Marsh | Microsoft

The state of cyber resilience

A new report by Marsh and Microsoft to help leaders from all departments align and prioritize their cyber strategies for 2022 and beyond.

Contents

Introduction

The toll of almost three years of unrelenting workplace disruption, digital transformation, and ransomware attacks means most leaders are no more confident in their ability to manage cyber risk than they were two years ago. That's one of the findings from the 2022 Marsh and Microsoft Cyber Risk Survey, the third such collaboration our companies have undertaken in the past four years.

One thing holding back confidence is that most companies have not adopted an enterprise-wide approach to cyber risk; one that at its core is about broad-based communication and fosters collaboration and alignment between stakeholders during key decision–making moments of truth on their cyber resilience journey. For example, all departments that touch cyber risk should be involved in cyber incident management, and cyber insights should be shared across the enterprise to appropriately address organizational cybersecurity weak spots.

This year, our report looks at how cyber risk is viewed by various functions and leaders in the company, specifically cybersecurity and IT, risk management and insurance, finance, and executive leadership.

While all of these functions have common interests around cyber risks, we found they often act independently, missing the potential benefits that an enterprise-wide approach offers. Their different views and separate ways of managing cyber risks are reflected in our finding that only 41% of organizations engage legal, corporate planning, finance, operations, or supply chain management in making cyber risk plans.

In the following pages, you'll find eight key trends that your company's cyber leaders can discuss as they seek a common understanding of cyber risk. The report also looks at the roles and responsibilities of your enterprise's cyber team to help them understand each other's needs, responsibilities, and perspectives. And finally, we share some best practices your company can use in aligning the enterprise to more effectively manage cyber risk.

We'd like to thank the more than 650 cyber risk leaders at organizations around the world who took the time to share their thoughts on this important topic. We hope this report brings your organization together, and spurs conversations as you build an enterprise-wide approach for cyber resilience.

Only 41% of organizations engage legal, corporate planning, finance, operations, or supply chain management in making cyber risk plans

Executive Summary

Cyber risk is pervasive at most organizations. An employee or vendor firing up their laptop from home brings risk. A user connecting a new product to the Internet of Things introduces risk. Deciding not to launch a new product, fearing cyber threats, is a risk. And the list goes on. Countering such risks requires enterprise-wide alignment.

Key cyber risk trends

As we analyzed the responses from the *2022 Marsh and Microsoft Cyber Risk Survey*, eight trends stood out:

1. Cyber-specific enterprise-wide goals — including cybersecurity measures, insurance, data and analytics, and incident response plans — should be aligned to building cyber resilience versus simply preventing incidents, as every organization can expect a cyberattack. *73% of companies said they had experienced a cyberattack.*

2. Ransomware is considered the top cyber threat faced by companies, but not the only one. *Other prevalent threats include phishing/social engineering, privacy breaches, and business interruption due to an external supplier being attacked*.

3. Insurance is an important part of cyber risk management strategy, and influences the adoption of best practices and controls. *61% said their company buys some type of cyber insurance coverage.*

4. Adoption of more cybersecurity controls leads to higher cyber hygiene ratings. *Just 3% of respondents rated their company's cyber hygiene as excellent.*

5. Organizations lag in measuring cyber risk in financial terms, which hurts their ability to effectively communicate cyber threats across the enterprise. *Just 26% of respondents said their organization uses financial measures for cyber risk.*

6. Increased investment in cyber risk mitigation continues, though spending priorities vary across the enterprise. *64% said the spur to increasing cyber risk investments was having experienced an attack.*

7. New technologies need to be assessed and monitored on a continuous basis, not just during exploration and testing prior to adoption. *54% of companies said they do not extend risk assessments of new technologies beyond implementation.*

8. Firms take many cybersecurity actions, but widely overlook their vendors/digital supply chains. *Only 43% have conducted a risk assessment of their vendor/supply chain.*

Building a resilient team

It's important to understand how professionals across an enterprise view their role when it comes to cyber insurance, cyber incident management, cybersecurity tools and services, and more. Do they consider their function to be the decision maker? To be part of the overall team, with inputs into the decisions? Or are they not involved at all? The answers will go a long way in determining the next steps your company needs to take to develop enterprise-wide cyber resilience.

We found the level of involvement in various areas of cyber risk management to be a mishmash of roles and responsibilities. For example, risk management and insurance professionals tend to be on the cyber incident management team, but generally absent from discussions of cybersecurity tools and services. There is no clear leader for decisions around cyber insurance. In addition, more than a quarter of risk managers and finance professionals say they are not involved in cyber incident management.

While responses reflected a widespread desire to increase spending on cyber risk, exactly where the investments should be made varies by function. The reason role clarity and clear authority for decision making matters is to help organizations maximize the efficiency of those investments.

Best practices

A best practices approach to cyber risk management spans organizational roles. This includes investing and engaging in a broad, balanced, and continuously updated array of resources and activities to mitigate cyber risks and reinforce cyber resilience. However, even the best tools and activities are unlikely to meet their potential if there is not effective communication across the enterprise.

Understanding cyber risks: 8 key trends to know today

It’s important that leaders across an organization have a common understanding of overall cyber risk trends and how these affect their business. Having a common understanding of the risk issues facing the company helps align decision makers and drive strategy, while also presenting a united message to other internal and external stakeholders.

As with any risk, cyber trends will change over time. Following are eight key areas in today’s cyber environment.

