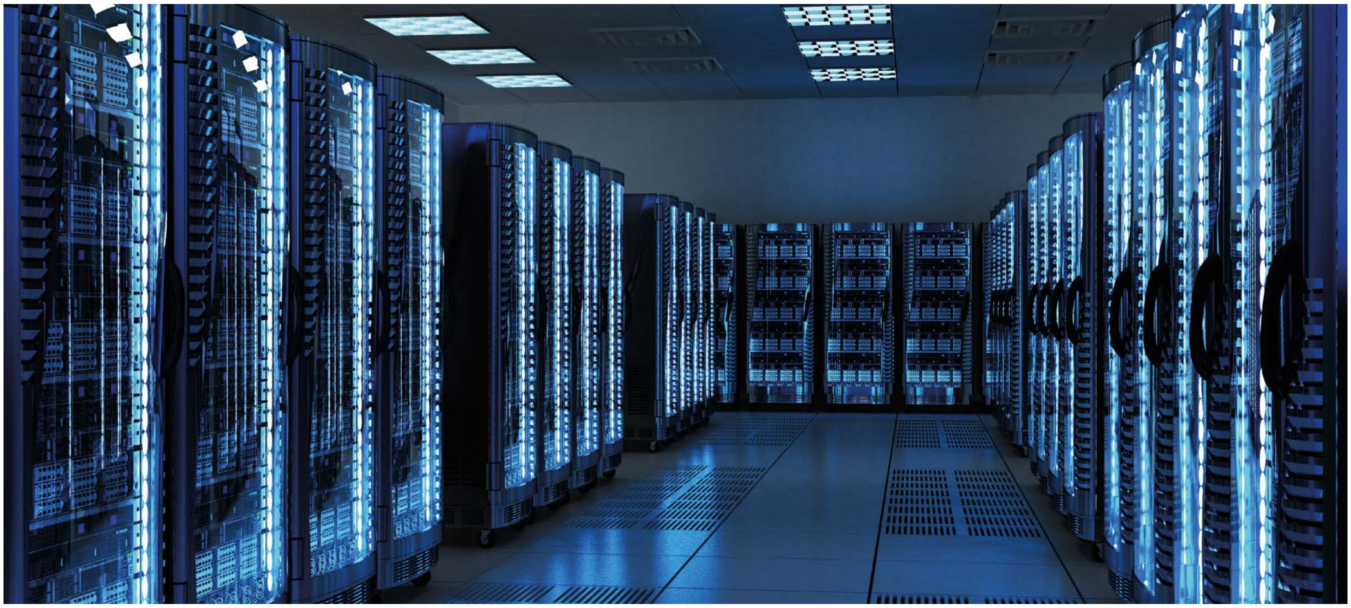
FIGURE 2

Cyber risks outrank all other risks by a wide margin.

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



Base: All answering; n=1512 (2019)



Cyber Confidence Declines

This year's survey found a notable decline in firms' confidence in each critical area of cyber resilience:

1. Understanding, assessing, and measuring potential cyber risks. Looking at the type, likelihood, and potential economic impact of exposures faced from the use of technology and data in an organization's operations.
2. Being able to reduce the probability of cyber-attacks from occurring, or preventing potential damage. This comprises a mix of technical and non-technical safeguards.
3. Managing, responding to, and recovering from cyber events. Clear and well-rehearsed contingency plans and readily available resources to minimize the negative consequences and time to recover from an incident.

Taken together, these areas provide an overall measure of an organization's cyber resilience — its ability to successfully navigate a cyber event; apply a range of planning, assessment, prevention, mitigation, and response capabilities to manage it; and return to normal operations with minimal downtime or losses. They align with the widely used National Institute of Standards and Technology (NIST) Cybersecurity Framework of detect, prevent, respond, and recover.

In 2019, the proportion of firms that reported feeling "high confidence" fell in all three areas compared to 2017 (see Figure 3). The decline was particularly sharp regarding businesses' understanding, assessment, and measurement of cyber threats.

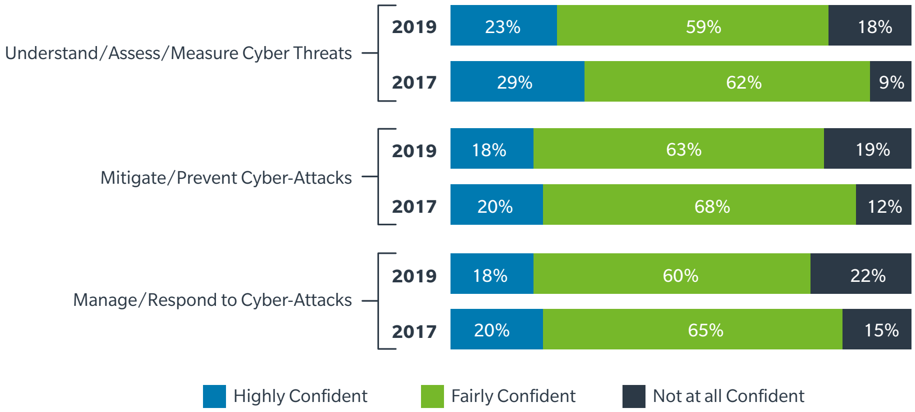
Equally concerning is that significantly more organizations reported being "not at all confident" across all three pillars. For example, more than 1-in-5 respondents in 2019 said they are not at all confident in their organization's ability to manage or respond to a cyber-attack.

In 2019, just 11% of firms reported a high degree of confidence in all three aspects of cyber resilience. That lack of confidence may stem in part from the relatively small effect organizations are seeing from ever-increasing investments in cybersecurity technology — products and services aimed at preventing or mitigating cyber-attacks. The cybersecurity market is forecast to surpass $124 billion in 2019, but despite soaring cybersecurity spending, the annual cost of cybercrime in 2019 is estimated at $1 trillion.

Organizations may be frustrated or confused when their increasing investment in cyber risk mitigation does not directly correlate to improved outcomes, as is usually the case with other areas of business investment and performance improvement.

FIGURE 3

Confidence in cyber resilience measures slipped from 2017 to 2019.



Base: All answering, excluding "don't know" responses; n=1312 (2017); n=1457 (2019)

Cyber Governance Still Largely Delegated to IT

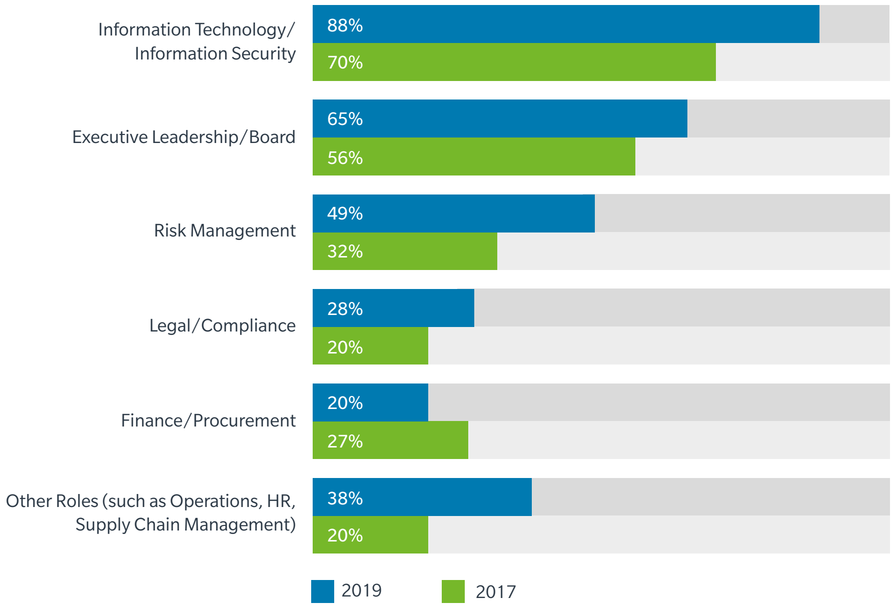
Despite cyber risk being ranked high among organizational priorities, governance and ownership of it generally does not align with that ranking. Often, stakeholders who should be focused on cybersecurity are not: Information technology and information security roles continue to be seen as the primary owners of cyber risk management.

In fact, the primacy of IT increased over the past two years, with almost 9-in-10 firms identifying IT/InfoSec as the main owner in 2019 (see Figure 4) — up from 70% in 2017. Also increasing from 2017, 65% of firms identified executive leadership/board members as among those spearheading cyber risk management efforts, although the involvement of other key functions lags.

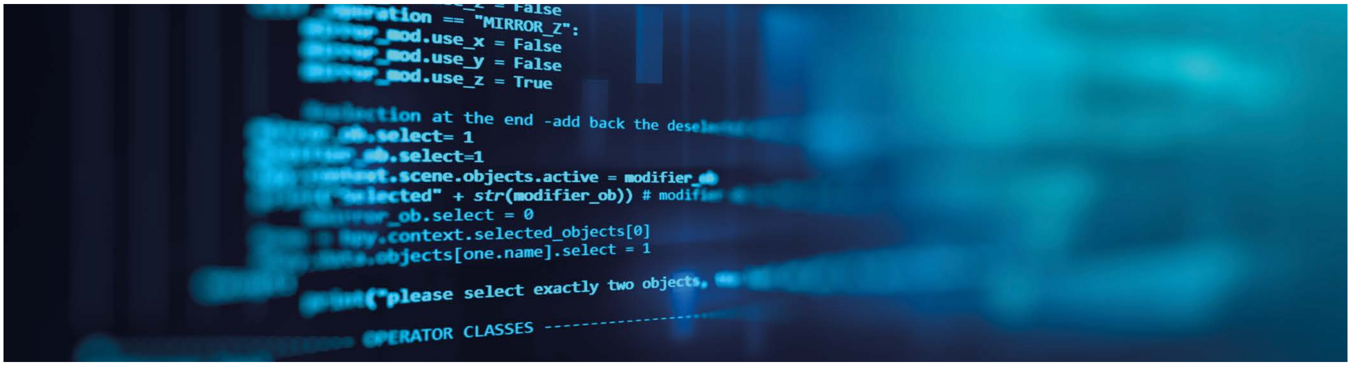
FIGURE 4

IT staff continue to be the main owners of cyber risk management at most firms.

