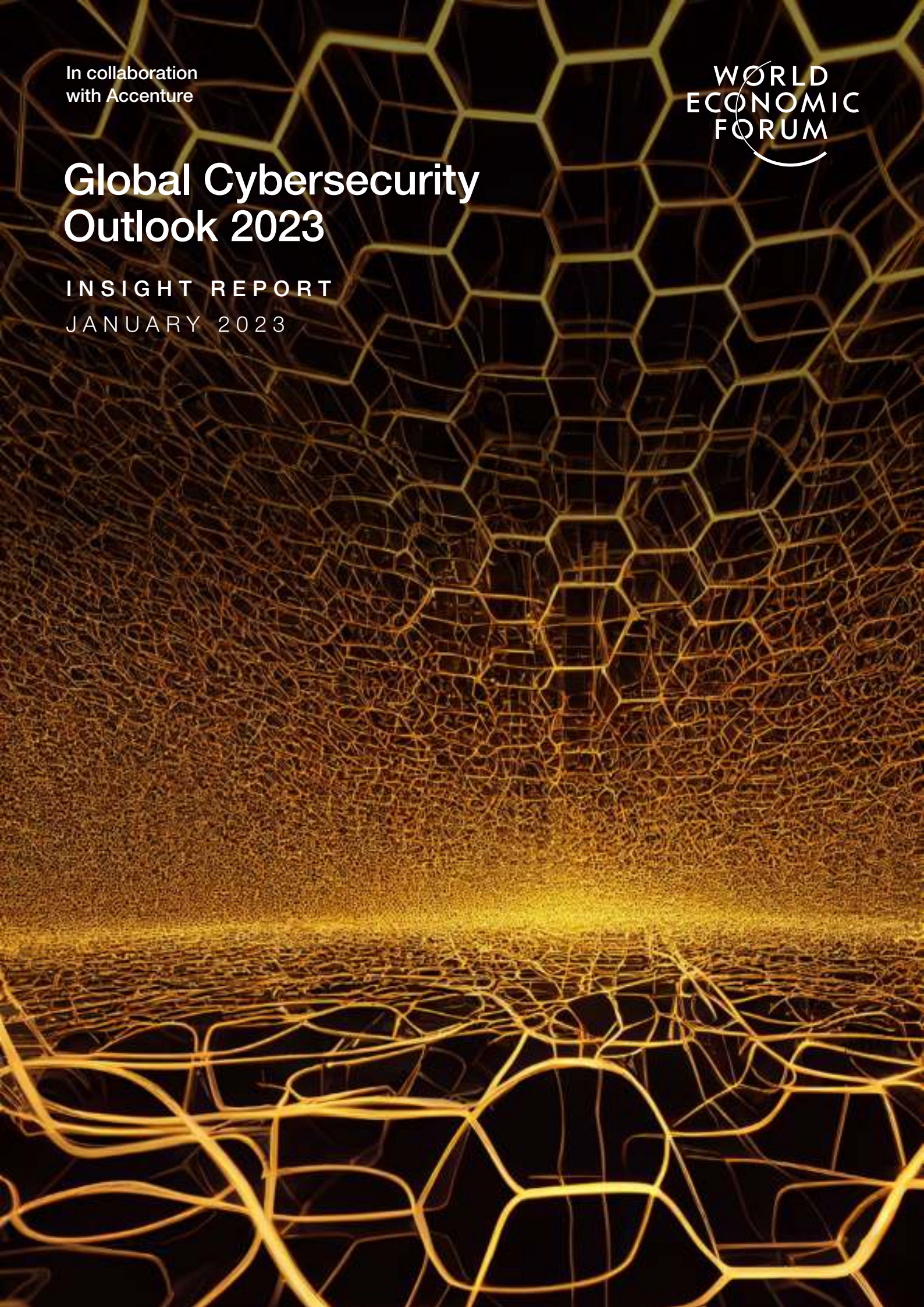
In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2023

INSIGHT REPORT

JANUARY 2023



Cover: Artwork created using artificial intelligence, prompt, art direction and refining by Studio Miko
Images: Getty Images

Contents

Foreword

Awareness and preparation will help organizations balance the value of new technology against the cyber risk that comes with it.

Paolo Dal Cin
Global Lead,
Accenture Security

Jeremy Jurgens
Managing Director,
World Economic Forum

Geopolitical instability, rapidly maturing and emerging technologies, lack of available talent, and increasing shareholder and regulatory expectations represent some of the significant challenges that concern cyber and business leaders. If the findings of last year's Global Cybersecurity Outlook reflected the lingering impact of the pandemic, and the effects of rapid digitalization, this year's Global Cybersecurity Outlook reveals concerns about an increasingly fragmented and unpredictable world.

Building cyber resilience, globally, has been one of the key priorities of the World Economic Forum's Centre for Cybersecurity since its inception. Inherent in that work is bridge-building – between the public and private sectors, and between cyber experts and business leaders. This year, when the Centre engaged its network of global cyber and business leaders to solicit their insights on emerging cyberthreats, we could see both how far we have come, and how far we have yet to go in helping translate cyber-risk issues into communication that C-suites and boards of directors can use effectively.

The outlook, however, need not seem bleak. There's hope for better understanding – and more effective action – in the future. The best leaders avail themselves of wide-ranging information and listen to all of their stakeholders, understand their role and impact, and exercise good judgement to achieve the optimum outcomes. These attributes are no less necessary in cybersecurity than they are in any other domain. In this edition of the Global Cybersecurity Outlook, we are pleased to see improvement in a crucial area – awareness of cyber-risk issues, at the executive level, has gone up. At the same time, this year's Global Cybersecurity Outlook report represents a challenge to leaders – to think more deeply about cybersecurity and listen more intently to cyber experts, and to each other, in order to ensure our shared resilience.

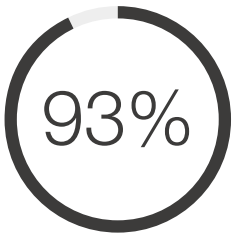
Executive summary

Hearing is not the same as listening. This aptly characterizes the relationship between cyber and business leaders in many organizations, according to research for the 2023 Global Cybersecurity Outlook study. The significance of cyber risk has certainly been heard in C-suites and boardrooms. Whether cyber leaders and business leaders understand each other well enough to meet this challenge is, on the other hand, an open question.

Overall, the study indicates that business leaders are more aware of their organizations' cyber issues than they were a year ago. They are also more willing to address those risks. Nonetheless, cyber leaders still struggle to clearly articulate the risk that cyber issues pose to their organizations in a language that their business counterparts fully understand and can act upon. As a result, agreeing on how best to address cyber risk remains a challenge for organizational leaders.

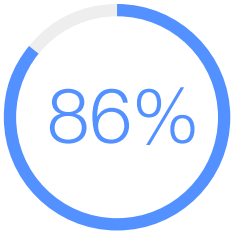
The 2023 Global Cybersecurity Outlook report presents the results from this year's study of cybersecurity and business leaders' perspectives on leading cyber issues and examines how they affect organizations around the world. Key findings include:

- The character of cyberthreats has changed. Respondents now believe that cyberattackers are more likely to focus on business disruption and reputational damage. These are the top two concerns among respondents.
- Global geopolitical instability has helped to close the perception gap between business and cyber leaders' views on the importance of cyber-risk management, with 91% of all respondents believing that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.
- Following from this, 43% of organizational leaders think it is likely that in the next two years, a cyberattack will materially affect their own organization. This, in turn, means that in many cases, enterprises are devoting more resources to day-to-day defences than strategic investment.
- The data protection and cybersecurity concerns created by geopolitical fragmentation are increasingly influencing how businesses operate and the countries in which they invest.
- Business executives acknowledge that their organization's cybersecurity risk is influenced by the quality of security across their supply chain of commercial partners and clients.
- Leaders intend to respond to these concerns by strengthening controls for third parties with access to their environments and/or data and re-evaluating which countries they do business in. However, business leaders are more likely to focus on in-house solutions for cyber-risk management, whereas security leaders place a higher priority on partnerships with other organizations.
- Many organizations are undertaking large digital transformation projects. Adding emerging technology to legacy IT increases the complexity of organizations' digital environments and therefore their cybersecurity risk. Leaders struggle to balance the value of new technology with the potential for increased cyber risk in their organizations.
- Cyber executives are now more likely to see data privacy laws and cybersecurity regulations as an effective tool for reducing cyber risks across a sector. This is a notable shift in perception from the 2022 Outlook report. Despite the challenges associated with compliance, cyber leaders acknowledged that regulation incentivizes much-needed action on cybersecurity.
- Structured interactions between cyber and business leaders are becoming more frequent – 56% of security leaders now meet monthly or more often with their board. This is rapidly narrowing the cybersecurity perception gap. However, more needs to be done to promote understanding between business and security teams to support effective action by organizational leaders.
- Building a security-focused culture requires a common language based on metrics that translate cybersecurity information into measurements that matter to board members and the wider business.
- Changes in organizational structure that embed cyber-risk discussions across a business can also promote more fluid communication and effective cyber-risk management.
- Ultimately, cyber leaders must present security issues in terms that board-level executives can understand and act on. Business leaders, for their part, need to accept more accountability for operational cyber requirements to advance their organizations' overall cyber capabilities.
- Cyber talent recruitment and retention continues to be a key challenge for managing cyber resilience. A broad solution to increase the supply of cyber professionals is to expand and promote inclusion and diversity efforts. In addition, understanding the broad spectrum of skills needed today can help organizations to expand their hiring pools. A number of promising initiatives are already in place, but these tend to focus on small cohorts. Time, thought and investment are needed to make cyber-skills development programmes scalable.