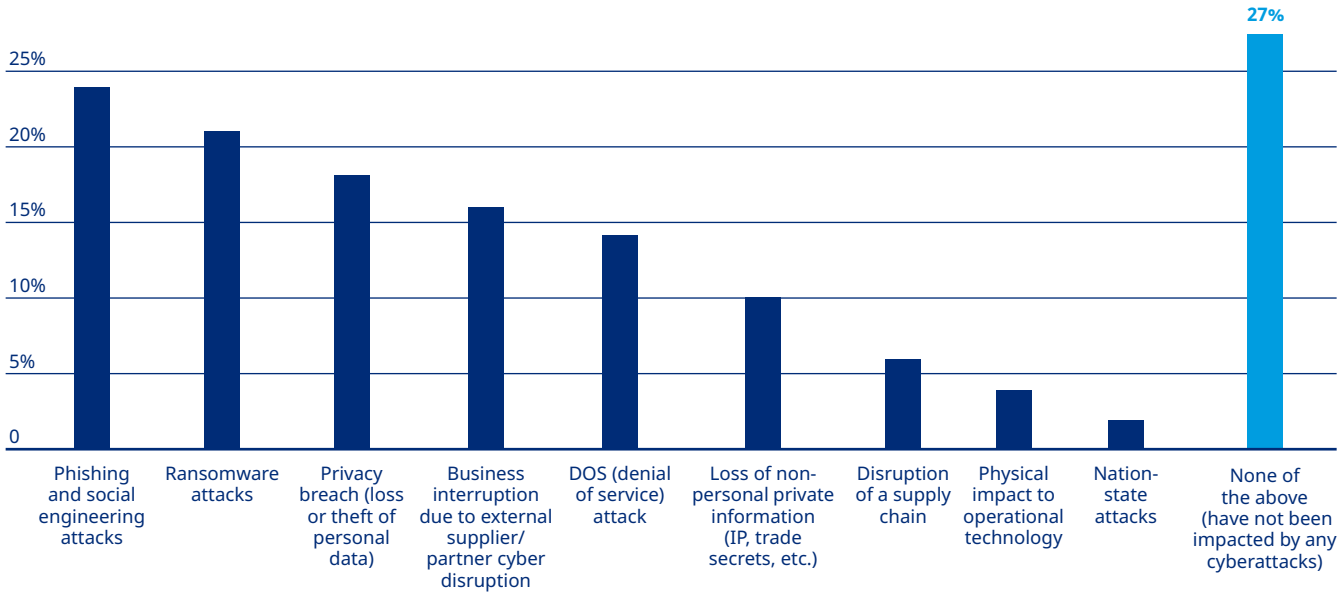
KEY TREND #1

Cyber-specific enterprise-wide goals should be aligned to building cyber resilience as every organization can expect a cyberattack.

A truism has developed around cyber risk that is worth repeating: What would you do differently now, if you knew you would be breached today? Among our survey respondents, nearly three-quarters said their organization had experienced one or more cyberattacks in the past year, with the most common types involving phishing/social engineering and ransomware.

- The largest companies by revenue faced more attacks in both number and variety, with 85% saying they had been subject to at least one attack, compared to 68% of smaller organizations.
- Regionally, businesses based in Latin America were the least likely to report having experienced any type of cyberattack, particularly privacy breaches. Those in the Pacific region were significantly more likely to have experienced privacy breaches than those in other regions.

Types of cyberattacks experienced by organization



Nearly

75%

of organizations have experienced cyberattacks

KEY TREND #2

Ransomware is considered the top cyber threat facing companies, but not the only one.

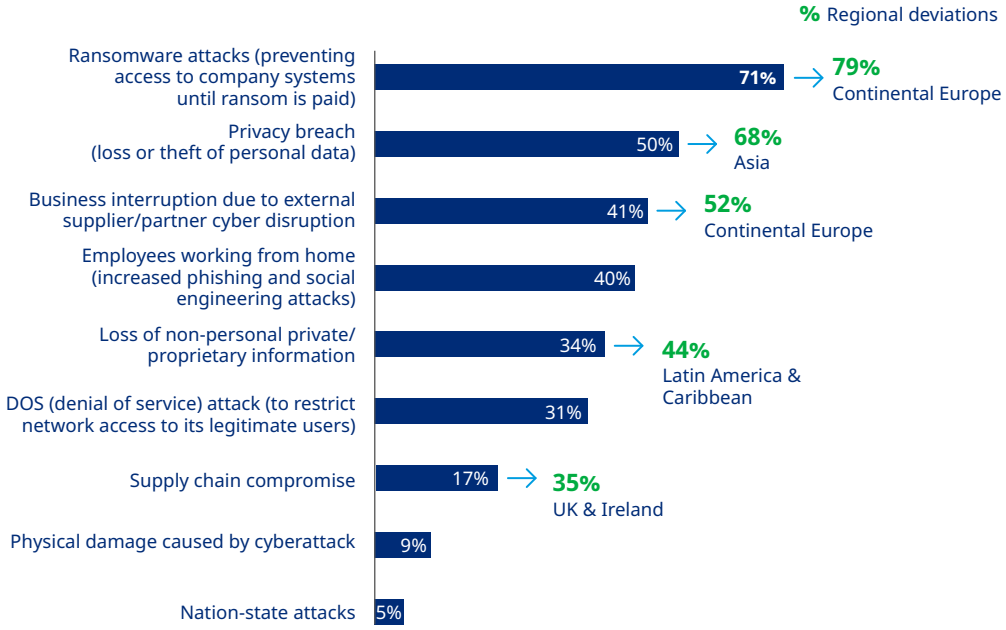
Many conversations about cyber risk today begin with a discussion of the pervasiveness of ransomware. Survey respondents ranked ransomware at the top of cyber risks facing their organizations, with more than one-third saying it is the number one threat, and nearly three-quarters placing it in the top three.

- Organizations feel that the infinite number of vulnerabilities make ransomware nearly impossible to safeguard against. This hammers home the importance of developing a cyber resilient organization.
- Professionals in risk management and insurance roles are more likely to point to ransomware as a key driver of attacks; board and CEO-level leaders are less likely to hold that view.
- Over half of North American firms say companies that pay attackers' ransom demands contribute to the increasing incidence.

While ransomware topped the list of cyber threats, privacy breaches, supplier disruptions, and phishing/social engineering followed behind, globally. Setting ransomware aside, the top concerns differed by region. For example, European organizations were more likely to single out supplier/partner disruptions, Asian organizations showed greater concern around privacy breaches, and Latin American ones more often cited loss of proprietary business information.

Ransomware tops the list of cyber threats

Top cyber threats to organization



KEY TREND #3

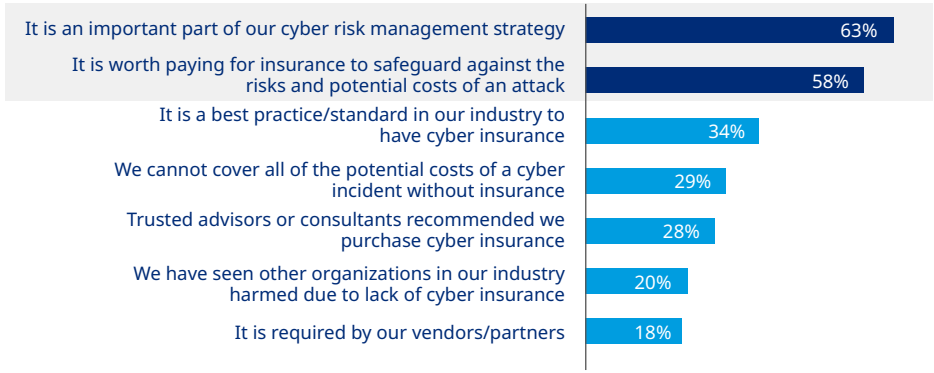
Insurance is an important part of cyber risk management strategy, and influences the adoption of best practices and controls.

Cyber insurance has proven resilient since it was introduced in the late 1990s. It has developed into a product that addresses an array of digitally derived risks and has effectively paid claims as intended, which helps companies to manage risks more responsibly and holistically as they innovate and digitalize their businesses. It also creates a valuable feedback loop as insurers learn from claims and shift the focus of their underwriting requirements to those controls that could have mitigated them.