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



% Identifying each function as one of the main owners/drivers of cyber risk management
Base: All answering in 2017 and 2019; n=1514 (2019); n=1312 (2017)


```
ration == "MIRROR_Z":
mod.use_x = False
mod.use_y = False
mod.use_z = True
ection at the end -add back the desel
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
lected" + str(modifier_ob)) # modif
r_ob.select = 0
y.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES ----------------
```

17%

Only 17% of executive leaders/board members spent more than a few days over the past year focusing on cyber risk issues.

There is considerable room to increase the involvement of risk management teams to drive cyber risk agendas — only 49% of organizations reported this was the case in 2019. Still, that is a sizeable increase over the 2017 response of 32%, signaling a trend toward increased ownership by risk management.

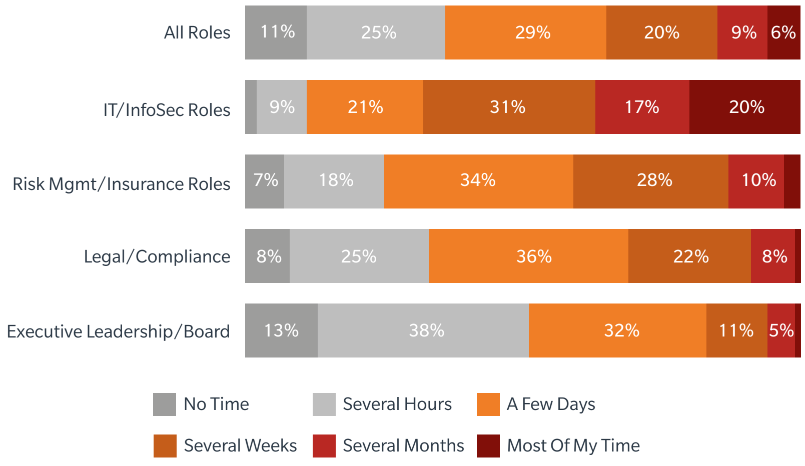
The collective ranking of IT, boards, and risk managers as the primary owners of cyber risk management is a positive sign that the right stakeholders are leading the way. But the fact that IT is named as a primary owner nearly twice as often as risk management points to a continuing, mistaken view of cyber risk as primarily a technology issue, rather than a critical business risk that merits a strategic enterprise risk management approach.

The question of who leads cyber risk management is just one area in which there is dissonance between an organization's perceptions and actions. Despite the high level of strategic concern organizations say they have for cyber risks, not all internal "risk governors" give the issue the attention it deserves (see Figure 5). Only 17% of executive leaders/board members spent more than a few days over the past year focusing on cyber risk issues. Even among IT respondents, 30% said they spent only a few days or less. This low allocation of time is concerning given that these two constituencies are ranked among the top three organizational owners of cyber risk management.

FIGURE 5

Key decision makers are not spending much time on cyber risk management.

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



% Reporting time spent on cyber risk/cyber security issues by each role
Base: All answering; n=1422 (All roles, 2019)

```
.field_information {cursor: pointer; float: left; margin: 1px 0 0 5px;}
.field_information_container {float: left; }
.label {font-size: 82% !important;}
.btn_copy_text {width: 110px;}
#btn_get_first {width: 110px;}

.title {width: 701px !important;}
.description {width:701px !important; height: 73px !important;}

.tag-editor {line-height: 25px !important; height: 225px; padding: 5px 0px !important; border: 1px solid #ccc !important; border-radius: 4px; overflow: auto !important;}
.tag-editor-delete {height: 25px !important;}
.tag-editor-delete i {line-height: 25px !important;}
.tag-editor-spacer {width: 10px !important;}

#btn_settings {-webkit-user-select: none; -khtml-user-select: none; -moz-user-select: none; -o-user-select: none; user-select: none; transition: all 0.5s ease-out 0s;}
#btn_settings:hover {cursor: pointer;transform: rotate(180deg);transition: all 0.5s ease-out 0s;}

#select_theme_container {width: 280px;}
#google_api_key {width: 400px;}
#get_first_n_value {width: 50px;}
.simple_text {text-decoration: none !important;}
.panel-settings {padding: 10px !important;}
.panel-settings-container {margin-bottom: 5px !important;}

#google_translate_api_info {font-size: 10px; margin-left: 35px;}
.checkbox_comment {font-size: 10px;}
.btn-default .badge {margin-left: 3px; border-radius: 5px !important;}
mark {padding: 0 !important;}

#add_and_translate {font-size: 10px;}

.tooltipster-box {background: #fff !important;}
.tooltipster-arrow-background {border-top-color: #fff !important;}
.tooltipster-box {-webkit-box-shadow: 0 1px 4px rgba(0,0,0,.2); box-shadow: 0 1px 4px rgba(0,0,0,.2)}
.tooltipster-arrow{height:10px !important;}
.tooltipster-content {margin: -2px 0px !important; }

#user_language {width: 50px;}
```

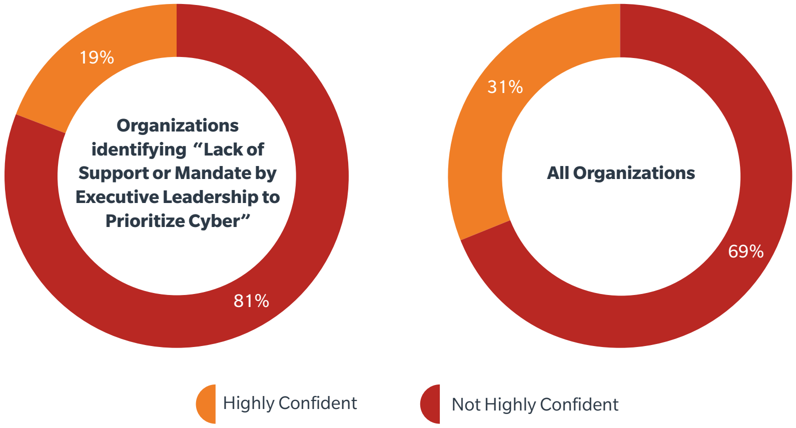
The importance of senior leadership driving the cyber risk agenda is underscored by the confidence gap in overall cyber resilience as reported by those who lack such leadership (see Figure 6). Only 19% of organizations without a senior-level mandate to prioritize cyber risk were highly confident in any of the three areas of cyber resilience, compared to 31% of all respondents.

Despite wide acknowledgement of cyber risk as a top priority, too few organizations currently take actions to create a strong cybersecurity "culture" with appropriate standards for governance, prioritization, management focus, and ownership. This places them at a disadvantage both in building cyber resilience and in confronting the increasing cyber challenges of a changing technology and supply chain environment.

FIGURE 6

Confidence in cyber resilience is very low where senior leaders don't prioritize cyber risk management.

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



"High Confidence Score" - % selecting "Highly Confident" in any of the three areas of cyber resilience
Base: All answering; n=1517 (2019)

New Technology Brings Increased Cyber Exposure

Businesses are embracing technological innovation, and most don't see cyber risk as a barrier. But assessment of new technology cyber risk is not as rigorous and continual as it should be.

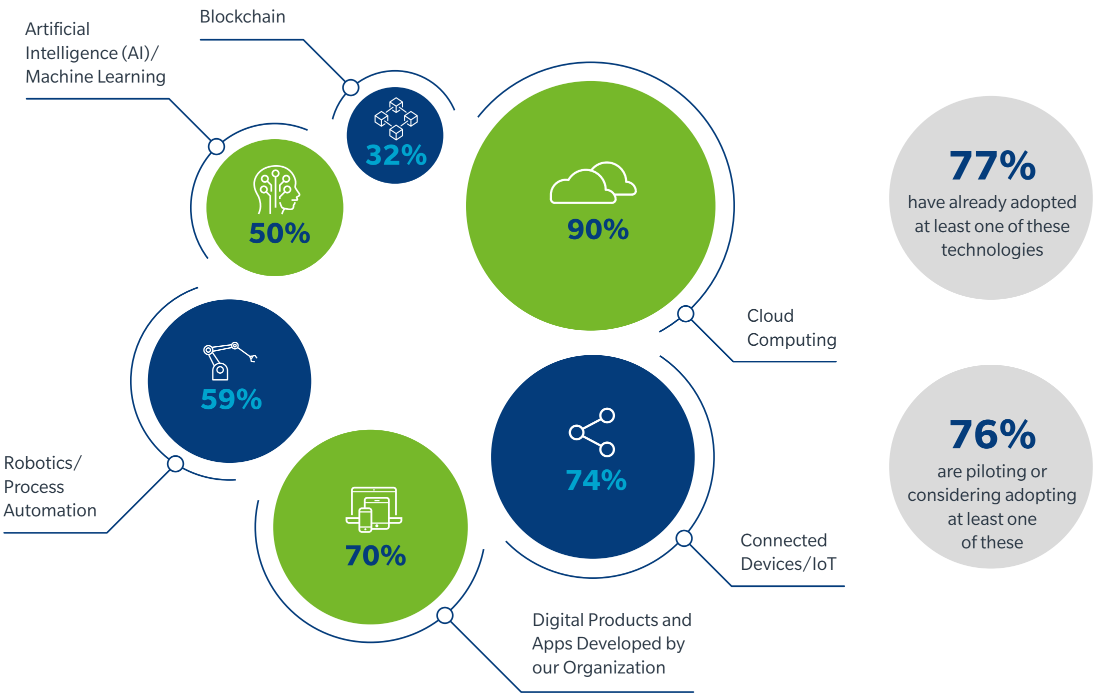
The number of internet connected devices is estimated to be 75 billion by 2025. As the world moves closer to an "Internet of Everything", the amount and variety of digital assets that are stored, processed, and shared by enterprises rises. Even traditional sectors such as manufacturing expect almost 50% of the products they develop to be "smart" or "connected" in some way by 2020, opening up new revenue streams in data-driven services.

More than three-quarters of 2019 survey respondents cited at least one innovative operational technology — including cloud computing, proprietary digital products, and connected devices/IoT — that they have adopted or are actively considering (see Figure 7).

FIGURE 7

Most organizations are considering or using a range of new technologies.