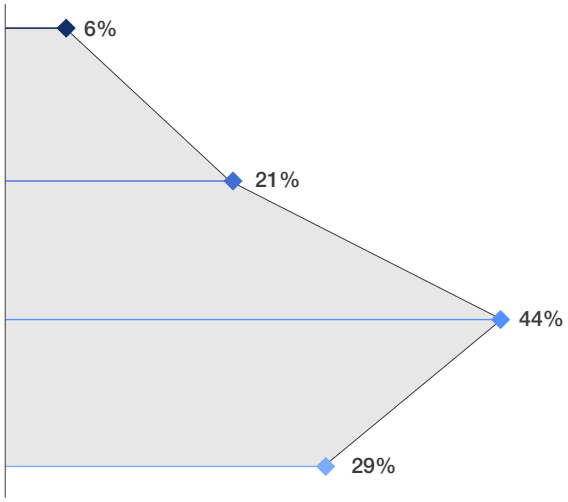
Cyber leaders

Business and cyber leaders believe global geopolitical instability is **moderately or very likely** to lead to a catastrophic cyber event in the next two years.

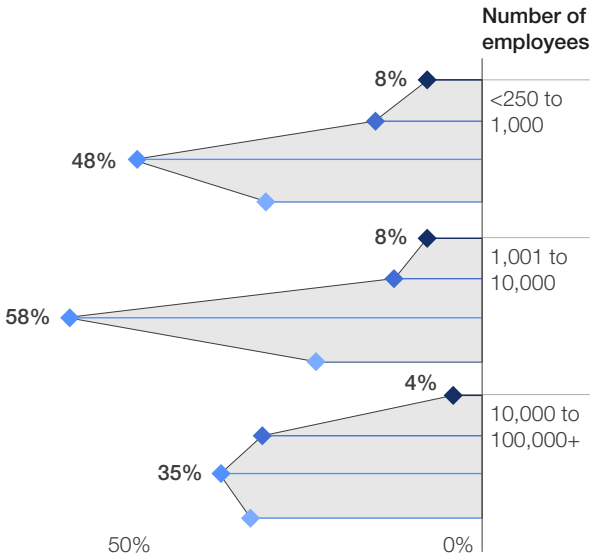


Business leaders

Do organizations expect geopolitical risks to affect their cybersecurity strategy?

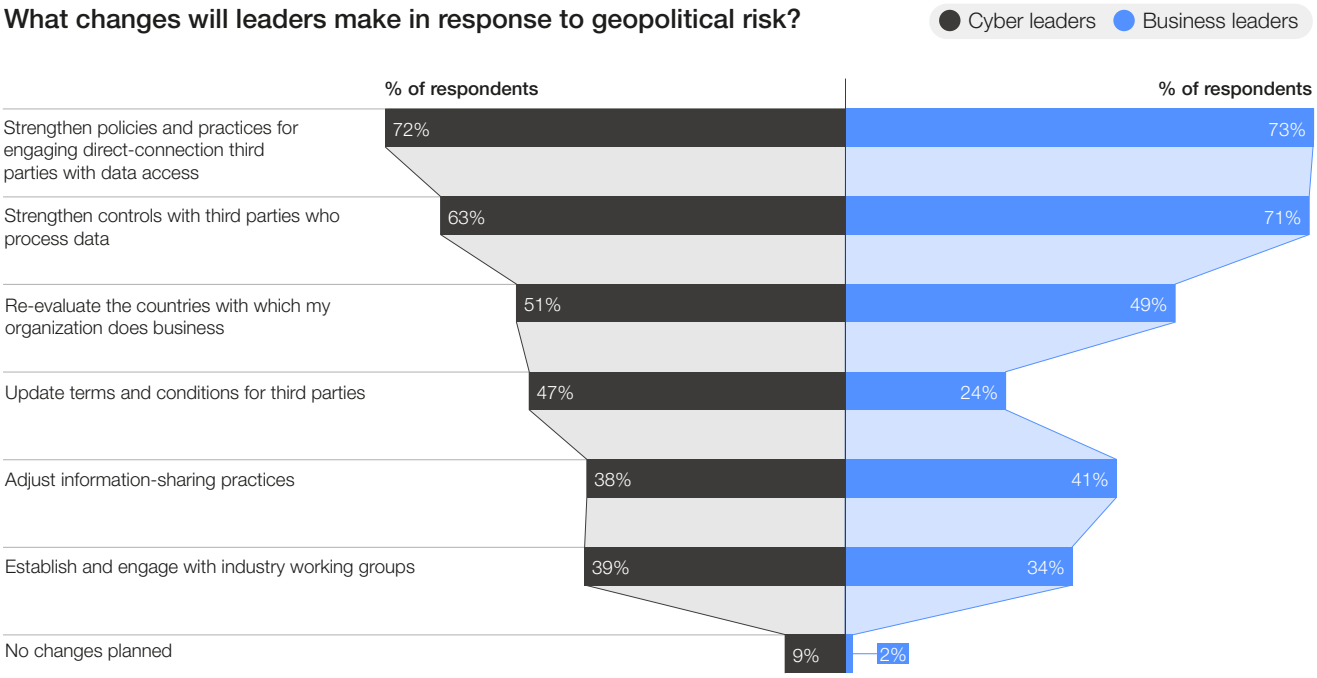


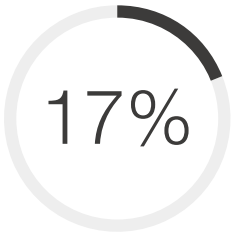
Do small and large enterprises have different expectations of geopolitical influence?



Not at all | Minimally | Moderately | Substantially

What changes will leaders make in response to geopolitical risk?





Cyber leaders

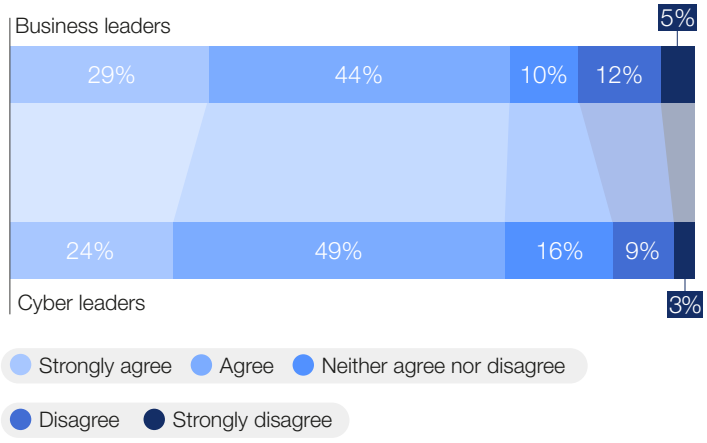
In comparison with cyber leaders, business leaders are substantially more likely to **strongly agree** that more sector-wide regulatory enforcement would increase cyber resilience.

Business leaders

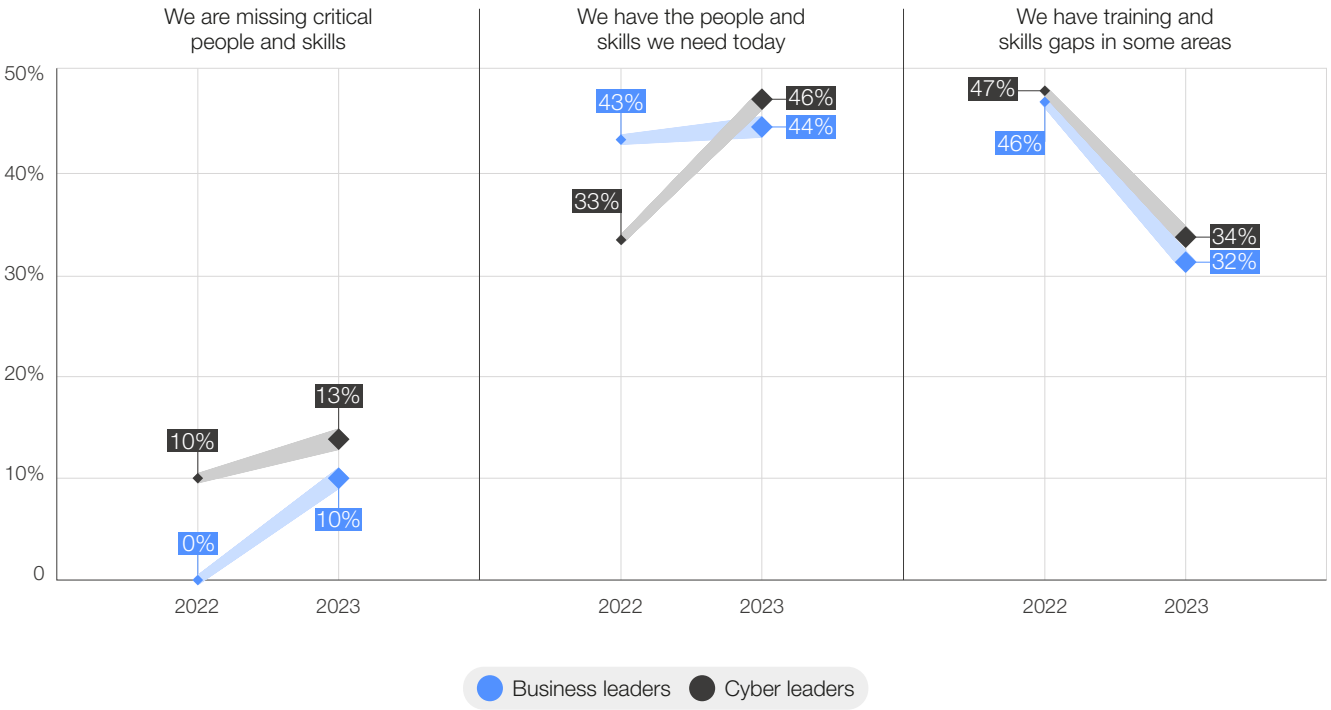
What will have the most positive influence on an organization's approach to cybersecurity in the next 12 months?