- Among survey respondents, 61% said their organization purchases some type of cyber coverage, nearly a 30% increase since our last survey in 2019. Insurance was often cited as an important part of the overall cyber risk strategy, as a safeguard against the potential costs of an attack.
- The adoption of certain controls has now become a minimum requirement for a majority of insurers, with organizations' potential insurability on the line. This was said to have a positive effect on cybersecurity postures, with 41% of respondents saying insurers' requirements influenced decisions to augment existing controls or adopt new ones.
- While these controls have been established as best practices for several years, some organizations are still struggling to adopt them — most often because they have not been able to justify the cost or did not understand or see the need for them.

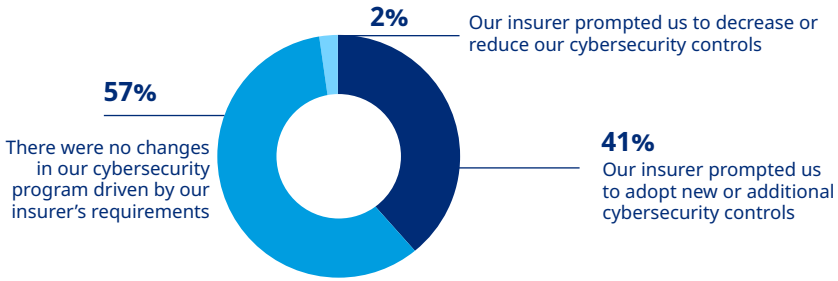
Insurance is widely viewed as an important part of cyber risk management strategy

Reasons for purchasing cyber insurance



Cyber insurance underwriting requirements impact the adoption of controls

Impacts of insurance underwriting requirements/cybersecurity controls on cybersecurity decisions



KEY TREND #4

Adoption of more cybersecurity controls leads to higher cyber hygiene ratings.

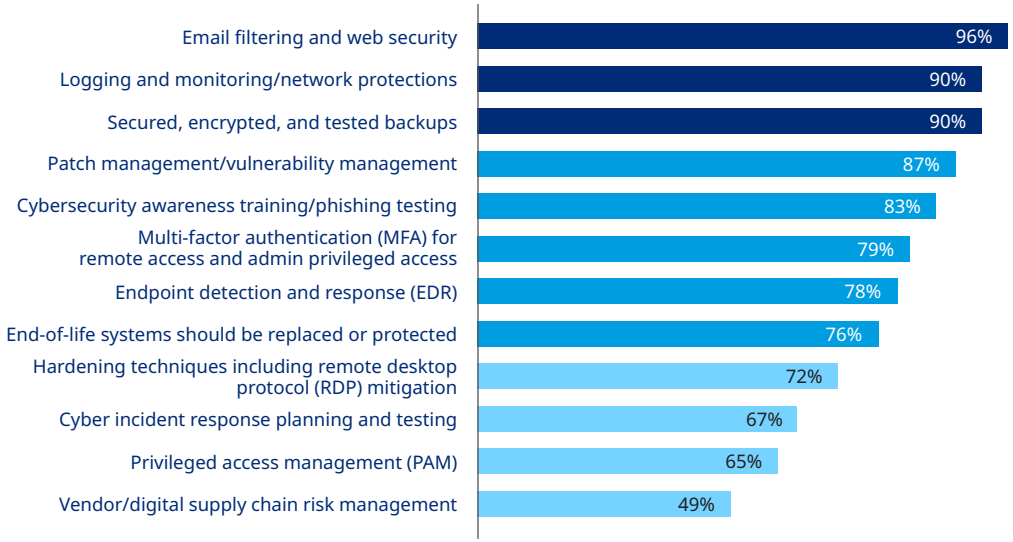
Organizations looking to strategically address cyber risk and increase cyber hygiene should consider adopting 12 cybersecurity controls recognized by cybersecurity experts to help prevent, respond, minimize, and recover from a cyberattack. While these controls have been established for quite some time, more focus has been placed on them of late. This is due in part to the continuing rise of the frequency and severity of ransomware attacks and in part to insurers' ability to identify the effects of certain controls on corresponding cyber incidents and claims.

- Organizations using all or most of the 12 cybersecurity controls were nearly two times more likely to rate their cyber hygiene as "very good" or "excellent."
- Larger companies are generally ahead of smaller ones and are more likely to have nearly all of the controls in place, though even here some companies face gaps.
- Companies with cyber insurance were likely to have taken more actions to build security and to have stricter controls in place than those without.

66% **of respondents say home and and remote working tops the list of technologies seen as enabling cyberattacks**

Email filtering and web security are widespread among a dozen cyber hygiene controls

Cybersecurity controls currently used



How respondents rate their organization's overall "cyber hygiene"

40%

Needs improvement

34%

Satisfactory

23%

Very good

3%

Excellent

KEY TREND #5

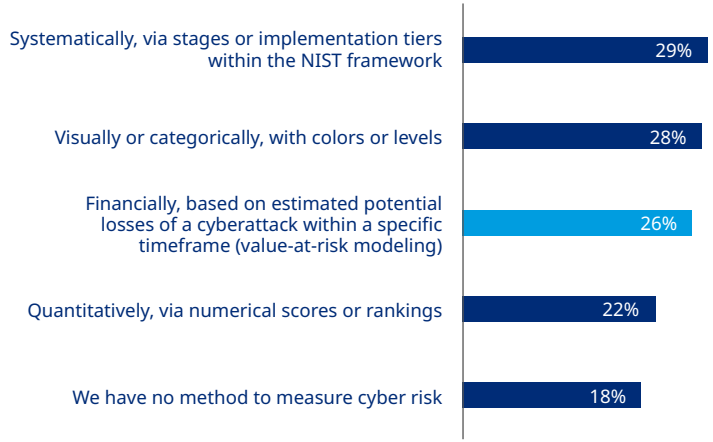
Many organizations lag in measuring cyber risk in financial terms, which hurts their ability to effectively communicate cyber threats across the enterprise.

Putting cyber risks into financial terms is critical to building an enterprise-wide approach to its management. Part of cyber risk resilience involves understanding how cyberattacks and other events can create financial volatility, over both the near and long term. Yet most respondents said their organizations do not use a financial measure when evaluating cyber risk. Which leads to questions such as: How can they know how much risk — or which risks — they can afford? How do they reserve for it?

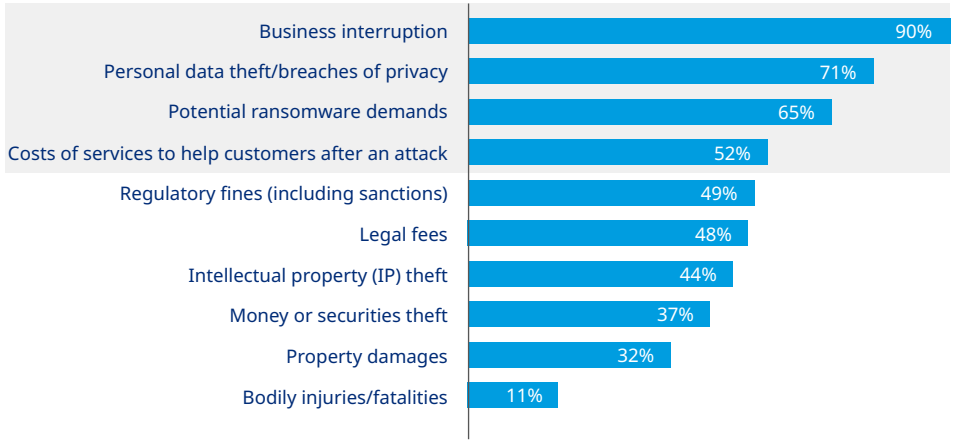
- Large enterprises are significantly more likely to use formal methods to assess cyber risk exposure.
- Regionally, organizations based in the Latin America and Caribbean region are more likely to use qualitative assessment methods.
- Among the 26% that use value-at-risk calculations, most (90%) use business interruption in their calculations, while more than half use theft of personal data/privacy breaches, potential ransomware demands, and the costs of services to help customers following an attack.