Q: For each of the following technologies, please indicate which consideration or usage scenario best applies to your organisation



% of organizations that have adopted or are piloting/considering each technology
Base: All answering, excluding don't know responses: n=588-773 (2019)

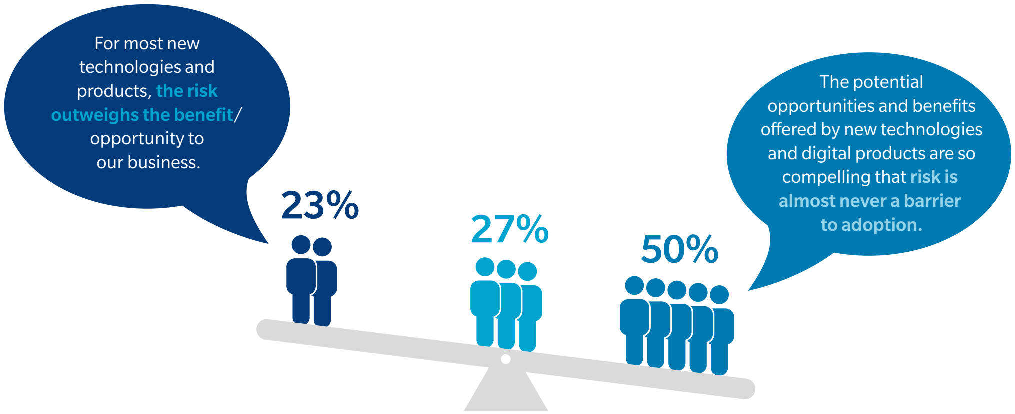
Security challenges can manifest whenever new technology is integrated into business infrastructure, bringing new and additional complexity to the organization's technology footprint. The risks and exposures presented by new technologies must be weighed against the potential transformative business effects, and risk tolerance varies both by industry and by individual company. Asked where their own organization falls on the new technology risk/benefit spectrum, half of respondents stated that cyber risk is almost never a barrier to new technology adoption, and a quarter of respondents had no strong views on the issue (see Figure 8).

The prevailing preference was to push ahead with digital transformation despite potential security issues. Still, 23% of respondents said that most new technologies present risks that outweigh the potential benefits and opportunities. This risk aversion was especially common among smaller firms (annual revenues under $100 million), regardless of sector.

FIGURE 8

The potential benefits of new technologies are generally seen to outweigh the potential risks.

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



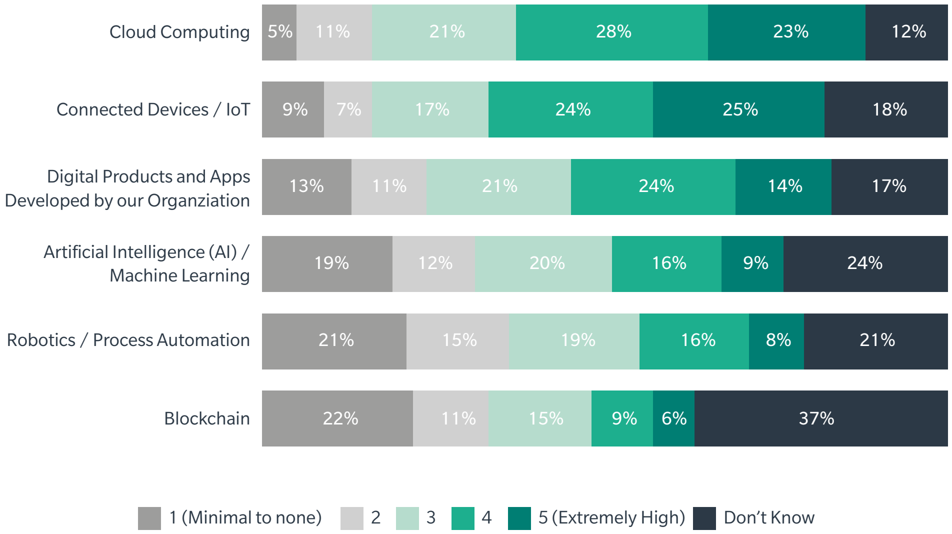
% of organizations agreeing with each of the statements (presented to respondents as a trade off)
Base: All answering; n=852 (2019)

Despite the enthusiasm for new and emerging technologies, there was uncertainty about the degree of risk associated with them (see Figure 9). Cloud computing elicited the fewest “don’t know” responses regarding the degree of associated cyber risk (12%), while blockchain had the highest (37%). In the case of new digital products or apps being developed, opinions were evenly divided between those that perceived a high level of risk and those that saw a lower level of risk. The highest amount of uncertainty was expressed for the newest or most autonomous technology developments.

FIGURE 9

Many business decision-makers are uncertain about the degree of risk posed by new business technologies.

Q: Please rate the level of perceived cyber risk associated with each technology, on a 5 point scale.



Base: All answering for each technology: varies from n= 892 to n=900 (2019)

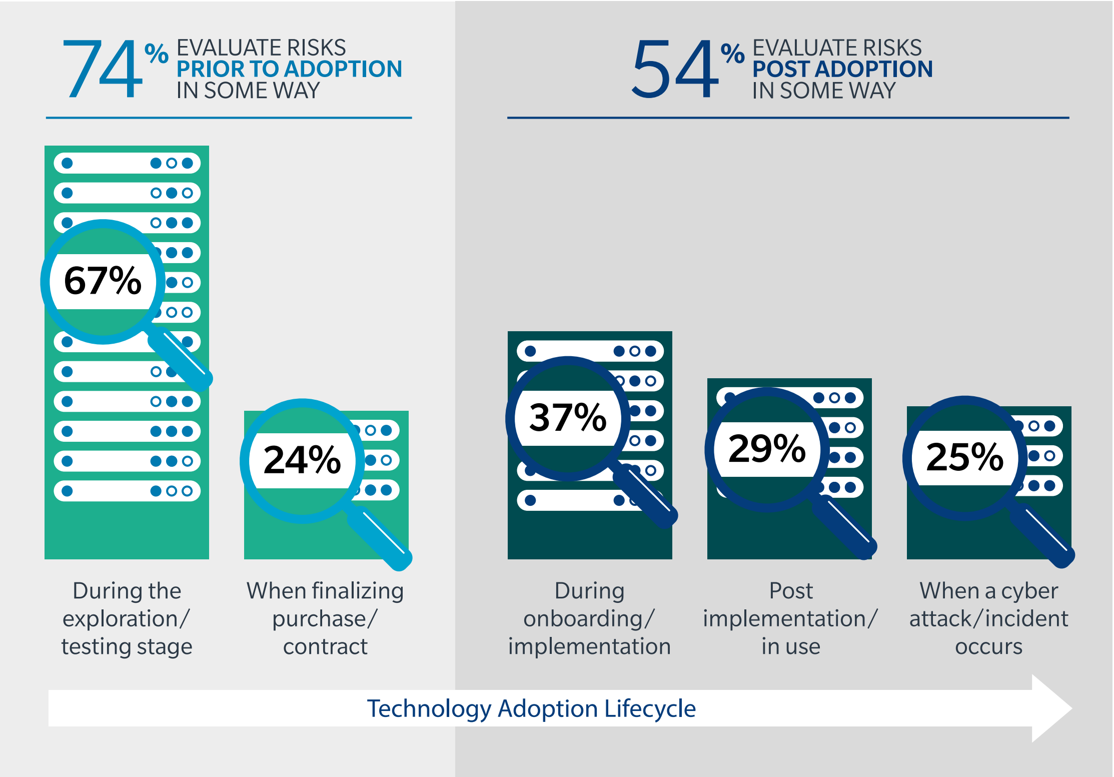
Among respondents, assessment of cyber risk was too often seen as an event that occurs at a single point in time — often, the initial exploration and testing stage — rather than a continuous evaluation at multiple stages of implementation (see Figure 10).

Only 36% of organizations reported examining potential risks of new technology both before and after adoption, and just 5% said they evaluate cyber risk at every stage in the technology lifecycle.

FIGURE 10

Cyber risk most commonly evaluated during the exploration/testing stage of technology adoption.

Q: When adopting and implementing new technologies, such as those you have just identified, at which of the following stages is cyber risk typically evaluated in your organization?



Only **36%** evaluated risks both prior to and after adoption.

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

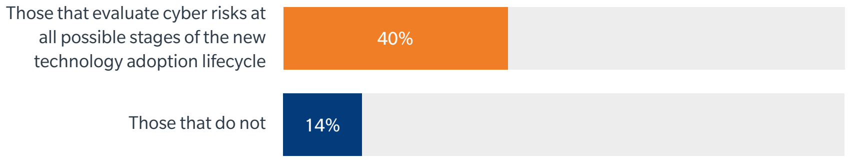
11% don’t evaluate at all.

Base: All answering, excluding don’t know: n=696 (2019)

Notably, the select group of organizations that evaluate cyber risks continuously throughout new technology implementation are also much more confident in their capabilities to manage or respond to cyber-attacks (see Figure 11).

FIGURE 11

Organizations that continuously evaluate new technology cyber risk are more confident in their overall cybersecurity.



% reporting high confidence in ability to manage or respond to a cyber attack
Base: All answering both Q9 & Q24: n=696 (2019)

Organizations that risk-test technology at multiple stages of implementation may feel better informed because continuous risk evaluation provides real-time visibility into the technologies' emerging vulnerabilities and risks. Armed with timely knowledge of potential security weaknesses or exposures, they are positioned to implement real-time improvements and develop contingency plans to manage risks involving these systems.

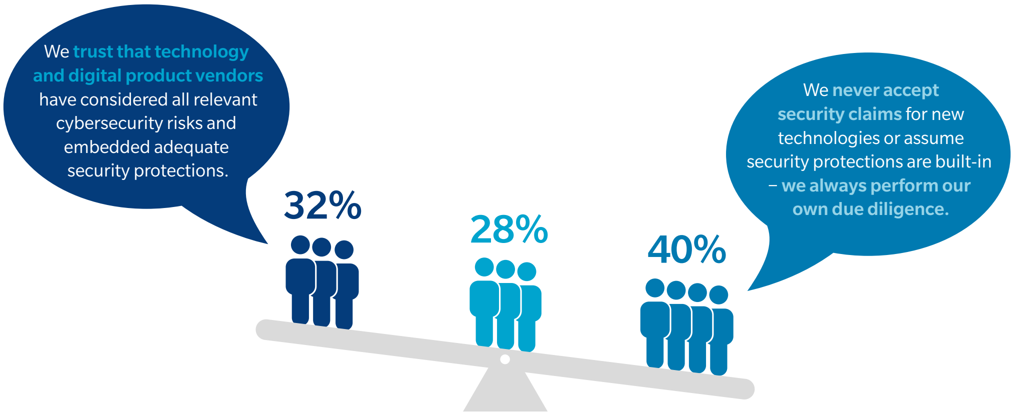
Assessment of new technology cyber risk is closely associated with the trust that organizations have — or lack — in the vendors that supply those technologies. Innovative technologies do not necessarily add new cyber exposures to the organizations that adopt them. Some technologies may add new risks if they have not been built in accordance with optimal security standards, but in many cases, security is factored by design into the development of the technology or device.