Business leaders' rank		Cyber leaders' rank
3	Increased use of cloud-based services	1
1	Increased employee awareness about cyberattacks	3
6	Digital transformation initiatives	2

Are cyber and privacy regulations effective in reducing an organization's cyber risks?



Compared to last year, business and cyber leaders are approaching consensus on the state of their organization's cybersecurity talent.



1 The global cyber landscape

Technologies are now shared across a multitude of organizations. These organizations consequently have common dependencies or weaknesses.

Although cyber leaders, business leaders and boards of directors are now communicating more directly and more often, they continue to speak different languages.

The impact of cybersecurity incidents can cascade from organization to organization and across borders. The risks this creates are potentially systemic, often contagious and frequently beyond the understanding or control of any single entity.[1]

Cybersecurity experts are themselves only beginning to grasp the extent and consequences of the technological interdependencies being created by their organizations' digital transformation. These changes range from the important but unexciting, such as increased dependence on shared IT services, to the more exotic, such as the creation of communication services on Earth that depend on "constellations" of software-enabled satellites in space.[2]

News headlines have drawn leadership attention to shifts in the cyber landscape. Most business leaders are now conscious that new technologies are evolving quickly and that cyberattackers will exploit this.

They understand that geopolitical tension is rising in most regions and that cyberattackers are changing their targets as a result. Cybersecurity regulations have become a more prominent factor in compliance and board-level conversations across many regions.

Although cyber leaders, business leaders and boards of directors are now communicating more directly and more often, they continue to speak different languages. News about cyber incidents have often dominated the conversation, rather than discussions about why those incidents mattered to an executive's organization and how precisely businesses could help their cyber leaders manage their responses.

In many organizations, questions about the most recent cyber news continue to drown out conversations on the most important initiatives and investments needed to meaningfully reduce cyber risk.

1.1 Geopolitics

This year's Outlook report reveals that 93% of cyber leaders and 86% of business leaders think it is "moderately likely" or "very likely" that global geopolitical instability will lead to a far-reaching, catastrophic cyber event in the next two years.

Similarly, 74% of organization leaders say that global geopolitical instability has influenced their cyber strategy "moderately" or "substantially". Business continuity (67%) and reputational damage (65%) concern organization leaders more than any other cyber risk. Leaders intend to respond to these concerns by strengthening controls for third parties with access to their environments and/or data (73% and 66% respectively) and re-evaluating the countries with which they do business (50%).

FIGURE 3 **How likely is it that geopolitical instability will lead to a far-reaching, catastrophic cyber event in the next two years?**

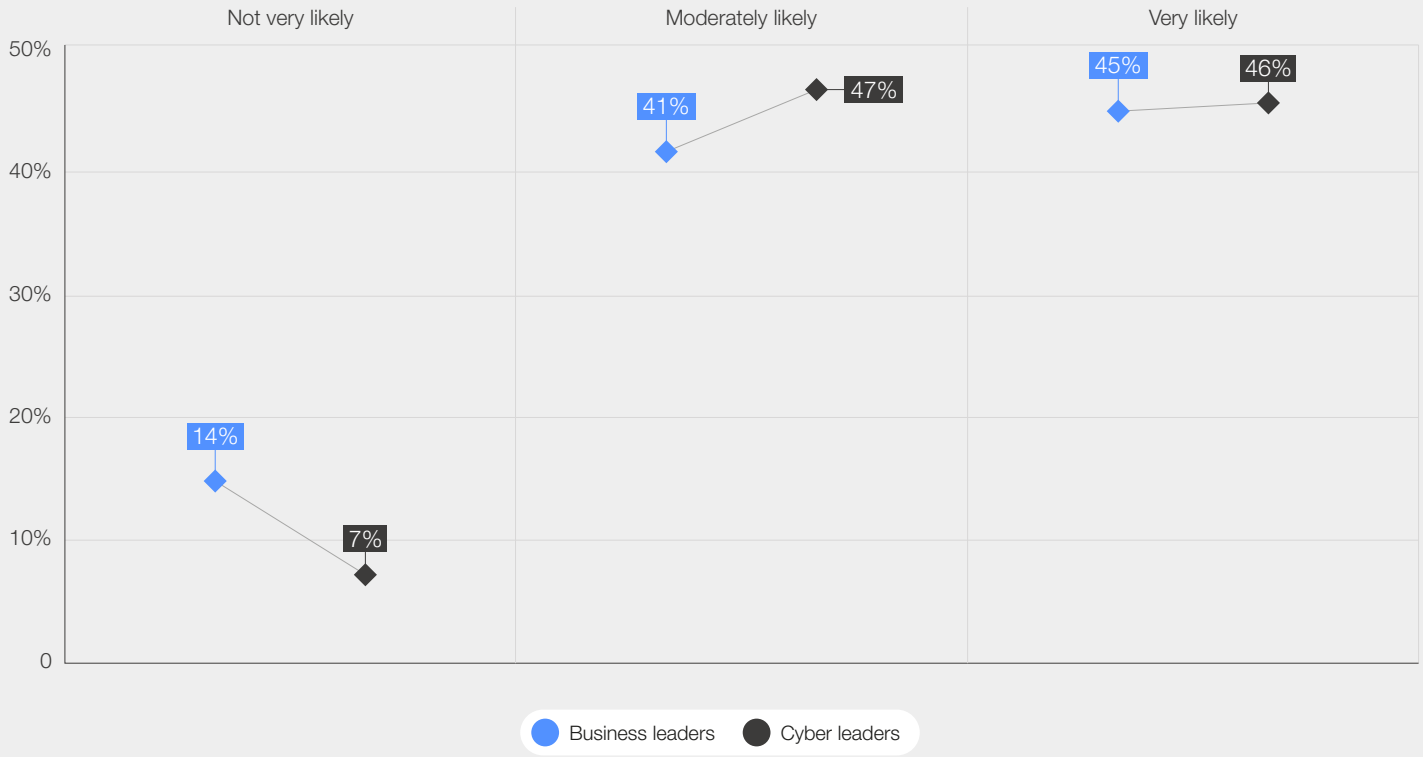
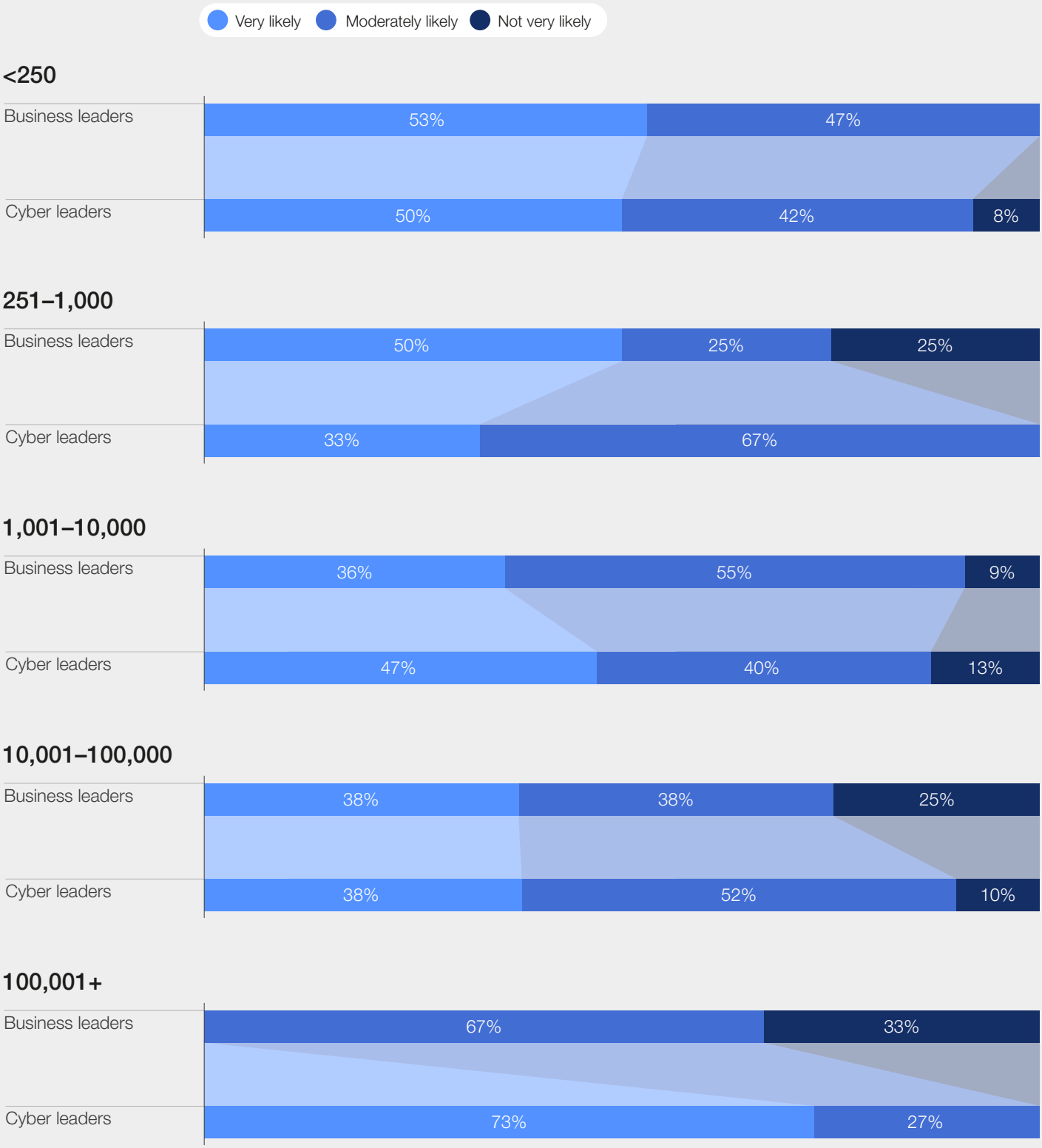