Measurements of cyber risk exposure would benefit by incorporating a financial method

Method used to measure cyber risk exposure



Factors used in financial calculations



Only 26% of respondents said their organization uses financial measures for cyber risk

KEY TREND #6

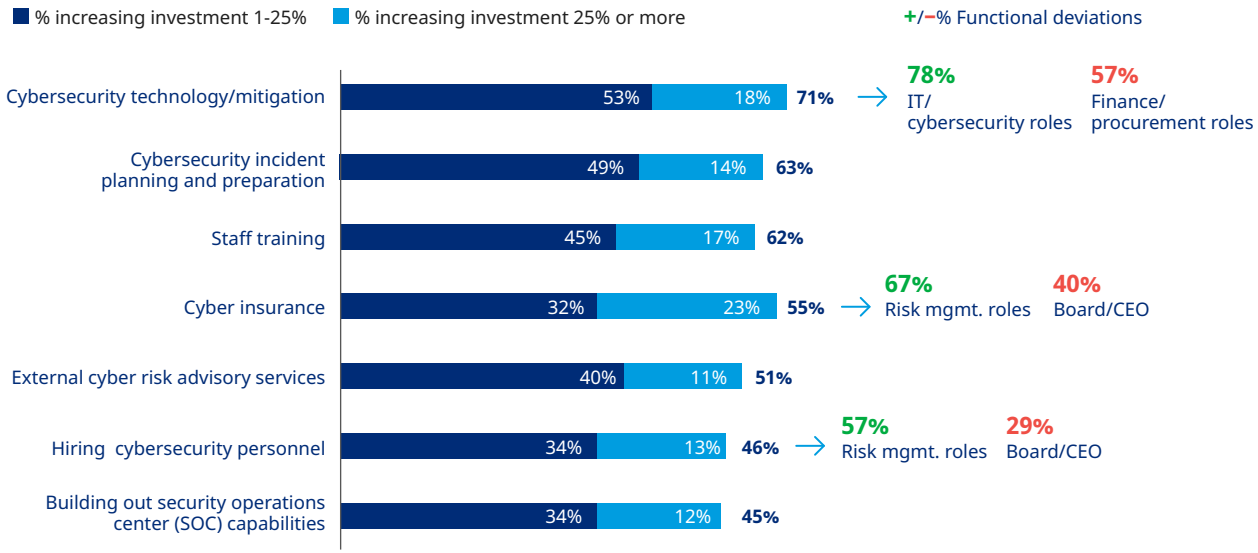
Increased investment in cyber risk mitigation continues, though spending priorities vary across the enterprise.

Globally, most organizations plan to increase spending on cybersecurity technology, incident planning, staff training, cyber insurance, and cyber advisory services over the next year. Cyber risk leaders, overall, recognize the need to invest in multiple internal and external resources to reinforce overall cyber resilience. However, thoughts on where investments should be directed often vary within an organization by department and by cyber risk leader.

- Having experienced a cyber incident was the main driver cited for the decision to increase investments. Other top reasons included external advisor recommendations and the adoption of new technologies/digital transformation.
- Nearly a quarter of organizations said their spending on cyber insurance will rise by 25% or higher in 2022.
- Risk management/insurance roles most often said they will look to prioritize investments in cyber insurance and hiring cybersecurity personnel.
- CEO/board-level roles generally saw increases coming in cybersecurity technology/mitigation, staff training, and cybersecurity incident planning and preparation.
- Larger organizations were more likely to say they will use investments to hire cybersecurity talent and build out SOC capabilities.

Cybersecurity technology and mitigation is the most common area for investment increases

Expected change in cyber risk investments over next 12 months



KEY TREND #7

New technologies should be assessed and monitored on a continuous basis, not just during exploration and testing prior to adoption.

While 69% of surveyed companies find it important to assess the risks from new technologies while they are in the exploration and testing stage of development, 54% said they do not extend risk assessments of new technologies beyond implementation. Continuous assessment and monitoring of a new technology past the implementation phase is necessary given the fact that digitalization and technological advancements increase exposure to new and more intense cyber vulnerabilities.

- The decline in evaluating the risks post-adoption may be related to a broader issue around barriers that exist in implementing cyber risk assessment methods. These include a lack of talent, relevant data, and internal consensus.
- When respondents were asked what the largest barriers to cyber risk assessment are for their organization, 53% believe the largest barrier is not having the right employees and talent to do so, while 33% claim that having access to the right data was an obstacle.
- There may also be issues related to "handing off" a new technology from the development team to other parts of the organization. This is an example of the potential advantages in approaching cyber risk as an enterprise-wide endeavor; such gaps would be less likely to appear if a coordinated, cross-functional mentality was the norm.

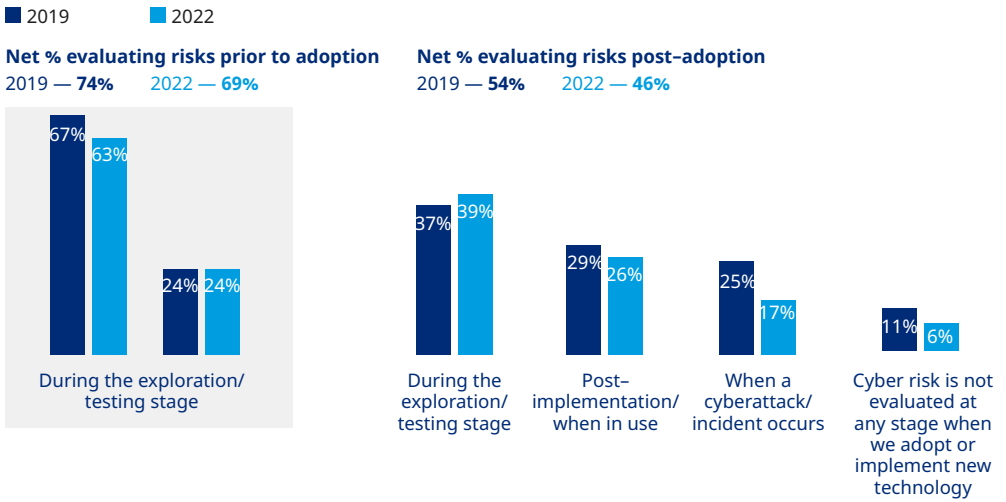
Barriers to implementation of cyber risk assessment methods