One-third of organizations acknowledged they assume that technology vendors have already considered all relevant cyber risks and that further verification is unnecessary. The converse view is not significantly greater: 40% of respondents said they "always perform their own due diligence" to verify security claims and built-in protections that vendors make regarding new technologies (see Figure 12).

FIGURE 12

One third of organizations assume technology vendors have considered all relevant cyber risks.

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



% of organizations agreeing with each of the statements (presented to respondents as a trade off)
Base: All answering: n=830 (2019)

Every company necessarily relies on a certain level of trust in its relationships with vendors and suppliers. However, given the potential importance of technology platforms and services to core assets and operations, a rigorous, trust-but-verify stance can help ensure the validity and adequacy of protections pledged by third-party providers. This heightened vigilance is especially important where new digital processes will be inherent to firms' business models.

2/5 of survey respondents said they thought their supply chain posed a high or somewhat high risk to their organization.

Supply Chain Risk: Moving to Technological Social Responsibility

In increasingly interdependent digital supply chains, cyber risk needs to be a collective responsibility.

In a world of hyper-connected supply chains, there is a critical need for trust among partners; a lack of trust risks impeding business performance and innovation. Every organization needs to understand, have confidence in, and play a role in the integrity and security of the components and software of its digital supply chains. The concept of "technological social responsibility" — the recognition and acknowledgement by each organization of its role and cybersecurity obligations within the supply chain — is on the agenda for many industry leaders.

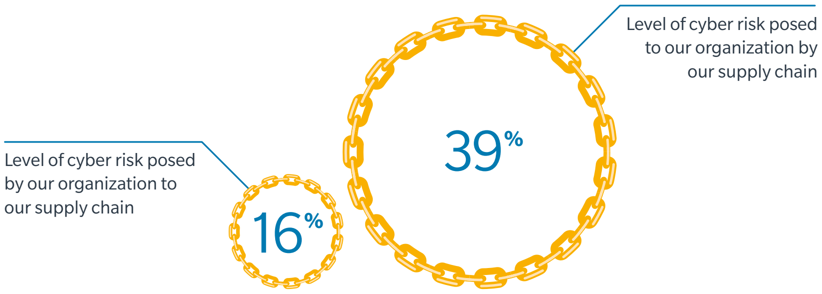
But while many organizations recognize the potential risks their supply chain partners may pose to their own cyber posture, most don't fully appreciate the risk in reverse. There was a marked discrepancy in many organizations' view of the cyber risk they face from supply chain partners, compared to the level of risk their organization poses to its counterparties.

Notably, 2-in-5 survey respondents said they thought their supply chain posed a risk to their organization (see Figure 13). At the same time, respondents were more than twice as likely to say they faced risk from third-party partners as they were to say that their organization posed a risk to those in their supply chains. This pattern appeared consistently across industry sectors and geographic regions.

FIGURE 13

Many organizations are more attuned to the risks they face from their supply chains than the risks they themselves pose.

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?

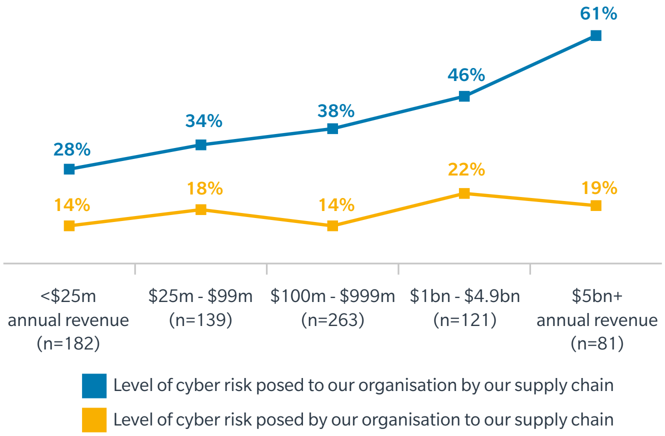


% regarding each risk as "somewhat" or "very high"
Base: All answering: n=786 (2019)

FIGURE 14

Larger organizations are more likely to perceive risks from their supply chains than to recognize risks they themselves pose.

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 it's supply chain / third parties?



% regarding each risk as "somewhat" or "very high"
Base: All answering (2019): Base varies as indicated.

Only

19%

of large enterprises say they pose a risk to their supply chain.

Moreover, the largest organizations exhibited the largest dissonance on this topic. Among the smallest firms, 28% stated that they faced high risks from their supply chain, while half of that said they posed risks to it (see Figure 14). This gap increased markedly with revenue size, with 61% of companies of $5 billion revenues or more saying they faced high risks from their supply chain and only 19% saying they posed a risk to it.

This is a perception gap that many organizations, especially large ones, need to address in order to effectively protect their supply chain ecosystem — embracing their own technological social responsibilities.

Overall

43%

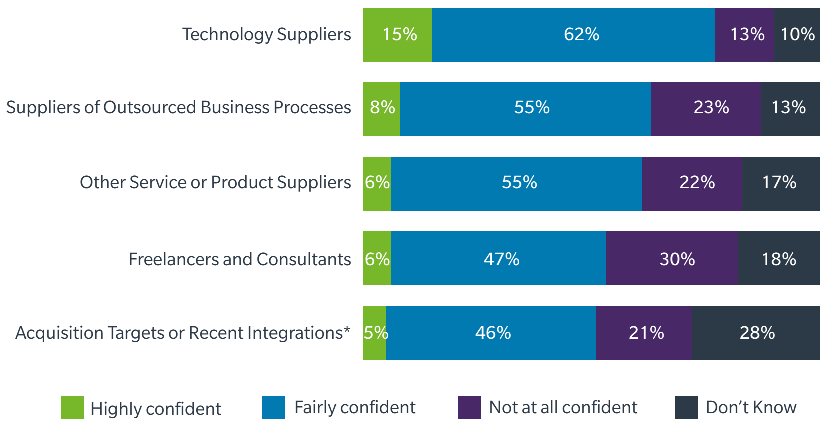
reported "no confidence" in their ability to prevent cyber threats from at least one of their third-party partners.

The disconnect may be driven by organizations' low confidence in their abilities to prevent or mitigate cyber risks posed by commercial partners. The share of organizations that said they are "highly confident" about mitigating cyber threats from their supply chain partners ranged from lows of 5% to 15%, depending on the type of third party (see Figure 15). The proportion stating they are "not at all confident" was generally twice as high, ranging from 13% to 30%. Overall, 43% reported "no confidence" in their ability to prevent cyber threats from at least one of their third-party partners.

FIGURE 15

Few organizations are highly confident in their ability to manage cyber risk from third parties.

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



% of organizations reporting different levels of confidence
Base: All answering; n=878 (2019); *Results for this option only shown for businesses with US$1bn+ revenues (n=215)

Midsize firms tended to report the strongest levels of confidence in managing suppliers of various types. For example, 71% of firms with between $100 million and $1 billion in annual revenue stated that they were "fairly" or "highly confident" in their ability to mitigate risks arising from outsourced business process providers, compared with 60% in all other size categories. This may suggest that midsize firms are small enough to know their supply chain partners' risks, yet large enough to have the resources to adequately assess them.

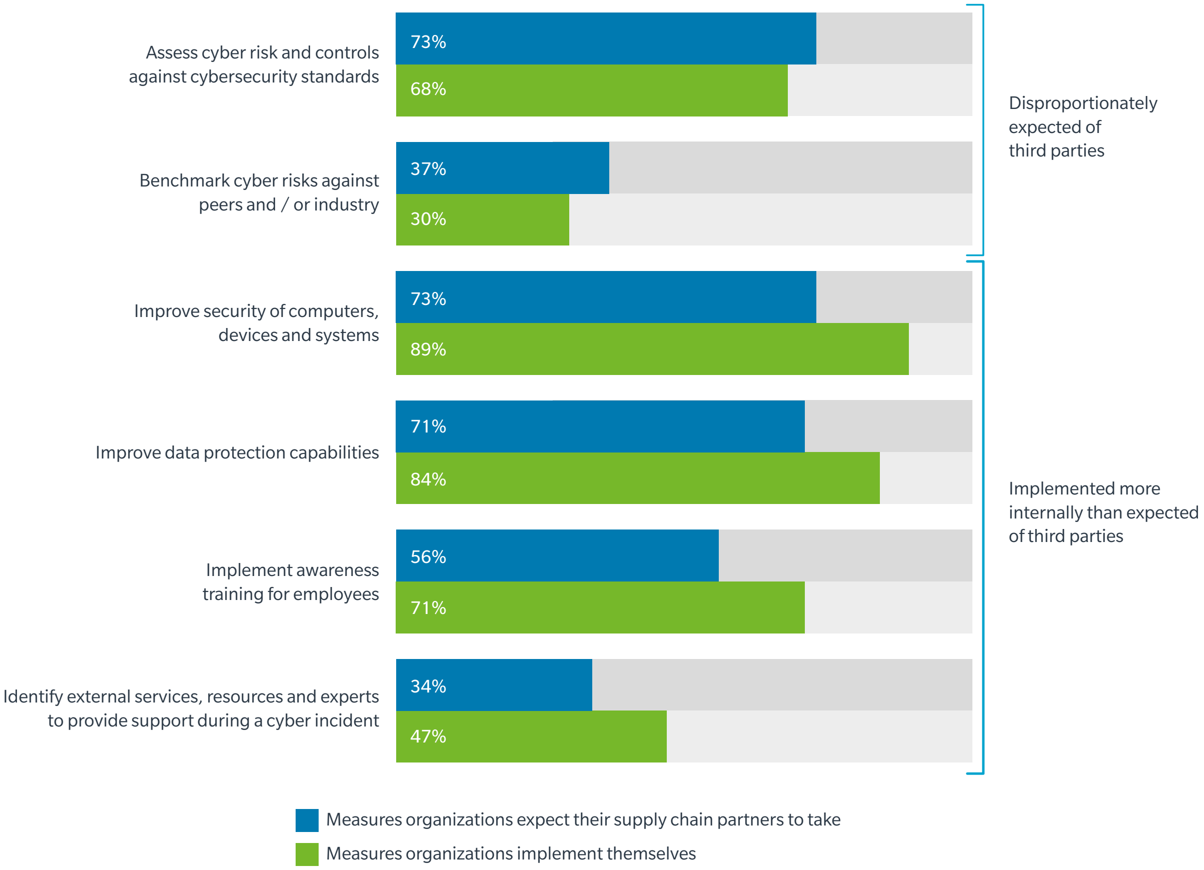
There was also a disparity between the cybersecurity measures and standards that organizations apply to themselves, versus those they expect from suppliers (see Figure 16). On balance, respondents were more likely to set a higher bar for their own organization's cyber risk management measures than they do for their suppliers.