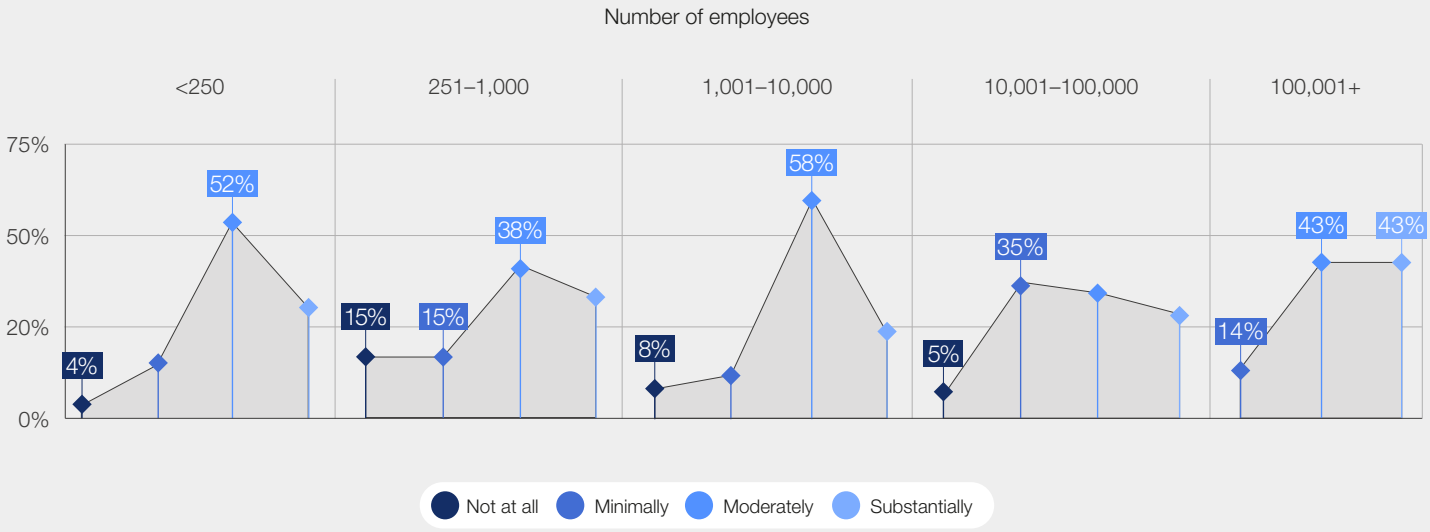
FIGURE 4 | **Likelihood of geopolitical instability leading to a far-reaching cyber event in the next two years (by number of employees per organization)**



Cyber leaders, business leaders and board members have a nearly equal understanding of cyber risks related to geopolitical instability, more so than with any other source of cyber risk. The tangible and immediate nature of the effects and pervasive news coverage make it easier for all three groups to fully appreciate these risks.

Business leaders are often adept at adapting their organizations to new political realities. This makes geopolitical risk an entry point for the wider conversation between security leaders and business leaders on how cyberthreats are changing and how cyber risk can affect their organization's business continuity planning.

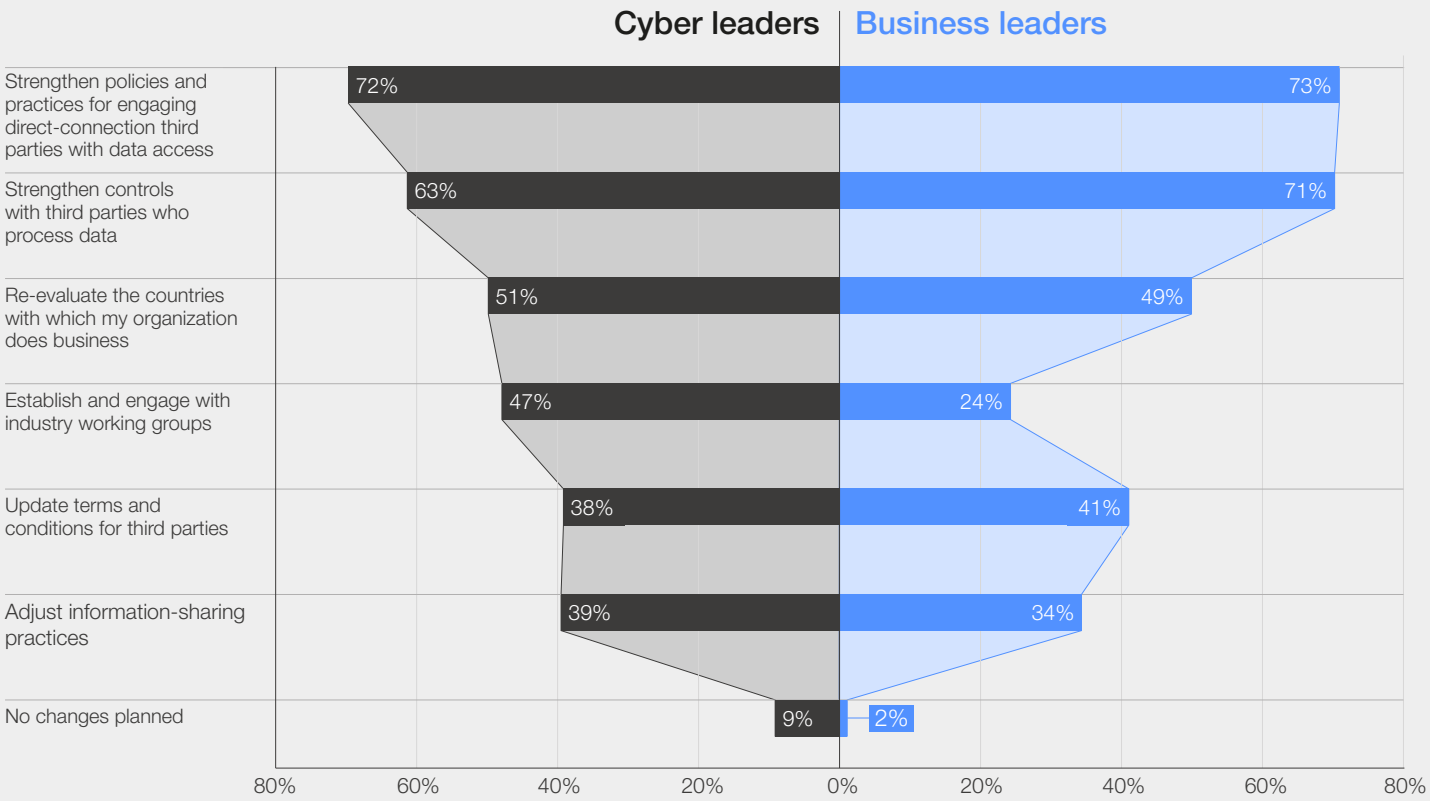
FIGURE 5 | **Geopolitical risk is influencing cybersecurity strategies across all sizes of business surveyed**



Most respondents, across all sizes of organizations, stated that geopolitical instability had influenced their cybersecurity strategy. Respondents who reported successful changes in their cybersecurity strategy also said they had organizational structures in place that supported interaction among cyber leaders, business leaders across functions and boards of directors. These structures encouraged collaboration on digital resilience across business activities.

Separate research undertaken for the World Economic Forum's Earning Digital Trust initiative in 2022 suggests that building trustworthy technology – by focusing on the interplay between cybersecurity, privacy, ethics and transparency, with the aim of protecting all stakeholders' interests and upholding societal expectations – can aid in this cross-organizational cooperation.[3]

FIGURE 6 | **How geopolitical risk has influenced my organization's cybersecurity strategy**



The geopolitical events of the past year have significantly influenced cyber strategy and tactical cybersecurity operations across the globe. Efforts are being made to strengthen internal policies and processes as well as to increase the effectiveness of cybersecurity controls with third parties. This suggests that organizational responses to cyber risk being undertaken now will have a positive long-term impact.

At the same time, geopolitical tensions might be responsible for a greater volatility in the character of cyberthreats, with more variation in the types of widely available malware, as well as changes in the type of assets or value-creating processes that cyberattackers target.

This volatility has made it increasingly difficult to think strategically about the operational elements of an organization's internal cybersecurity practices. As noted by one respondent interviewed for this report: "Geopolitics arising from the Russia-Ukraine war have also altered how we think about our threat environment. We have needed to spend time and resources on understanding how the threat landscape has changed, whether the difference in the attacker's motivation makes us more likely to be targeted, what will be attacked and how it might be attacked. We are now using more resources for active monitoring of the threat picture compared to 12 months ago. We focus on our tactical and short-term (three-month) planning and become less detailed in our three- to 12-month planning as the environment is so volatile."[4]

FIGURE 7 **Regional breakdown of how geopolitical risk influences cybersecurity strategy**

	AMR[1]	APAC[2]	EMEA[3]
Adjust information-sharing practices	42%	25%	33%
Establish and engage with industry working groups	43%	13%	38%
No changes planned	9%	13%	2%
Re-evaluate the countries with which my organization does business	52%	63%	45%
Strengthen controls with third parties who process data	63%	88%	67%
Strengthen policies and practices for engaging direct-connection third parties with data access	67%	88%	79%
Update terms and conditions for third parties	46%	13%	33%

2% 88%

Note: 1. AMR = Region of the Americas; 2. APAC = Asia-Pacific; 3. EMEA = Europe, the Middle East and Africa.

1.2 Emerging technology

Business and cyber leaders are most closely aligned in their perspectives on emerging technology.

Most organizational leaders appreciate that several fields of emerging technology, such as the use of machine learning, are being implemented at speed, used across a widening range of processes and will affect their organization's cyber-risk profile.

Respondents said that artificial intelligence (AI) and machine learning (20%), greater adoption of cloud technology (19%) and advances in user identity and access management (15%) will have the greatest influence on their cyber risk strategies over the next two years.