53% of organizations believe the largest barrier to cyber risk assessment is not having the right employees/talent to do so

33% claim not having the right data is an obstacle in evaluating new technologies

Many companies stop evaluating new technologies' cyber risk at some stage of adoption

When cyber risk is evaluated during technology adoption and implementation



KEY TREND #8

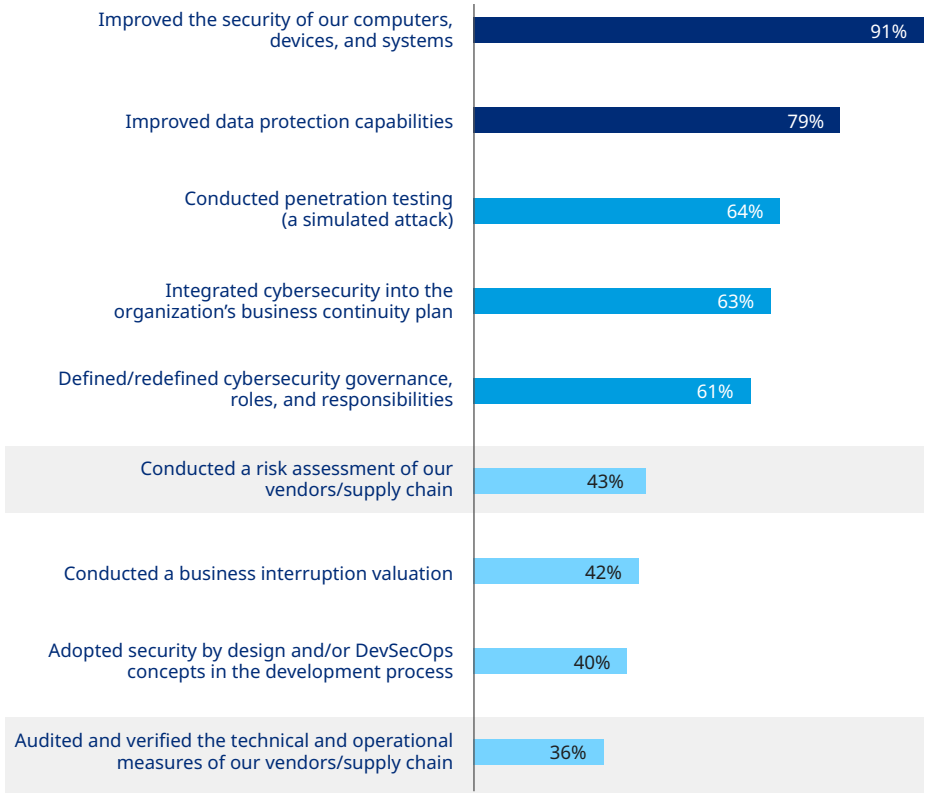
Firms take many cybersecurity actions, but widely overlook their vendors/digital supply chains.

For many organizations, understanding the full scope of the relationship between cyber risk and their third-party suppliers/vendors can be a blind spot. Yet it is critical. It's part of the reason, for example, that many cyber insurers have increased their requests for information about the vendor ecosystem as they seek to identify and underwrite critical dependencies beyond tier one suppliers/vendors.

- Auditing and verifying vendors and supply chains is the area that larger organizations are least likely to have addressed, although they have been fairly aggressive overall in taking cybersecurity actions.
- Smaller organizations are even less likely to have taken actions around supply chains.
- Financial services firms are ahead of other sectors in conducting vendor assessments.
- Most companies are taking actions to improve some "basic" areas such as the security of computers, devices, and systems.

Vendor and supply chain issues lagging among cybersecurity actions taken

Cybersecurity actions taken in the past 12 months



Building your enterprise's cyber risk team

Cyber risk management should be a shared responsibility in your enterprise. Risk managers, CFOs, CISOs, executive leaders and their teams should all be discussing key cyber risks and working together to identify, quantify, and manage them. The reality is often very different, with views of cyber risks and organizational strengths and weaknesses differing by function. This often leads to tunnel vision, where firms cannot get the big picture view necessary to identify and respond to cyber risks early enough to mitigate them.

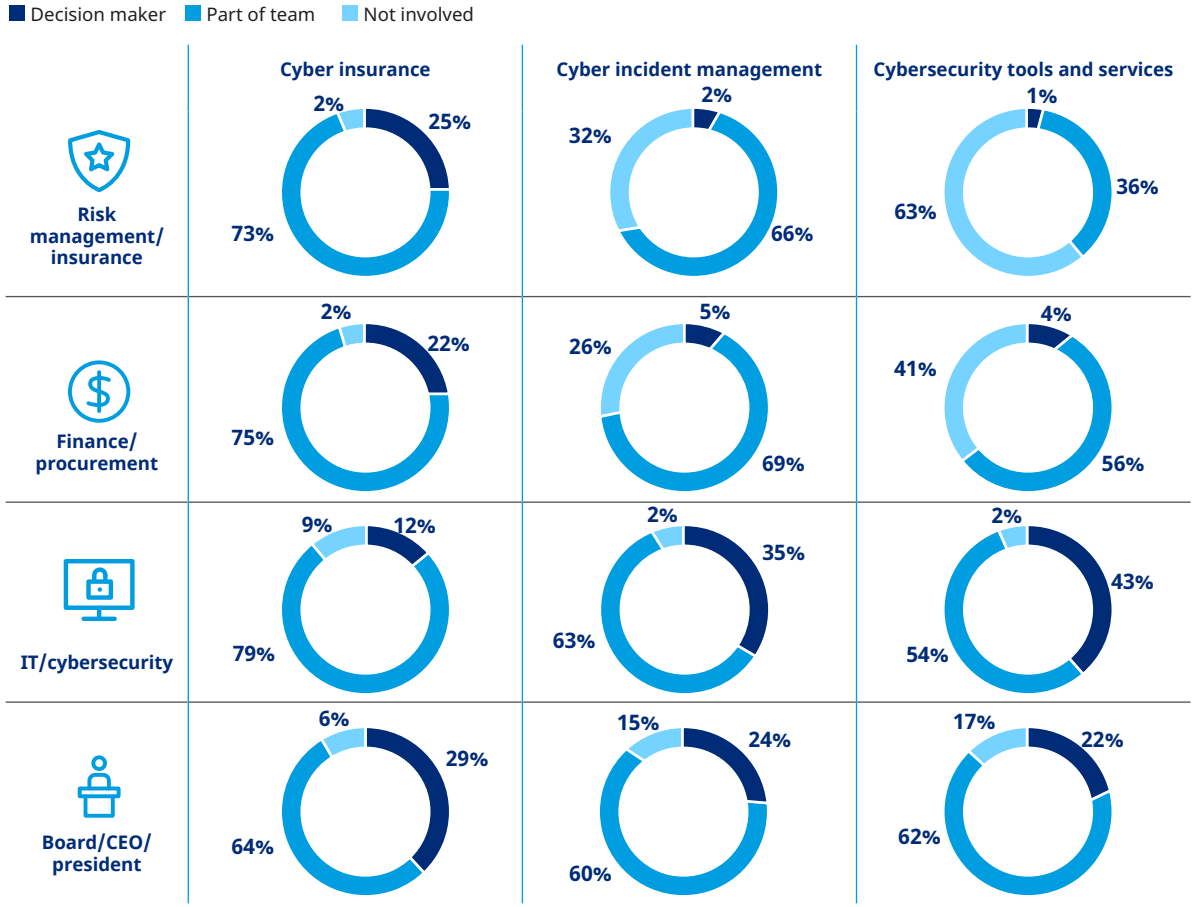
In this section, we'll look at information that can help you build better alliances across the enterprise — between CEOs, boards, and presidents; risk managers and insurance professionals; finance; and IT and cybersecurity. Achieving synergies will help reduce risk, lower costs, and build cyber resilience.