For example, 56% of organizations said they expect suppliers in their digital supply chains to implement awareness training for their employees; yet 71% said that their organization has implemented such a requirement for itself. Such disparities could lead organizations to think their suppliers are less prepared to manage cyber risk than they themselves are, thus diminishing the organization's trust in its supply chain.

FIGURE 16

There is a disparity between what measures organizations expect of themselves versus what they expect from third parties.

Q: What cybersecurity measures do you expect your supply chain partners / thirds parties to take? Please indicate whether your organization has taken the specific actions listed below.



Base: All answering both questions: n=706 (2019)

Appetite for Government Role Draws Mixed Views

Companies see limited effectiveness of government regulation in helping manage cyber risk, but are keen for help with cyber challenges that they cannot effectively address alone.

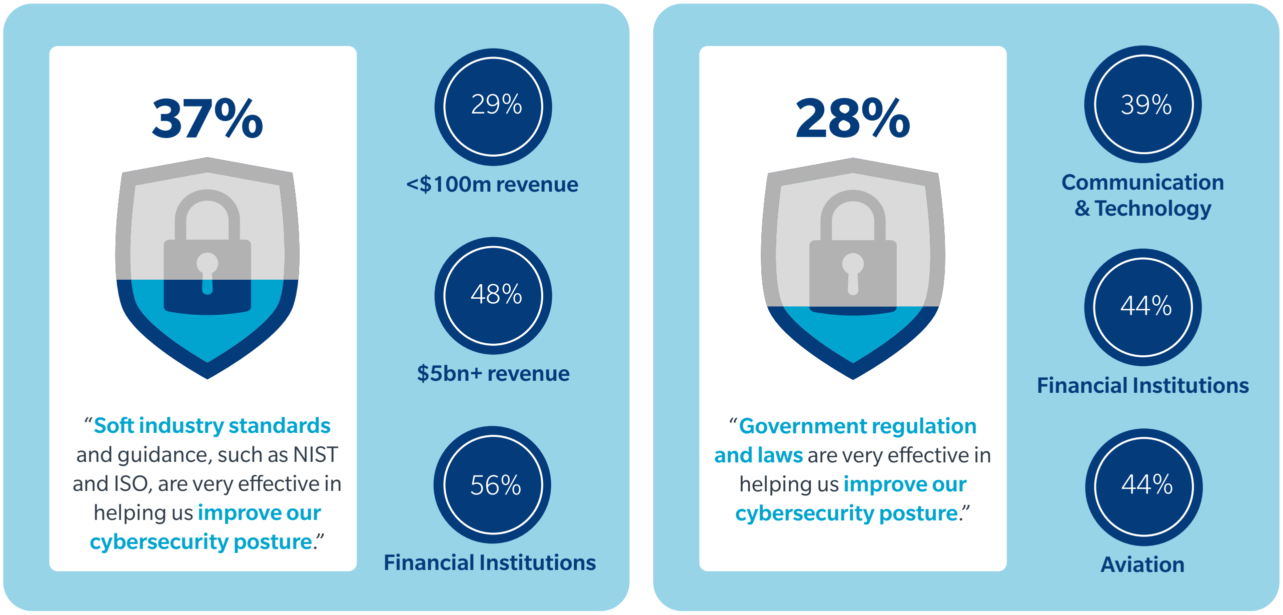
In recent years, regulators globally have enacted numerous measures to hold corporations and executives more directly accountable for ensuring effective cybersecurity and for keeping customers' data safe. Many of these regulations and legal frameworks require a greater degree of transparency from organizations at all levels of their data handling activities, and in their cyber risk management readiness. The growth in such laws and regulations complement a body of well-established cyber and information security standards from industry authorities, such as the NIST and the International Organization for Standardization (ISO).

Most 2019 survey respondents said government laws and regulations are less effective in helping them improve their cybersecurity posture compared to "soft" — voluntary — industry standards and guidance (see Figure 17). Even then, few respondents believe that either regulation or industry guidance are "very effective" in helping to improve their organization's cybersecurity posture.

FIGURE 17

Fewer than half of businesses globally regard government regulations or industry standards as being effective in improving cybersecurity.

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



Base: All answering: n=822 (2019)

Base: All answering: n=828 (2019)

Industry guidance and standards, such as NIST and ISO, appear to be best appreciated by the largest, best-resourced companies. Only 29% of organizations with revenues of under $100 million revenue see these as being effective, compared to nearly half (48%) of companies with annual revenues over $5 billion. Notably, 41% of organizations that carry out rigorous economic quantification of their cyber risks viewed NIST and ISO-type standards as being very effective.

Barely a quarter of respondent organizations identified government regulations and laws as being very effective in improving cybersecurity. This held across all major regions, despite considerable variance in local laws and regulation. However, highly regulated industries, such as aviation, financial institutions, and communications, were more likely to see value in government regulation of cyber risk.

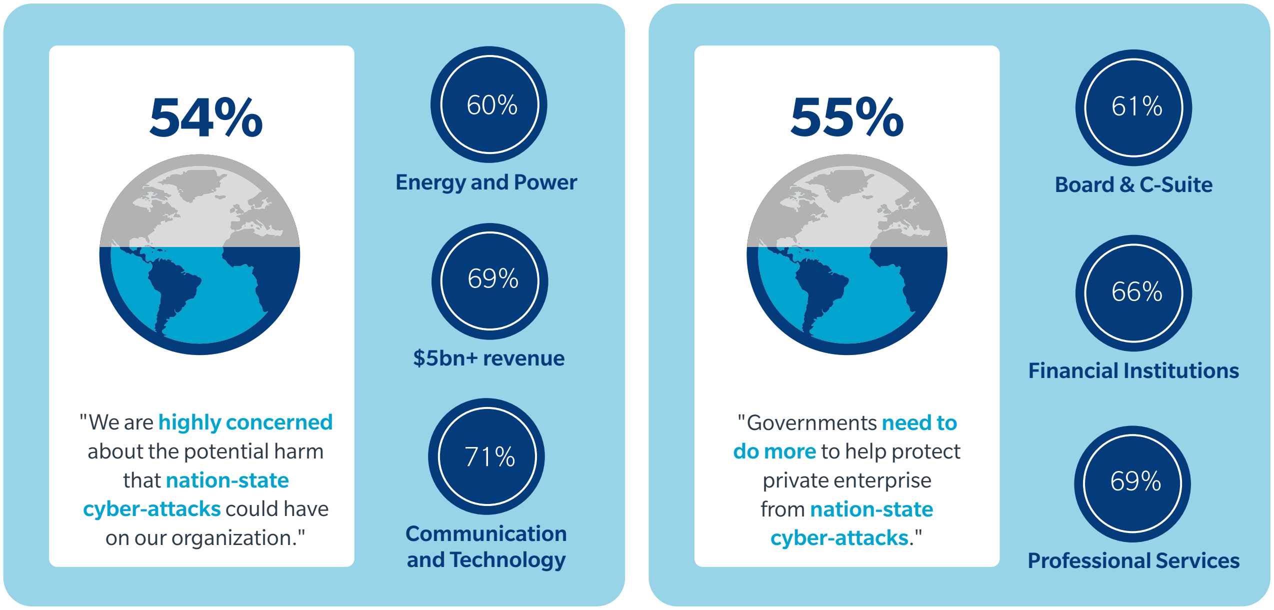
The major area of difference in the attitude toward cyber regulation related to cyber-attacks by nation-state actors (see Figure 18). In this context, a majority (54%) of respondents said they are highly concerned about the impact of nation-state cyber-attacks. This percentage rises to 60% to 70% for the largest organizations and those engaged in critical national infrastructure, such as financial institutions, aviation, communications, and energy firms. Of companies with under $100 million annual revenue, 49% registered “high concern”.

Consistent with that view, 55% of organizations said there is a need for governments to do more to protect private enterprise from nation-state cyber-attacks. This call-for-action resounds consistently across regions, with the highest positive response among financial institutions and professional services organizations. Such calls for government assistance were most often voiced by executive leadership. These results show that while firms generally prefer a non-prescriptive approach to managing their cyber security and cyber risk affairs, nation-state activity is a clear exception.

FIGURE 18

Organizations looking to government for help addressing nation-state cyber-attacks.

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



Base: All answering: n=825 (2019)

Base: All answering: n=821 (2019)

Cyber Investments Focus on Prevention, Not Resilience

Effective cyber risk management requires quantitative risk expression. Although more businesses measure their cyber risks economically than two years ago, there's a long way to go for all organizations to embrace this best practice — and then to apply that quantified measurement to drive sound cyber risk investment decisions.

Investments in cybersecurity technology are rising quickly and far outpacing spending on cyber insurance. The global cyber insurance market as measured by gross written premiums is forecast to be just under $8 billion by 2020 (see Figure 19), compared to a $124 billion global cybersecurity market.

Many organizations focus their cyber risk management strategy on prevention by investing in technological frontline cyber defenses. Meanwhile, spending on other tools and resources for cyber risk management, such as cyber insurance or event response training, remains a fraction of the technology budget. This suggests that many organizations continue to believe they can eliminate or manage their cyber risk primarily through technology, rather than through a comprehensive range of planning, transfer, and response measures.