However, respondents did not rank other categories of emerging technology significantly lower than the top three. This suggests that the implementation of new technologies will be undertaken in combination, significantly increasing the complexity of an organization's digital environment and highlighting the need to embed cyber-risk management through all stages of a digital transformation process.

Organizations must balance the value of new technology and the potential cyber exposure that comes with it to effectively manage their risk in the coming years.

1.3 Emerging threats

> **More resources are being thrown at cybercrime campaigns by criminal groups. There's a sense that cybercrime is converging with nation-state actors and that this is leading to a higher number of new campaigns being launched as well as attacks that are more clearly tailored to the target organization.**
>
> **The greater the volatility in the threat, the more time is being spent on tactical defence by CISOs and their teams. It's important to create the space for strategic development and effective risk management.**
>
> Derek Manky, Chief Security Strategist and Vice-President, Global Threat Intelligence, Fortinet.

Cyberattackers come in many forms and with different motivations. In cybersecurity terminology, these disparate groups are often bundled together using the term "threat actors". In 2022, malicious threat actors adapted quickly to exploit changes in the political, technological and regulatory landscapes.

In cybersecurity, attackers have a structural advantage: they need to find only one exploitable weakness across an organization. This means attackers have less ground to cover than a defender and the attacker can often adapt faster than organizations can defend or recover.

The threat landscape has become increasingly volatile. Professionalized cybercriminal groups have continued to grow and create a higher volume of new attack types. Volatility is not only risky; the time it takes to develop a response creates an opportunity cost for an organization's cybersecurity experts. Cybersecurity teams sometimes feel forced to ignore strategically important activities to address immediate tactical issues.

In interviews, security leaders shared the belief that the variety of attacks has increased significantly since last year, and that the impacts are systemic rather than isolated in one target or sector. The findings for this report indicate that a series of major global cyber incidents in 2021–2022, such as the exploitation of the widespread Log4j vulnerability[5] forced many organizations to focus on monitoring and assessing threat information. Threat data, when viewed from the perspective of an individual organization, contains a lot of "noise" and it can take a great deal of time to identify which threats matter to an organization and what the possible impact might be on operations. Further, several leaders indicated that their monitoring and assessment cycles shortened drastically from annually to quarterly, frequently diverting, and heavily taxing, their cyber resources.

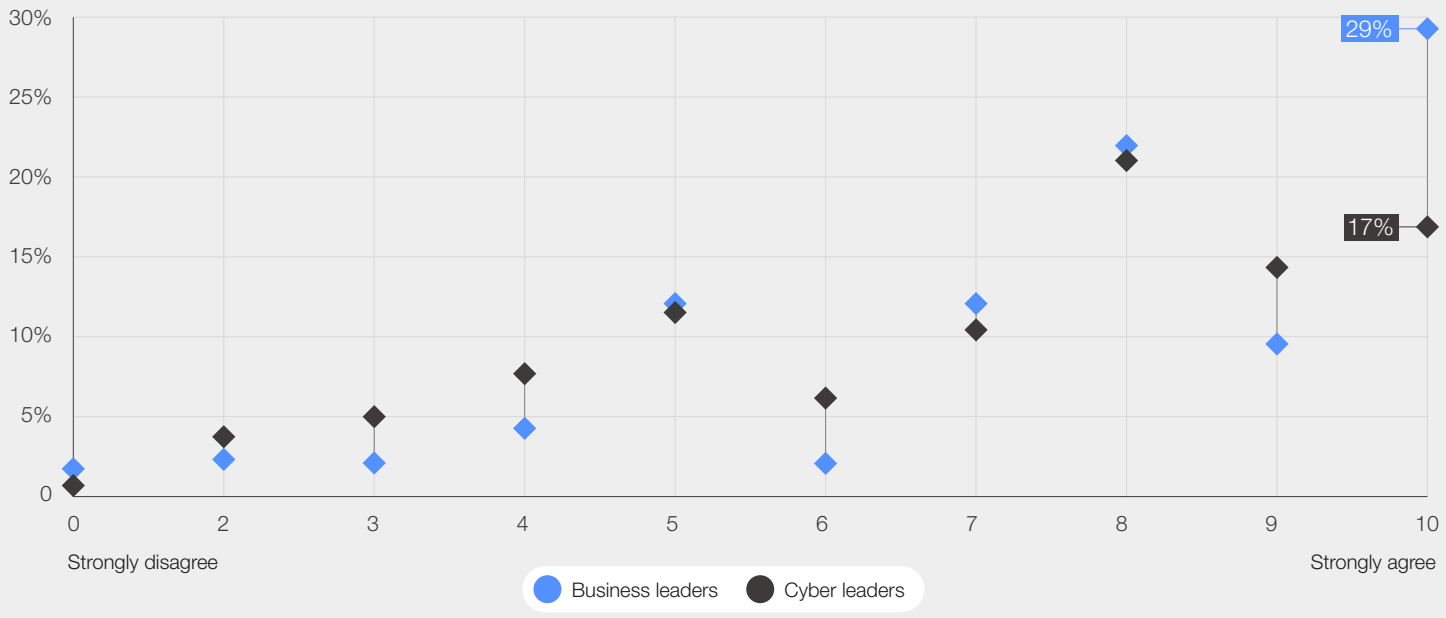
Interview and workshop findings indicate that organizations which embed cyber-risk management across multiple parts of their activities, such as risk management, business continuity planning, finance, product development etc., find it easier to create the space needed to develop strategic responses to changes in the threat environment in order to better protect their assets and make their organization more resilient to cyberattacks when they occur.

1.4 Laws and regulations

> **The way we build regulations for cybersecurity is centralized. The regulations this system creates are valuable, but the process takes time. It can take two years for a regulation to be developed. Standardization can take 18 months. A cyberattack takes seconds. The speed at which emerging technologies are implemented often outpaces our ability to build security measures around them. We need to go beyond simple compliance with regulations if organizations are to be cyber resilient.**
>
> Hoda Al Khzaimi, Director, Center for Cybersecurity, New York University (NYU), Abu Dhabi; Founder and Director, (EMARATSEC) Center for Emerging Technology and Advanced Research in Cyber Security, AI and Cryptology, NYU

The 2023 Outlook shows a significant shift in the perception of how regulations affect cyber risk. In the 2022 report, more than half of respondents did not agree that cyber and privacy regulations are effective in reducing their organizations' cyber risks. This year's outlook indicates that 73% of respondents agree with the same statement.

FIGURE 8 **Having more effective enforcement of regulatory requirements across my sector would increase my organization's cyber resilience**



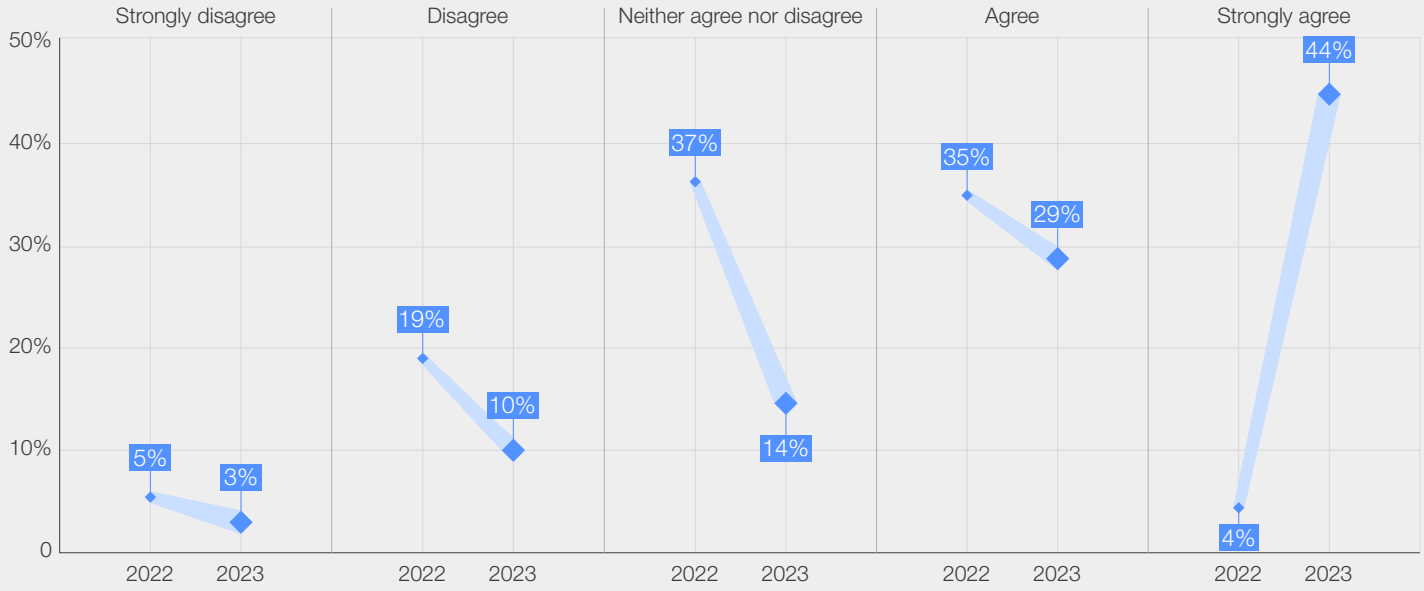
This is a notable shift in perception of the effectiveness of cybersecurity and privacy regulations. Some elements of cybersecurity regulations, particularly for organizations operating in more than one country, remain duplicative and can move resources from core cybersecurity work towards activities that aim primarily to demonstrate compliance rather than to keep an organization secure.

These compliance challenges remain; however, in the context of mitigating a large-scale cybersecurity event, regulations are increasingly seen as an effective measure for moving private-sector resources towards cybersecurity and resilience activities.

A large increase in cyber incidents, related fines, investigations and engagements between policy-makers and the private sector has elevated the perception of regulations as a critical influence on organizations' cyber resilience.