Understanding roles, responsibilities, and perspectives will strengthen cyber risk resilience.

How do professionals across an enterprise view their role in cyber insurance, cyber incident management, and cybersecurity tools and services? Do they consider their function to be the decision maker? To be part of the overall team, with inputs into the decisions? Or are they not at all involved?

- **IT/cybersecurity professionals** were the most involved across the board, according to our survey respondents. In more than 90% of responses, they were either the decision maker or part of the team in the three areas, and had the lowest level overall of "not involved." They were also the most likely to see themselves as the decision makers for cyber incident management and cybersecurity tools and services.
- **The board/CEO/president respondents** were most likely to see themselves as the ultimate decision makers on cyber insurance, with risk management and finance close behind.
- It's interesting that 90% of **risk manager respondents** said a cyber incident response plan existed, while only 60% of **executive level leaders** said so. Possibly, some of the low response among executives had more to do with a lack of engagement with those responsible for cyber risk management than a lack of an actual plan.
- Cyber insurance decisions show the highest level of respondents saying they are part of the team.
- Cybersecurity tools and services have the lowest levels of collaboration among professionals across the enterprise compared to other areas.

Level of involvement in cyber areas varies by role



Level of involvement in cyber areas varies by role

Quality of cyber incident response plan
(% rating each aspect “good” or “excellent”)

79%

of organizations have a response plan in place

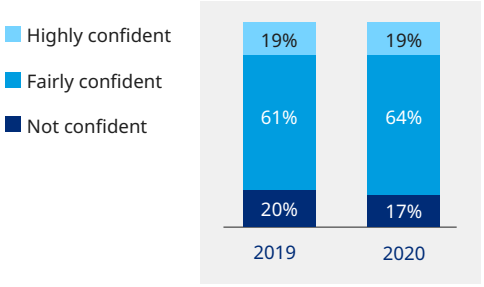
Confidence in cyber risk management strategies relatively low.

Confidence in one's organization's ability to assess, measure, mitigate, and respond to cyber threats remains low, with no substantial changes seen in survey responses from those gathered in the *2019 Marsh and Microsoft Cyber Survey* — only 19% of respondents indicated they are highly confident in their cyber risk management in both 2019 and 2022. Overall, executive leaders expressed the lowest level of confidence in these areas compared to departmental leaders. For example, regarding the organization's ability to manage and respond to cyberattacks, just 9% of executive leaders said they were highly confident, compared to 19% of departmental leaders. Such differing perceptions could well affect where resources are ultimately deployed as part of a cyber risk strategy.

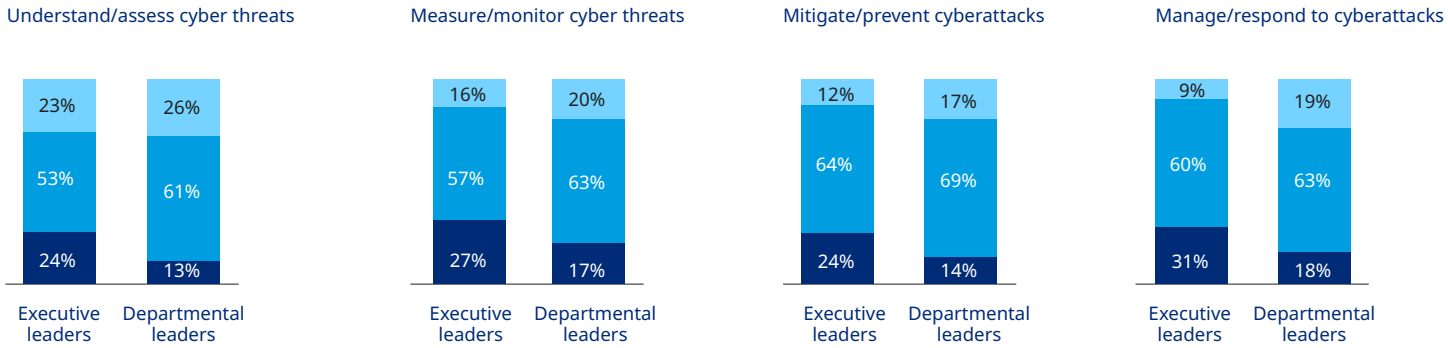
- Both the executive leaders and departmental leaders showed the highest confidence levels regarding organizations' ability to understand and assess cyber threats. This reflects the ever-increasing exposure to information about cyber risk experienced by most areas of society.
- The biggest gap in perception also related to the ability to manage and respond to cyberattacks, with nearly one-third of executive leaders saying they were not confident, compared to 18% of departmental leaders. More effective cross-enterprise communication holds the potential to bridge such gaps. As information is shared across functions, there may well be better alignment around the organization's abilities — and where to make investments.

Executive leaders most likely to lack confidence in cyber risk management programs