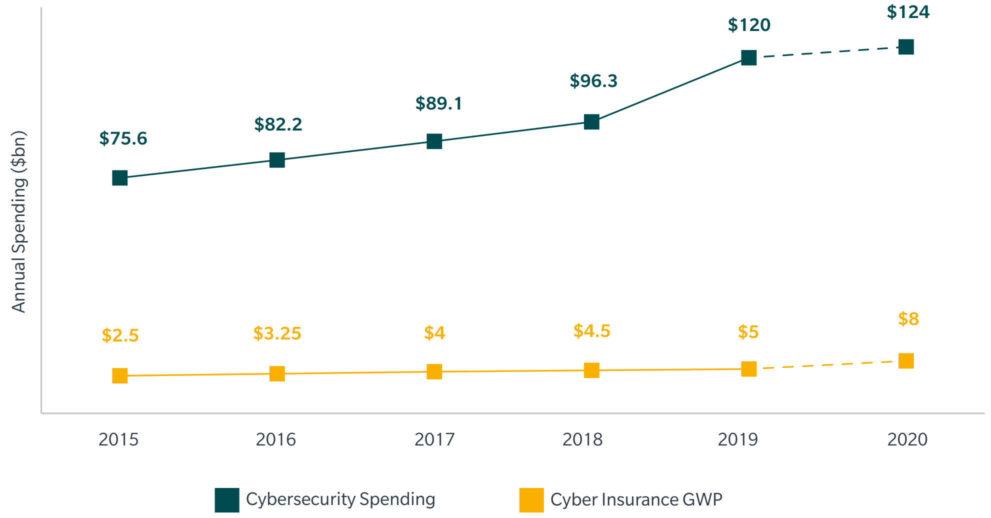
Best practice calls not for parity of spending, but an investment strategy that, reflecting an organization's unique risk profile and appetite, leverages the complementary roles of technology and insurance to deter cyber-attacks where possible and transfer the risk of those that cannot be prevented. However, the emphasis on cybersecurity spending and technology over other measures reveals that many organizations have not yet embraced this truth.

For example, the vast majority of survey respondents cited one or more technical improvements as actions they have taken over the past 12 to 24 months (see Figure 20). Fewer initiatives are taken in areas such as employee training, cybersecurity policies, and cyber incident response plans.

FIGURE 19

Cybersecurity spending far outpaces cyber insurance spending.

SOURCE: Gartner, Munich Re

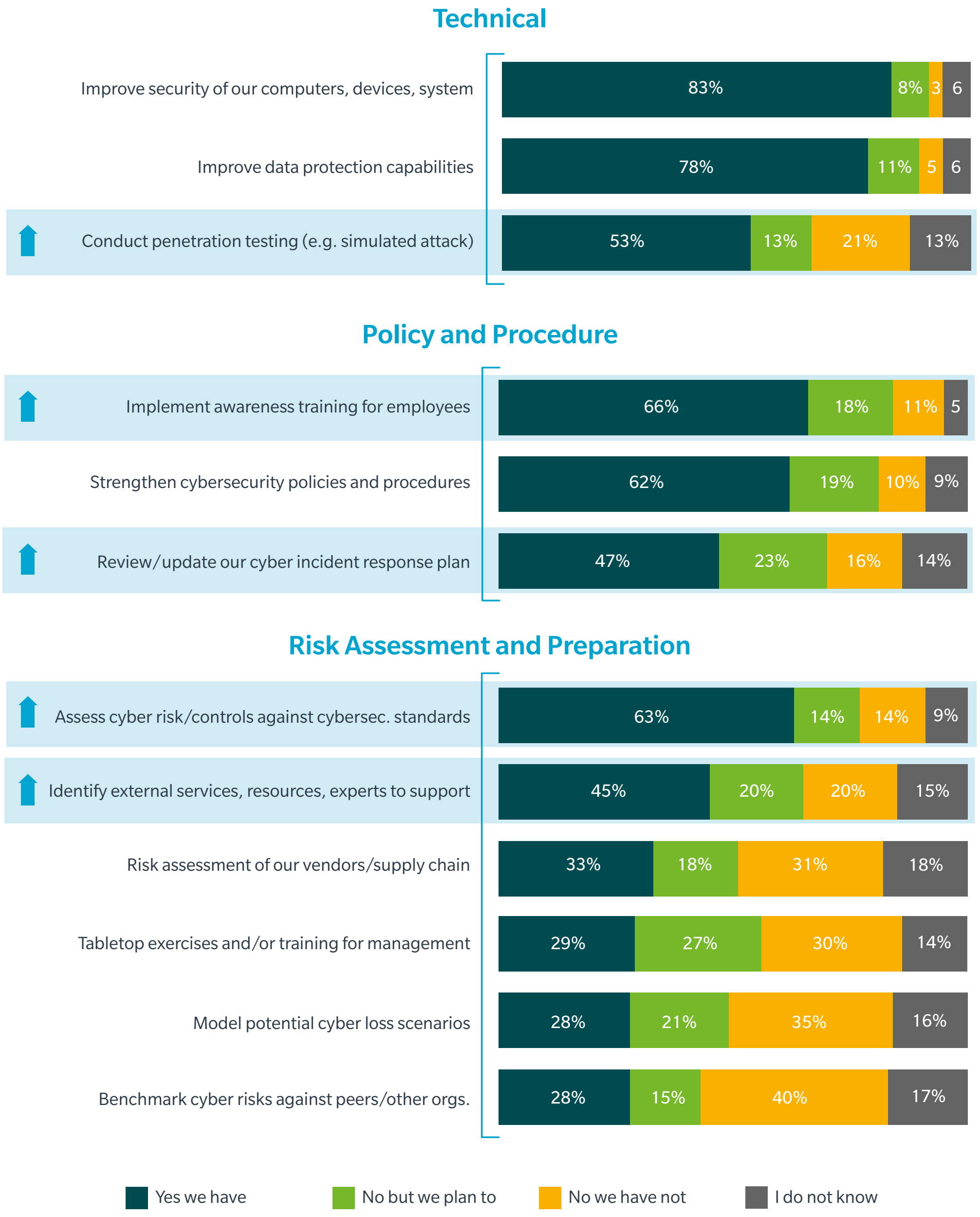


Some of the least commonly reported actions were those closely aligned with the assessment and modeling of cyber risks. The range of actions was largely unchanged from 2017. The exception regarding cyber risk assessment was where the risks were primarily technical — 63% said they assessed their technical controls against established cybersecurity standards.

FIGURE 20

Cyber risk actions tend to focus on technical measures.

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



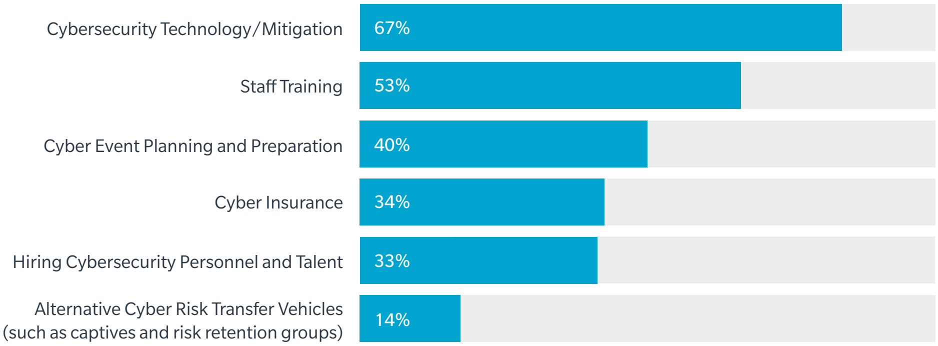
Base: All answering: n=1118 (2019) ⬆ Significantly more firms taking action vs. 2017

Looking forward, the trends appear set to continue. Among areas in which firms plan to increase risk management spending over the next three years, two-thirds cited cybersecurity technology/mitigation, far more than in all other areas (see Figure 21).

FIGURE 21

Cybersecurity technology and mitigation 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?



% expecting to spend some or significantly more on each area
Base: All answering: n=885 (2019)

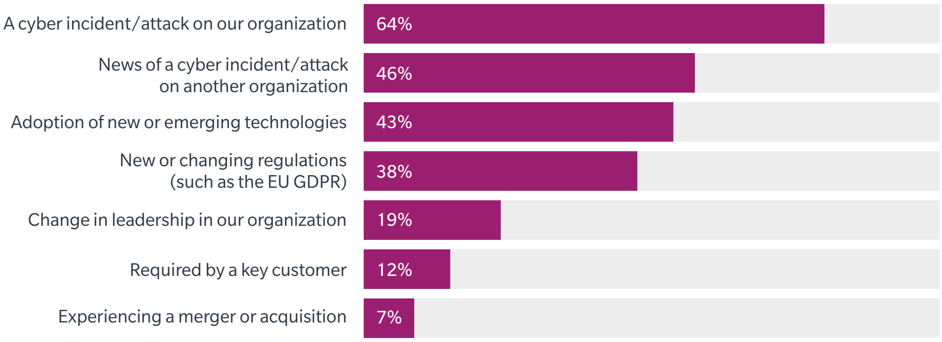
Spending on technology continues to rise, but without a corresponding increase in the use of economic frameworks — such as cyber risk quantification — to inform investment decisions, measure risk reduction effectiveness, or enable comparison with other corporate risk investments.

In fact, many organizations seem to have a reactive stance toward cyber risks: The most commonly cited trigger for increasing investment was for a cyber incident to occur (see Figure 22). Far less common was for business leaders to proactively initiate a focus on cyber risk investment.

FIGURE 22

Cyber incidents are the main trigger for increases in cyber risk management investments.

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?