Business and cyber leaders also support effective enforcement of regulatory requirements: 76% of business leaders and 70% of cyber leaders agreed that further enforcement would lead to an increase in their organizations' cyber resilience. This is not to suggest that organizations are actively requesting more regulatory scrutiny of their own activities, but, rather, that they believe properly enforced regulations will raise the quality of cybersecurity across their sector and their supply chains, which will in turn make their business less prone to collateral damage from attacks on other organizations.

FIGURE 9 **Cyber and privacy regulations are effective in reducing my organization's cyber risk (year-on-year change in responses to the question, 2022–2023 reports)**



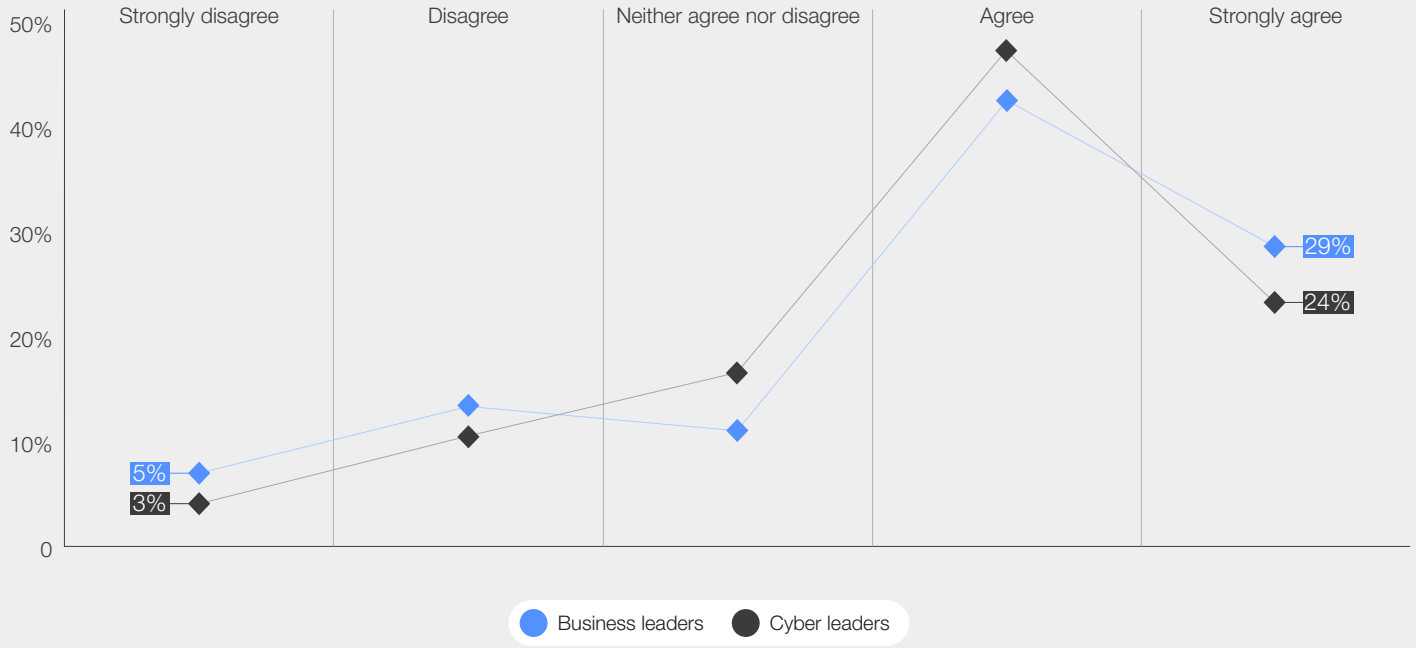
Note: The graph covers responses from both business and cyber leaders.

One leader put it this way: "Public statements by government as well as regulation help boards understand the need to assign resources."[6]

All leaders still anticipate challenges with applying a set of continuously expanding and changing regulations. As an interviewee said, "Regulation incentivizes action on cybersecurity but doesn't directly lead to resilience within an organization."[7]

Boards' and business leaders' awareness of the demand for cyber resources within their organizations is increasing. With regards to regulations, business leaders might fear hefty fines more than they value – and truly understand – the contribution regulations make to collaborative cyber policies. Nonetheless, regulations are something to which boards actively respond and are a valuable starting point for embedding cyber-resilience techniques across an organization.

FIGURE 10 **Cyber and privacy regulations are effective in reducing my organization's cyber risk**



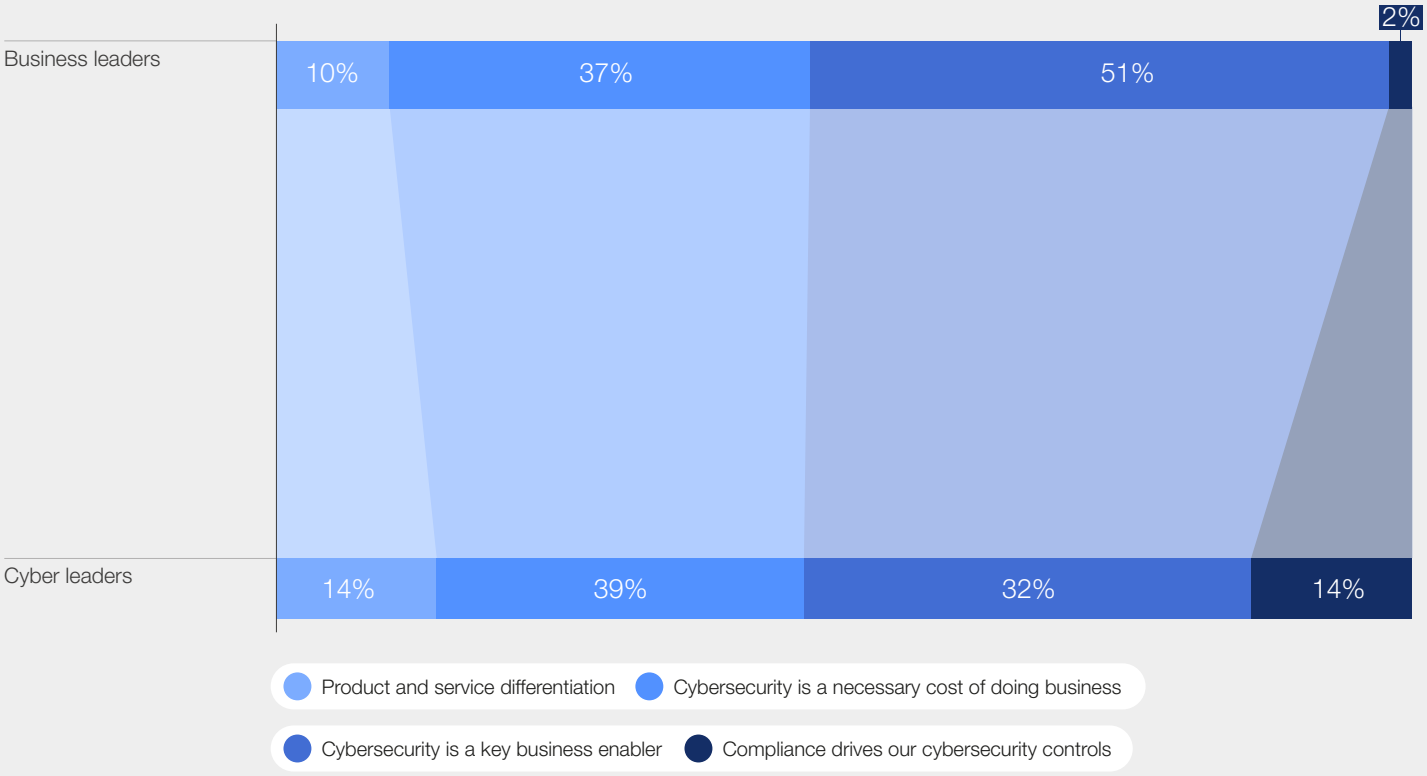
2 Leadership perception changes

Business and security leaders' perspectives on the importance of cyber-risk management are converging.

More than 39% of organization leaders agree that “cybersecurity is a key business enabler”. Interestingly, however, when broken down further, this equates to 51% of business leaders and 32% of security leaders giving an affirmative answer.

This indicates that perhaps business leaders have leapfrogged security leaders in championing the importance of cybersecurity or it could reflect a lingering perception gap worthy of further research.

FIGURE 11 **Leadership views on cybersecurity**



Note: The question asked “Which of the following describes your organization’s views of cybersecurity?”.