Overall confidence across cyber risk management



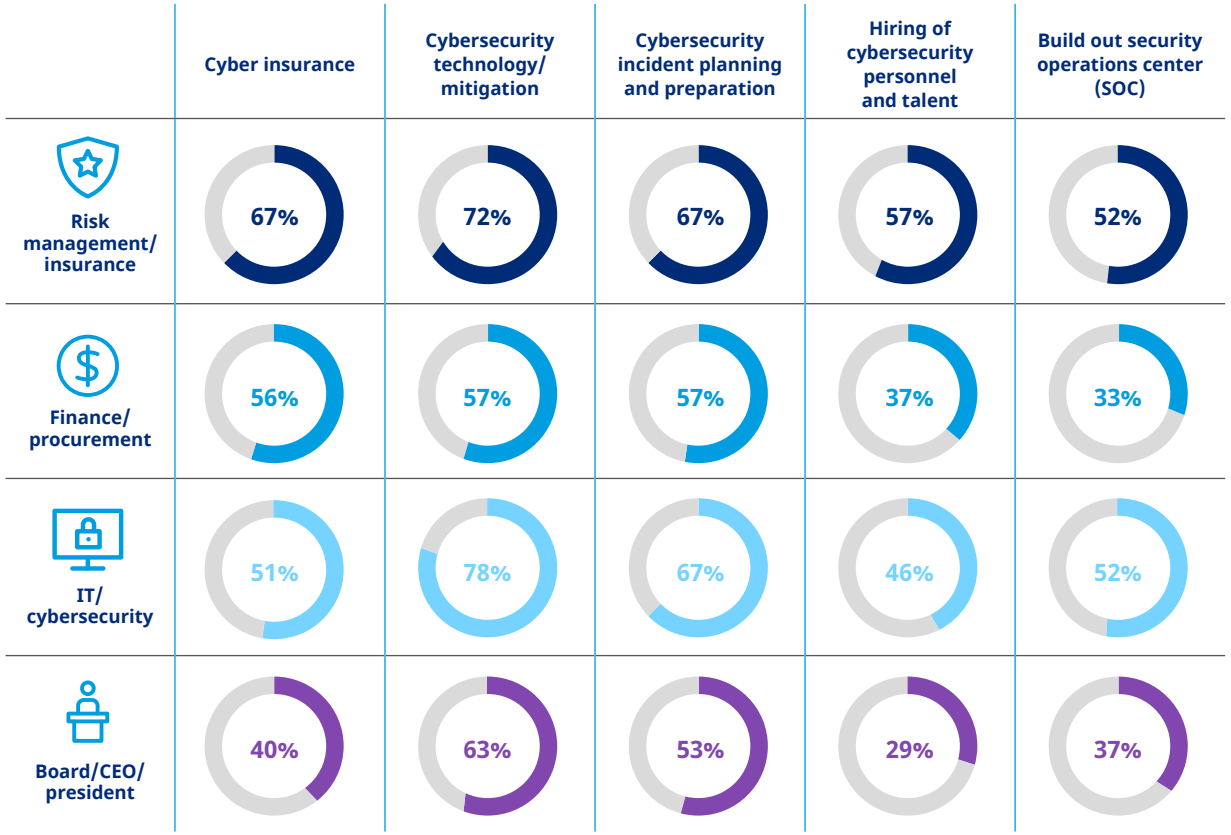
Confidence in organization's ability to...



Wide agreement across roles that cyber investments will increase in 2022

How do you expect your organization's investments to evolve in the next 12 months?

% Any increase



As cyber investments increase, cross-enterprise strategy is needed.

There was broad consensus among organizational roles on the need to increase investments in cyber risk management resources and capabilities, compared to 2019. Very few respondents expect investments will decrease, and more than half said some level of increase is likely in most areas. Like most budgetary decisions, deciding where to invest can be a complicated, time-consuming matter. Organizations that share their cyber risk expertise across the enterprise are likely to find the task more effective and efficient.

- Cyber risk leaders in different roles and departments can be expected to have varied plans and priorities for future investments. IT and cybersecurity respondents were more likely to plan increased spending on cybersecurity technology; those in finance and procurement roles less so.
- Risk management and insurance leaders were more likely to anticipate greater spending on cyber insurance and on hiring more cybersecurity professionals; those at the board and CEO level were significantly less likely. For example, 35% of risk management leaders expect to see increases of 25% or greater in insurance spending; just 9% of executive leaders expect that level of increase.
- Lack of relevant staff/talent was seen as one of the top barriers holding companies back from implementing more formal and rigorous risk assessment methods. At the same time, executive leaders were the least likely to foresee increased hiring of cybersecurity talent; just 29% expect any increase in this area, compared to 57% of risk managers and 46% of cybersecurity and IT leaders who expect it. Does this represent a miscommunication among the various functions and leaders? If it does, this is yet another area that would benefit from an enterprise-wide approach to cyber risk management.

Best practices for building enterprise-wide cyber risk management

A best practices approach to cyber risk management draws on an enterprise-wide commitment to share the responsibility. This includes investing and engaging in a broad, balanced, and continuously updated array of resources and activities to mitigate cyber risks and reinforce cyber resilience. Such items include, but are not limited to, cybersecurity technology and talent acquisition, incident response training, penetration testing, vendor/supply chain risk assessments, cyber insurance, and cyber risk advisory services.

In this section, we look at the eight trends identified earlier, focusing on what it means for cyber risk leaders to develop an enterprise-wide approach for each.

KEY TREND #1

Cyber–specific enterprise-wide goals should be aligned to building cyber resilience as every organization can expect a cyberattack.

Executive and departmental leaders

- Commit to ongoing, cross-functional communication regarding cyber risk threats, readiness, and strategy.
- Engage in cyber risk management planning, including regular exercise of plans.
- Be involved in post-incident reviews.

KEY TREND #2

Ransomware is the top cyber threat facing companies, but not the only one.

Executive leaders (board/CEO/president)

- Receive regular threat updates to bolster understanding of such risks as ransomware-as-a-service.
- Ask questions and provide guidance on the links between cyber risk and organizational growth strategy.
- Approve a response strategy that includes scenarios in which ransom will/will not be paid.
- Participate in annual cyber incident response plan testing.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- Regularly monitor, review, and share threat assessment updates from inside and outside the organization.
- Maintain a cyber incident response plan that is reviewed and tested annually.
- Engage in training exercises to help all stakeholders understand each other's roles and responsibilities and how to act in the event of an incident.

KEY TREND #3

Insurance is an important part of cyber risk management strategy, and influences the adoption of best practices and controls.

Executive leaders (board/CEO/presidents)

- Involve departmental leaders in discussions regarding how cyber risk finance fits into corporate growth strategy.
- Make decisions on allocating budget.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- Engage finance and risk management help to quantify cyber risks in financial terms and establish metrics regarding corporate risk tolerance.
- Assess risk finance needs across the enterprise.
- Acquire comprehensive cyber insurance coverage, such as technology errors and omissions, regulatory defense and penalties, physical damage to operational assets, network security liability, and others, as needs requires.
- Consider alternative risk finance, such as captives and parametric coverage.
- Risk management/insurance takes lead in communications with insurers and shares underwriter insights/requests with cybersecurity/IT, finance, executive leaders, and others.
- Risk managers should consider involving their CISO (or equivalent) in discussions with insurers.

KEY TREND #4

Adoption of more cybersecurity controls leads to higher cyber hygiene ratings.

Executive leaders (board/CEO/presidents)

- Adopt an organizational strategy that includes a cyber risk management mindset that includes development and maintenance of cyber hygiene among all of the organization's technology users.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- Adopt a risk management mindset that harnesses synergies among cyber risk management tools and tactics and reinforces a strong level of day-to-day cyber hygiene among all of the organization's technology users.
- Cybersecurity/IT takes lead in implementing a broad and balanced mix of cybersecurity technology tactics and controls, including email filtering and web security, endpoint detection and response, hardening techniques including remote desktop protocol mitigation, privileged access management.
- Risk management passes on to IT insights/requirements from insurers.