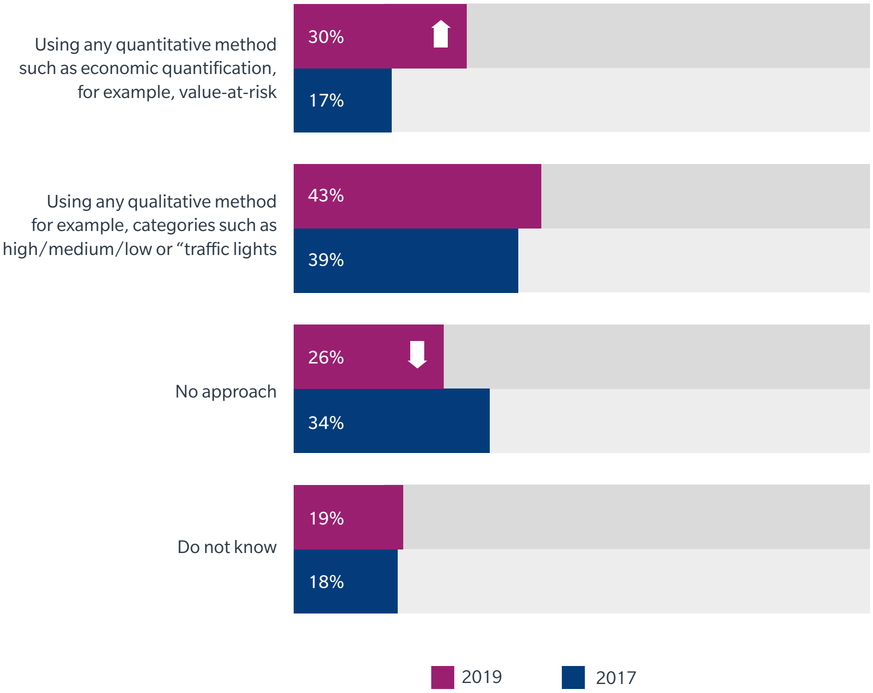
% selecting as a driver for any area of increased cyber risk investment
Base: All answering & stating they plan to invest more, excluding don't know responses: n=615 (2019)

The use of quantitative methods to express cyber risk exposures is making headway (see Figure 23). The proportion of organizations globally that used such methods nearly doubled since 2017, from 17% to 30%. There was a concurrent decrease — from 34% to 26% — in the share of respondents saying they have no approach to formally or systematically assess their cyber risk exposure.

FIGURE 23

Quantitative measurement of cyber risk exposure has increased substantially since 2017, but remains low overall.

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



Base: All answering: n=1303 (2019); n=1312 (2017)

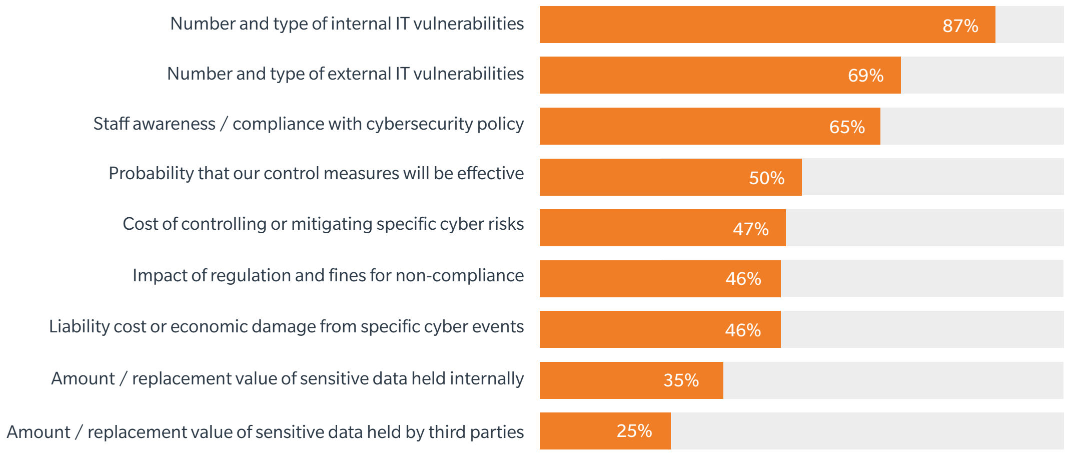
Still, most respondents in 2019 (70%) were not expressing their cyber risk exposures quantitatively or using quantitative data to drive investment decisions. This may stem from a lack of organizational expertise regarding cyber risk quantification, a lack of resources (time and money), or the likelihood that many companies still view cyber threats as more of a technology issue than an economic risk. The latter position is supported by the fact that nearly twice as many organizations assess cyber risk by counting IT vulnerabilities compared to those assessing potential costs, fines, and losses (see Figure 24).

Aside from how cyber risks are expressed, the areas considered when conducting assessments also varied widely. Organizations undertaking some form of cyber risk assessment tended to focus on counting technical vulnerabilities, rather than on remediation or recovery costs, fines, or other liabilities.

FIGURE 24

Risk assessment methods focus on counting technical vulnerabilities, but fail to adequately consider economic aspects of cyber exposure.

Q: Which of the following does your organization consider in its cyber risk assessment/measurement?



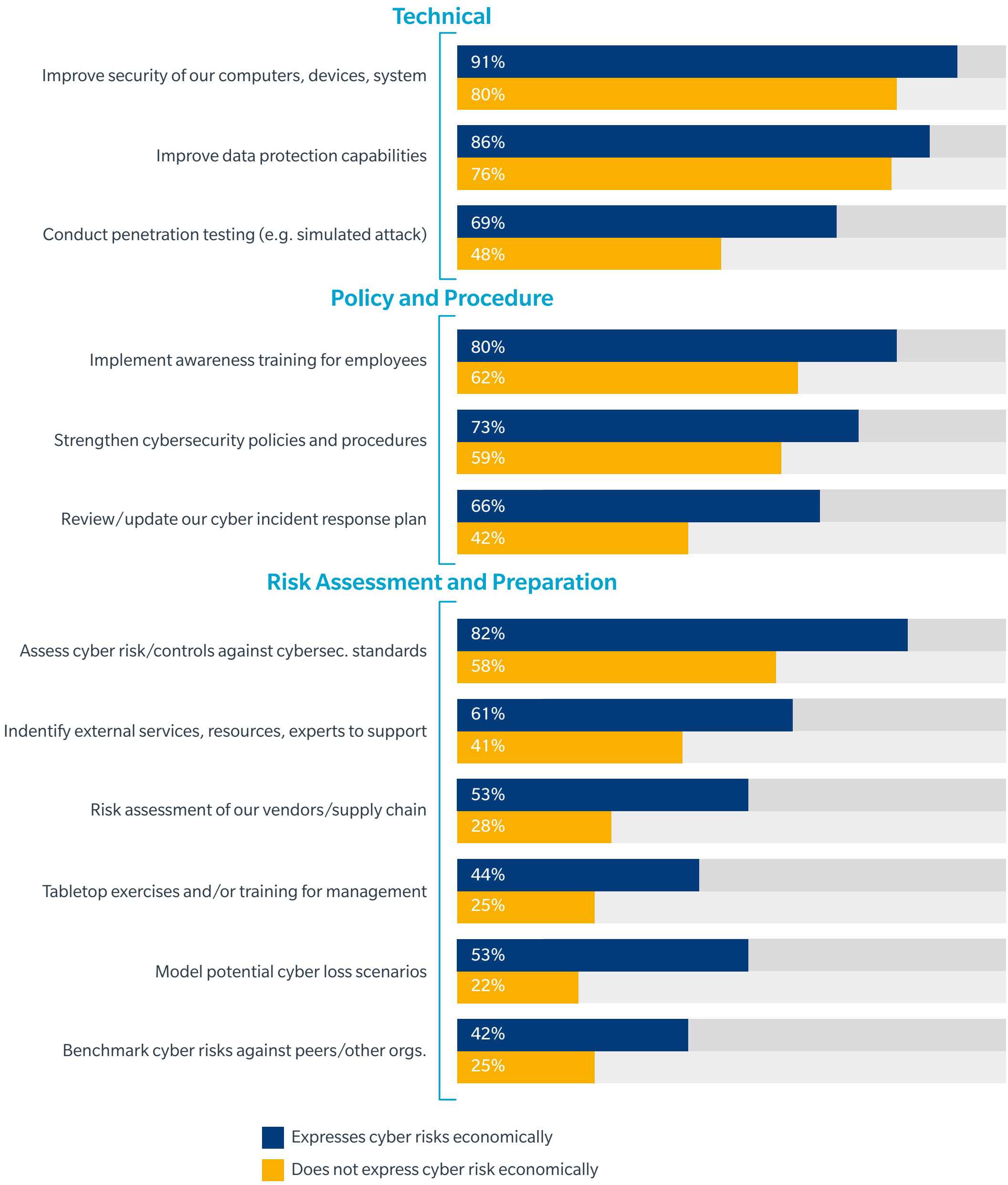
Base: Those with some form of cyber risk assessment method: n=660 (2019)

Organizations that express and report cyber risk economically appear to be substantially more likely to implement a greater range of assessment, planning, and training activities that complement technical measures, and are essential to building cyber resilience (see Figure 25). These entail risk transfer, policy and procedural measures, and a comprehensive approach to risk assessment, including evaluation of vendors and supply chains.

FIGURE 25

Companies conducting economic quantification of cyber risk are more likely to balance technical and non-technical actions.

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



Base: All answering: n=1118 (2019)

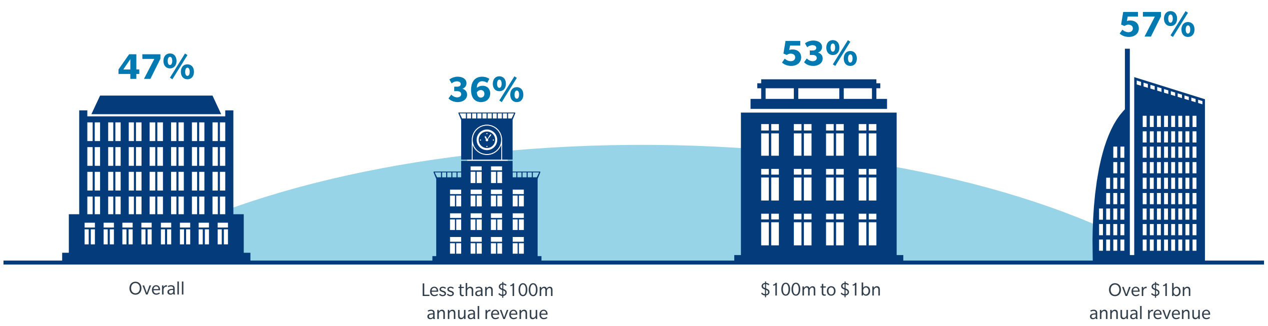
But not all cyber risks can be mitigated through technology, policy, or process, especially those low frequency but high severity losses that can inflict significant financial and operational damage. In these cases, risk transfer through insurance or other methods is essential.