2.1 Prioritizing cyber risk in business decisions

> **More and more corporate boards now have true cyber experts among their members. It helps when people at board level are sufficiently cyber-literate to ask pertinent questions of their security teams but also to bring cyber into strategic business discussions. Boards also need to understand what a cyber event means for their organization. Too many business leaders still underestimate the impact a cyberattack can have on their operations, on their reputation and on their company as a whole.**
>
> Maya Bundt, Director, Bâloise Holding; Board member, Swiss Risk Association; Member of the World Economic Forum’s Global Future Council on Cybersecurity

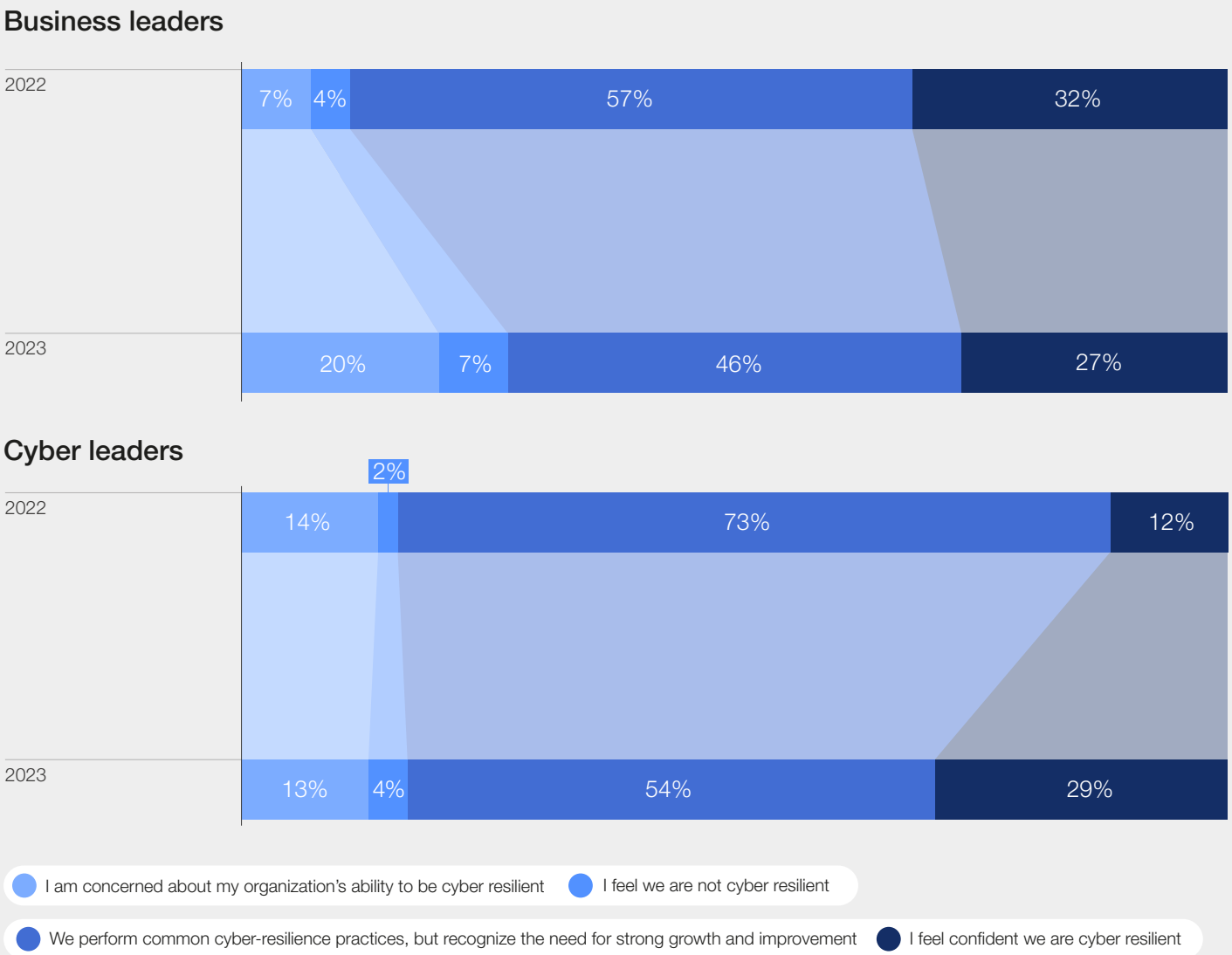
The 2022 Global Cybersecurity Outlook report highlighted a clear disparity in how business executives and cyber executives described the integration of cyber resilience into enterprise risk-management strategies.

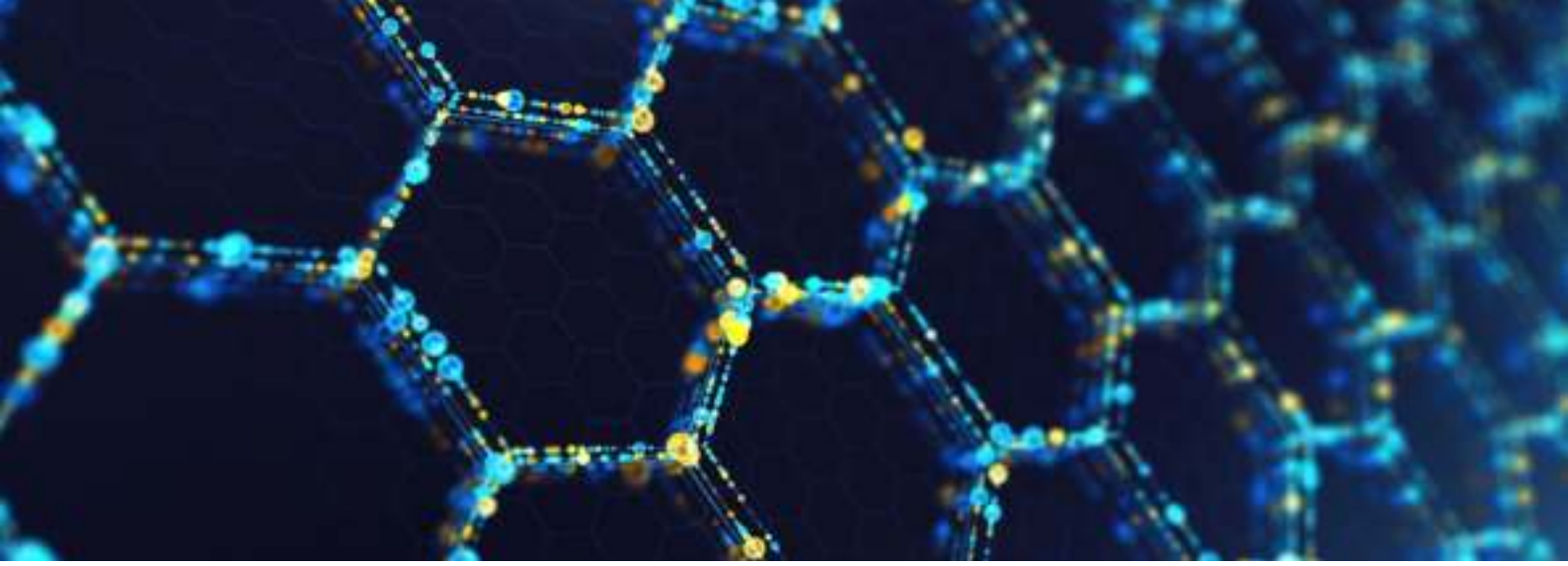
The 2023 survey findings illustrate a narrowing of that perception gap, with 95% of business executives and 93% (up from 75% in the 2022 edition) of cyber executives agreeing that cyber resilience is integrated into their organization’s enterprise risk-management strategies.

In addition, most business and cyber leaders also agree that incorporating cyber-resilience governance into their business strategy is one of the most impactful principles when it comes to cyber resilience.

FIGURE 12 | **Cyber resilience in my organization is integrated into enterprise risk management strategies**

FIGURE 13 | **How do you feel about your organization's ability to be cyber resilient?**





Not only is there a shift in leaders' perception of their priorities, but there is a shift in reported behaviours among cyber leaders. More than half (56%) of cyber leaders meet with business leaders monthly, or more frequently, to discuss cyber-focused topics.

More frequent communication means more opportunities to align on cybersecurity priorities. Perhaps as a corollary, organizational leaders who meet more often are more confident in their organization's cyber resilience than those who meet less frequently.

Of respondents who meet at least monthly, 36% are confident that their organization is cyber resilient. Only 8% of those respondents report that their organizations either are not cyber resilient or that they are concerned about their organization's ability to be cyber resilient.

Meeting frequently is one of many ways to boost the priority given to cyber risk in business decisions. A common theme in workshops and interviews was an increasing trend for chief information security officers (CISOs) to report directly to the chief executive officer.

One interviewee noted, "I think business executives really need to think about organizational design. In certain cases, CISOs are still reporting to CIOs [chief information officers]. That's sometimes an inherent conflict of interest," because chief information officers, when budgeting, might deprioritize security in favour of more functionality.

That noted, discussions with Forum partners at CIO level indicate that CIOs whose organizations have suffered a severe or sophisticated cyberattack are very likely to prioritize security after this experience. This suggests that board culture and executives' familiarity with cyber risk are also important.

Overall, it is a case of creating the right incentives regardless of the reporting line. Another interviewee stated, "You have a business-unit executive who has to trade-off functionality and security. They have limited budget and they get no credit for security."

Dealing with these conflicts is fundamentally a task for executive leadership, and a strategic question for corporate boards of directors. Ultimately, cyber resilience will require the adoption of better governance practices – including those developed by the World Economic Forum, the National Association of Corporate Directors (USA) and the Internet Security Alliance in their 2021 Principles for Board Governance of Cyber Risk.[8]

36%
are confident that their organization is cyber resilient.

Supply-chain risk

In the 2022 edition of this report, 39% of respondent organizations had been affected by a third-party cyber incident. To put it another way, they were "collateral damage" after their operations were disrupted by cyberattacks on companies from whom they bought or to whom they sold services.[9]

Third-party organizations that have direct connections with an organization or that process organizational data are a primary concern to all surveyed organizational leaders. Some 90% of respondents are concerned about the cyber resilience of such third parties.

Supply-chain risk is an indicator of the risk that is shared across a particular sector, sectors or countries and it is something that regularly affects important everyday services.