KEY TREND #5

Organizations lag in measuring cyber risk in financial terms, which hurts their ability to effectively communicate cyber threats across the enterprise.

Executive leaders (board/CEO/presidents)

- Request information putting potential costs of cyber risk in financial terms.
- Request regular updates regarding cyber risk appetite and tolerance.
- Incorporate those measures into setting business strategy priorities.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- Use quantitative approaches to assess and understand cyber risk exposures.
- Finance takes lead, requests information from other areas (operations, R&D, etc.) to help determine risk tolerance.

KEY TREND #6

Increased investment in cyber risk mitigation continues, though spending priorities vary across the enterprise.

Executive leaders (board/CEO/presidents)

- Synthesize inputs from across the company, ask questions, allocate budget.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- All areas input to finance and executive leaders regarding investment priorities.
- Risk management/insurance professionals provide input on investment priorities based in part on cyber insurer requirements/insights.

KEY TREND #7

New technologies need to be assessed and monitored on a continuous basis, not just during exploration and testing prior to adoption.

Executive leaders (board/CEO/presidents)

- Hold departments accountable for making sure there are no gaps in monitoring.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- When evaluating new technologies, technology leaders should work with cyber risk leaders in finance and procurement, and potentially engage external partners including insurers and cyber risk advisory services.
- Assess risks posed by new business technologies before and after implementation.
- Risk management and cybersecurity/IT work together towards a smooth transition from R&D to operations in the way cyber risk is deployed and monitored.

KEY TREND #8

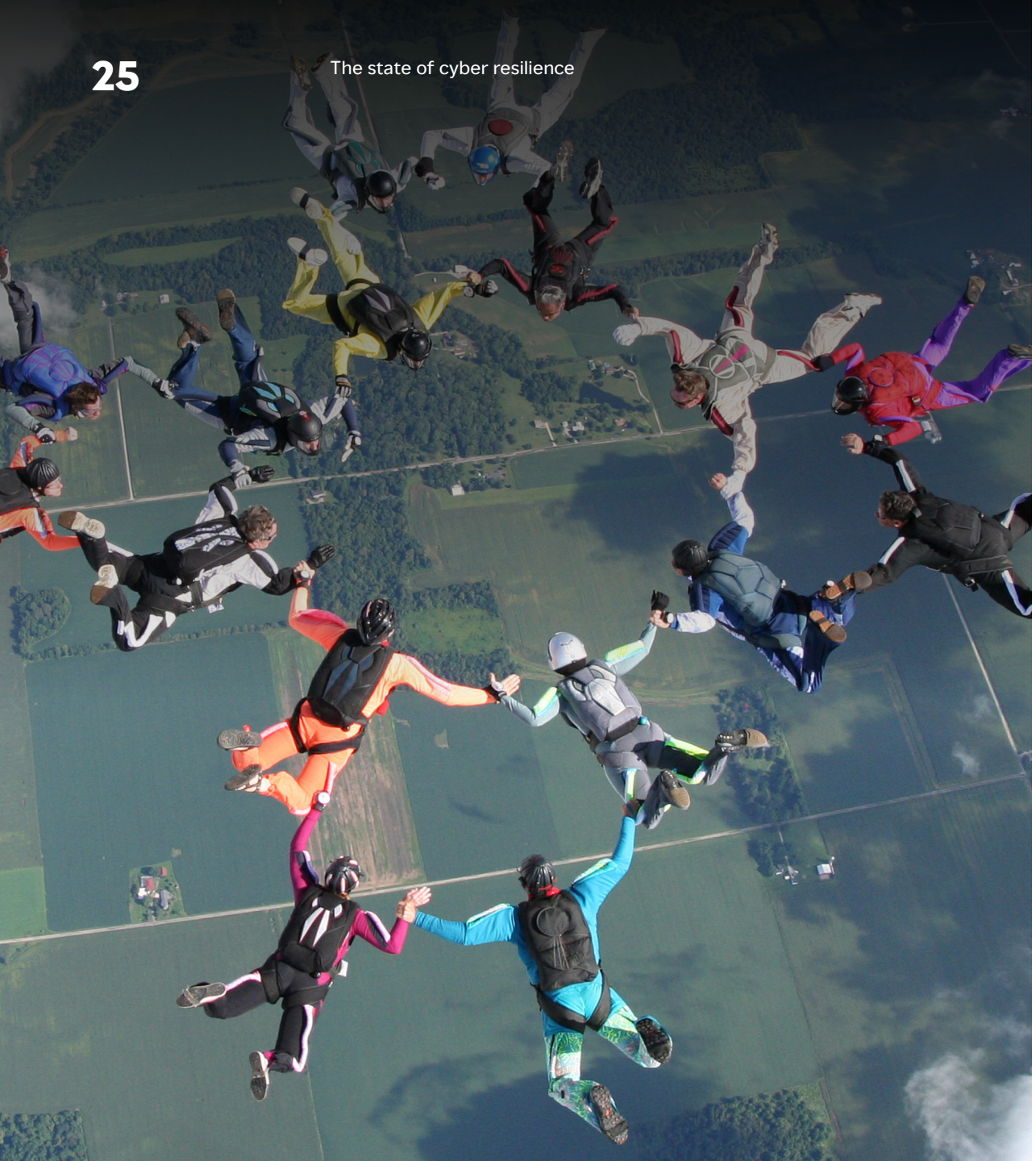
Firms take many cybersecurity actions, but widely overlook their vendors/digital supply chains.

Executive leaders (board/CEO/presidents)

- Thoroughly vet third-party suppliers and vendors from a cyber risk perspective.

Departmental leaders (risk management/insurance, finance/procurement, IT/cybersecurity)

- Assess vendors and supply chain partners, including audits of cybersecurity controls and protocols.
- Contracts with vendors and suppliers contain provisions related to cybersecurity posture.
- Work with legal, operations, procurement, and other departments, as appropriate, to audit and verify the technical and operational measures of suppliers.



Sharing responsibility builds cyber resilience confidence

There's no one-size-fits-all solution to the cyber risks facing organizations today. Cybersecurity measures, insurance, data and analytics, and incident response plans all play a role. However, a critical element to making these and other pieces work together is to develop an enterprise-wide alignment around cyber risk management, fostering a shared responsibility. All stakeholders — including risk managers, finance, cybersecurity/IT, executive leaders — will likely gain confidence in the organization's cybersecurity posture by being better connected to the broader enterprise.

Methodology

The research comprised a global online survey of n=662 cyber risk decision makers.
Surveys were administered in 16 languages and responses collected from 56 countries.
Survey fieldwork was conducted throughout November and December of 2021.
All respondents were sourced from the Marsh database and from online outreach by 7DOTS.

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.

About Marsh

Marsh is the world’s leading insurance broker and risk advisor. With around 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world’s leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on LinkedIn and Twitter or subscribe to BRINK.

1166 Avenue of the Americas, New York 10036