Globally, 47% of firms say they now have such insurance coverage in place (see Figure 26). Underlying this picture are diverging trends around company size: While more than half of midsize and large enterprises currently purchase cyber insurance, a minority (36%) of firms with less than $100 million revenue do so.

FIGURE 26

Midsize and larger enterprises are more likely to have cyber insurance.

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



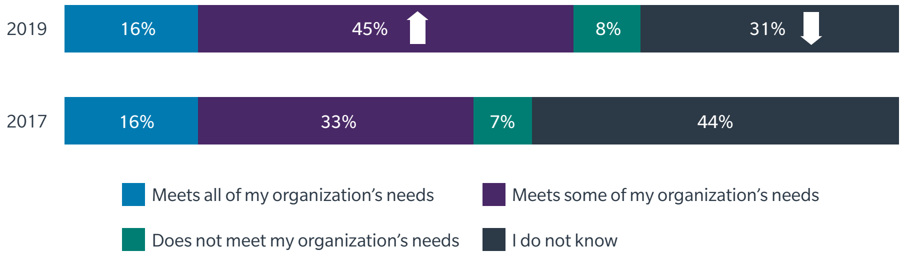
Base: All answering, excluding don't know responses: n=1120 (2019)

Since 2017, there has been a significant decrease in uncertainty around cyber insurance's capacity to protect against losses. Organizations stating that they "do not know" if the cyber insurance available is adequate fell from 44% in 2017, to 31% in 2019 (see Figure 27). Likewise, the proportion of all companies that say cyber insurance meets at least some organizational needs rose from 49% in 2017 to 61% in 2019. The challenge for insurers going forward is to increase buyer perceptions that cyber insurance can adequately meet organizational needs, as that figure remained constant at 16%.

FIGURE 27

Uncertainty in the ability of cyber insurance to meet an organization's needs declined significantly over the past two years.

Q: Please finish this sentence by selecting one of the options below: The cyber insurance available in today's market...



Base: All answering; n=1307 (2019); n=1120 (2017)

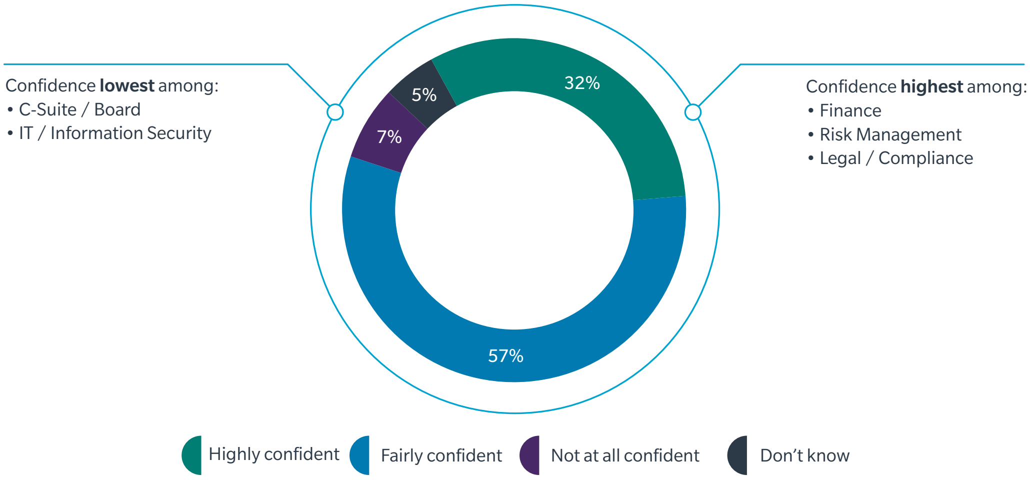
This moderate level of certainty is echoed in perceptions about the responsiveness of specific organizational cyber policies. One-third of organizations expressed high confidence that their insurance would provide cover for the costs associated with a cyber event, and more than half were fairly confident (see Figure 28).

Only 7% said they were "not at all confident." Confidence in the adequacy of existing insurance programs is higher among those respondents who are likely most familiar with their organization's insurance programs, such as those in risk management, finance, and legal/compliance roles.

FIGURE 28

More than 4/5 of organizations are highly or fairly confident their insurance policies would cover the costs of a cyber event.

Q: How confident are you that the coverages within your organization's insurance program - cyber policies and/or other policies - will respond to costs incurred by your organization in the event of a cyber event?



Base: All with cyber insurance: n=526 (2019)

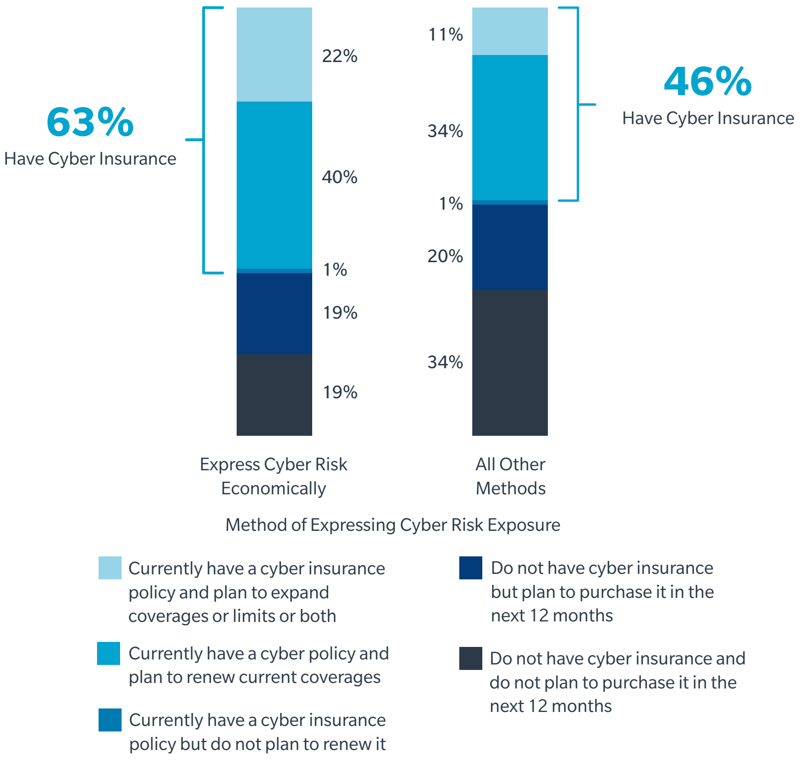
Organizations that use economic cyber risk assessment methods are more likely to purchase cyber insurance than those that use only qualitative methods or no method at all to assess exposures to cyber risks (see Figure 29).

Companies that economically quantify their cyber risk exposures may be more informed about, and disposed to capitalize on, the value of cyber insurance. Accordingly, twice the proportion of firms that express risk economically plan to expand coverage, compared to those that do not.

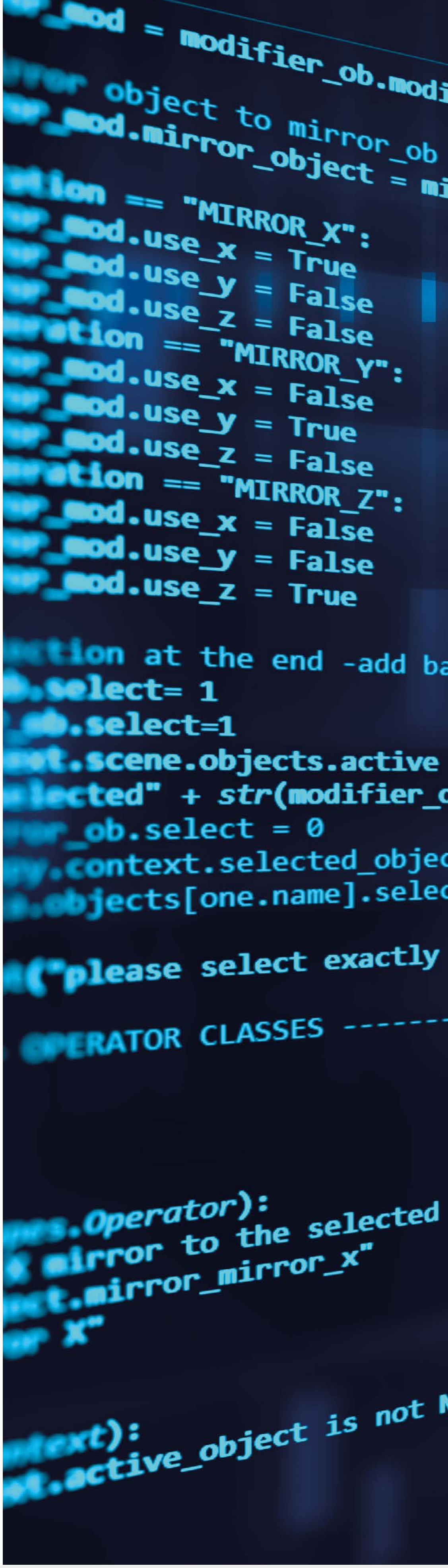
FIGURE 29

Organizations that use economic cyber risk assessment methods are more likely to purchase cyber insurance and increase current coverages.

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



Base: All answering, excluding dont know responses: n = 1120 (2019)



```
_mod = modifier_ob.modi
object to mirror_ob
_mod.mirror_object = mi
tion == "MIRROR_X":
_mod.use_x = True
_mod.use_y = False
_mod.use_z = False
ation == "MIRROR_Y":
_mod.use_x = False
_mod.use_y = True
_mod.use_z = False
ation == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True

tion at the end -add ba
.select= 1
.select=1
.scene.objects.active
lected" + str(modifier_
_ob.select = 0
.context.selected_objec
.objects[one.name].selec

("please select exactly

ERATOR CLASSES -------

s.Operator):
mirror to the selected
t.mirror_mirror_x"
r x"

xt):
t.active_object is not
```

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 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 your Marsh representative or a colleague below:

SARAH STEPHENS
Cyber Practice Leader
sarah.stephens@marsh.com
+44 (0)20 7558 3548

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

This is a marketing communication.

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511).