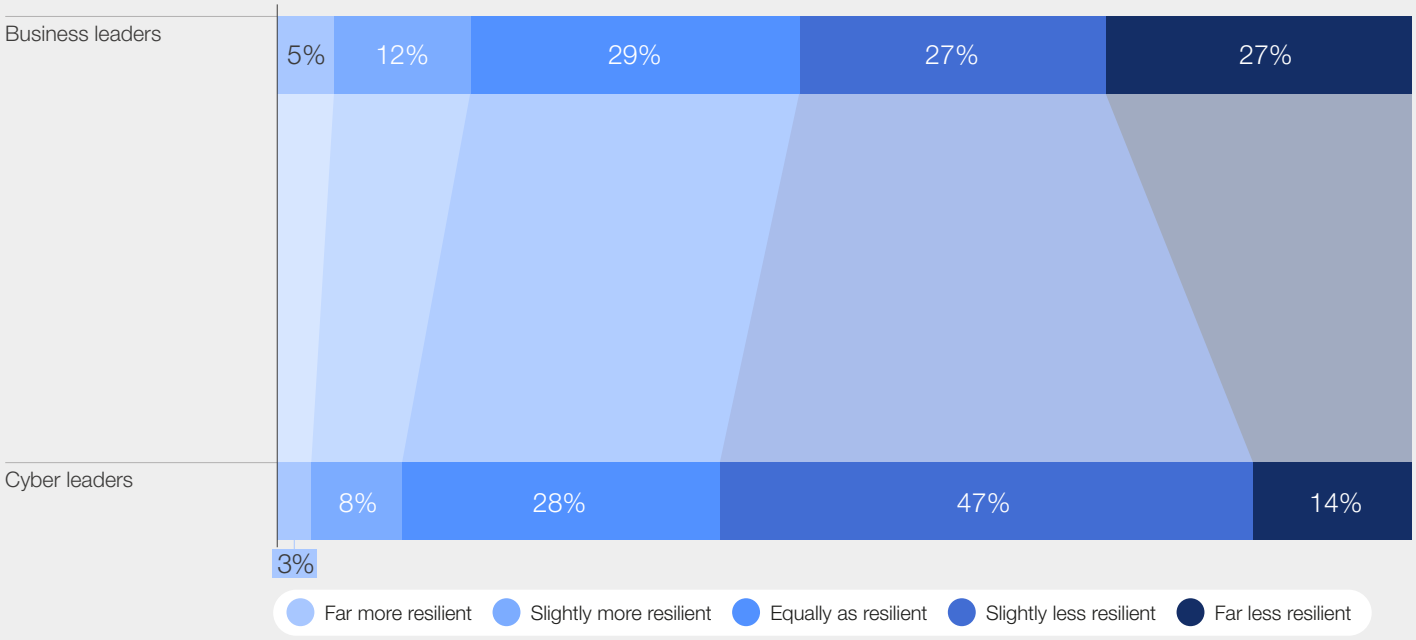
For example, in February 2022, a cyberattack on commercial satellite services in Ukraine caused electricity-generating wind farms to shut down across central Europe.[10] In July 2021, supermarkets in Sweden were forced to close their doors after a cyberattack on IT services provider Kaseya, based in Florida, USA.[11]

In both cases, the rolling flow of disruption across sectors was the result of a dependency on another organization's services and the outcome of a service breakdown was unpredictable.

These incidents show how the technologies that support businesses, infrastructure and societies are increasingly interdependent and vulnerable. This is because, as noted by the Forum's Global Future Council on Cybersecurity in 2022, "technological and comparative advantages can incentivize different organizations, often from different sectors, to rely on the same third-party hardware, software or service provider. Many firms, for instance, might have a reliance on poorly maintained open-source projects, or on the same cloud company or domain name services (DNS) provider. This concentrates risk when a shared service or commonly used technology is disrupted by cyberattackers."[12]

Larger firms typically have small and medium organizations in their supply chain and consider them as critical partners. When these critical partners are taken out of action through the technical or financial fallout from a cyber incident, the entire ecosystem, including the larger organizations, is negatively affected.

FIGURE 14 **Compared to my own organization's cyber resilience, I perceive our third-party organizations (who have direct connections, processes, or data) to be…**



Creating cyber resilience across a supply-chain

At the World Economic Forum's Annual Meeting on Cybersecurity in November 2022, the difference between the capabilities of larger and smaller organizations was raised as a point of concern by cybersecurity experts working across sectors and regions. Smaller firms were more likely to suffer from a lack of the trained cybersecurity experts needed to manage internal risk. Cross-sectoral resilience measures, such as cyberthreat information sharing, were of less value due to the same cyber skills and capacity issues.

Participants at the same meeting argued that it can be more difficult to hold the attention of the boards in small and medium-sized organizations because for them cyberattacks, while perhaps more likely to test the survival of a smaller organization, are episodic and potentially more easily forgotten than they are for larger firms that suffer regular attacks.

Added to this, smaller organizations do not often have the capacity to respond to incidents and are more likely to be economically paralysed by a major attack. This should make preparation for cyberattacks on suppliers a part of cyber-resilience measures and business continuity planning.

Leaders from larger organizations, those with more than 1,000 employees, were more likely to report incidents where they were negatively affected by a cyber incident originating from their suppliers, service providers or business partners (39% of larger organizations affected) than smaller organizations with fewer than 1,000 employees (25%).

In addition, larger organizations were less likely to report their third parties as being equally resilient as themselves (23%). Small to medium-sized enterprises, those with fewer than 1,000 employees, were more likely to consider those third parties to be equal in their cyber-resilience capabilities (38%).

The role of cyber insurance

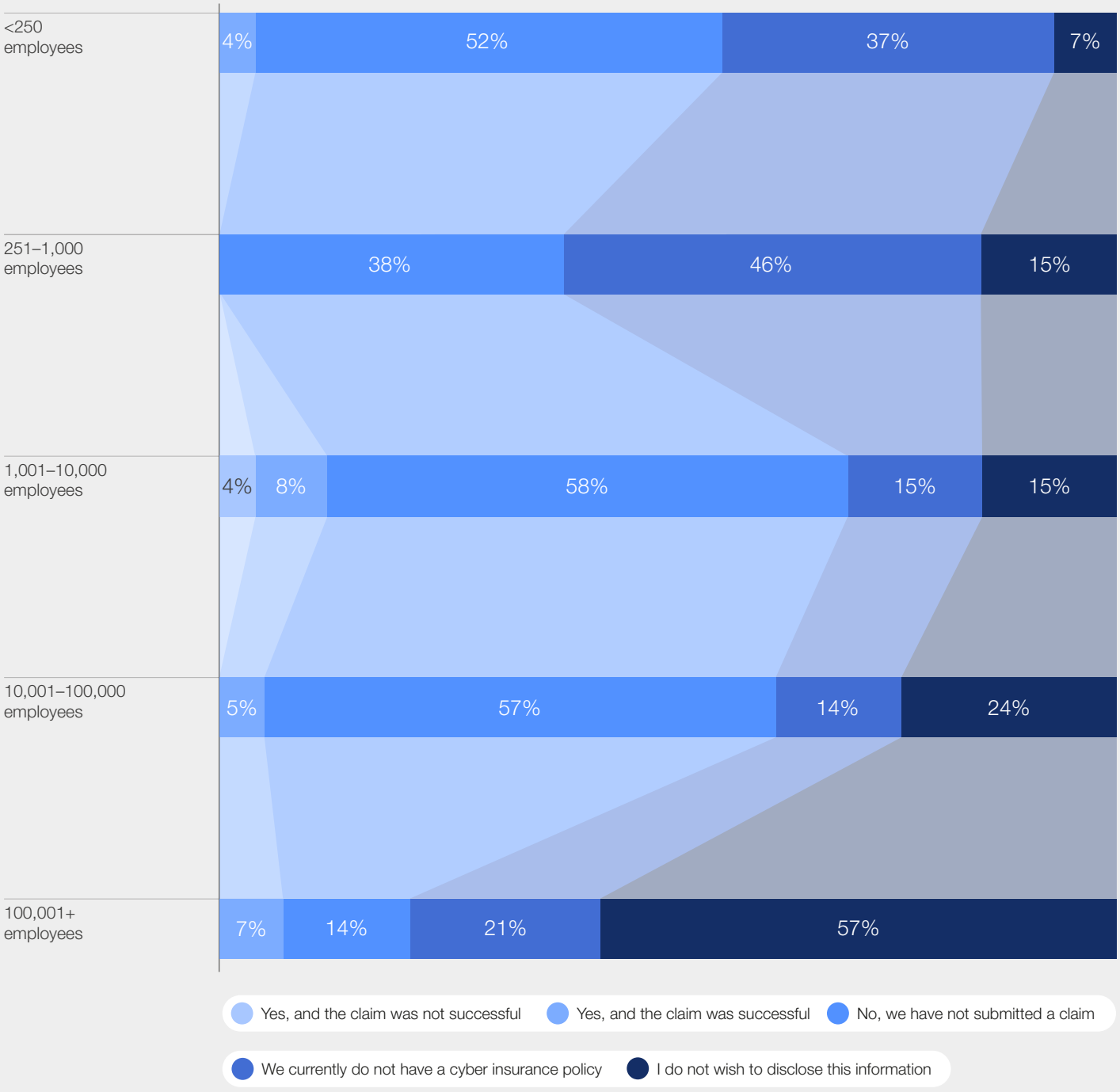
Cyber insurance is another way for organizations to mitigate the damage from cyber incidents.

Similar to supply-chain risk, organizational size was a determining factor in whether an organization was likely to have cyber insurance. Smaller organizations were more likely to report they did not have cyber insurance (48%) than larger organizations (16%).

This shows a critical gap in the cyber resilience of the entire ecosystem. Cyber insurance often comes with required actions that are likely to improve the cyber resilience of the insured party. If a smaller organization has an incapacitating cyber incident, with subsequent upstream effects on larger organizations, it will not have the resources to respond, nor will it receive assistance in its post-attack recovery in the form of an insurance payout.

In the absence of insurance, organizations would do well to focus on initiatives that support ecosystem resilience. By increasing the level of protection across their supply chain, organizations will enhance the cyber resilience of their own operations.

FIGURE 15 **Has your organization submitted a claim using your cyber insurance policy in the past two years?**



2.2 Gaining leadership support

> **Security executives gain by articulating a story to their board that aligns with corporate and business priorities. Boards should be presented with a cyber posture that resonates with customers' and authorities' expectations, and helps address sectorial ecosystem challenges.**
>
> Christophe Blassiau, Senior Vice-President Cybersecurity & Global Chief Information Security Officer, Schneider Electric

The shifts in perception and actions described above illustrate a closing gap between cyber leaders and business leaders in their perceptions of leadership support.

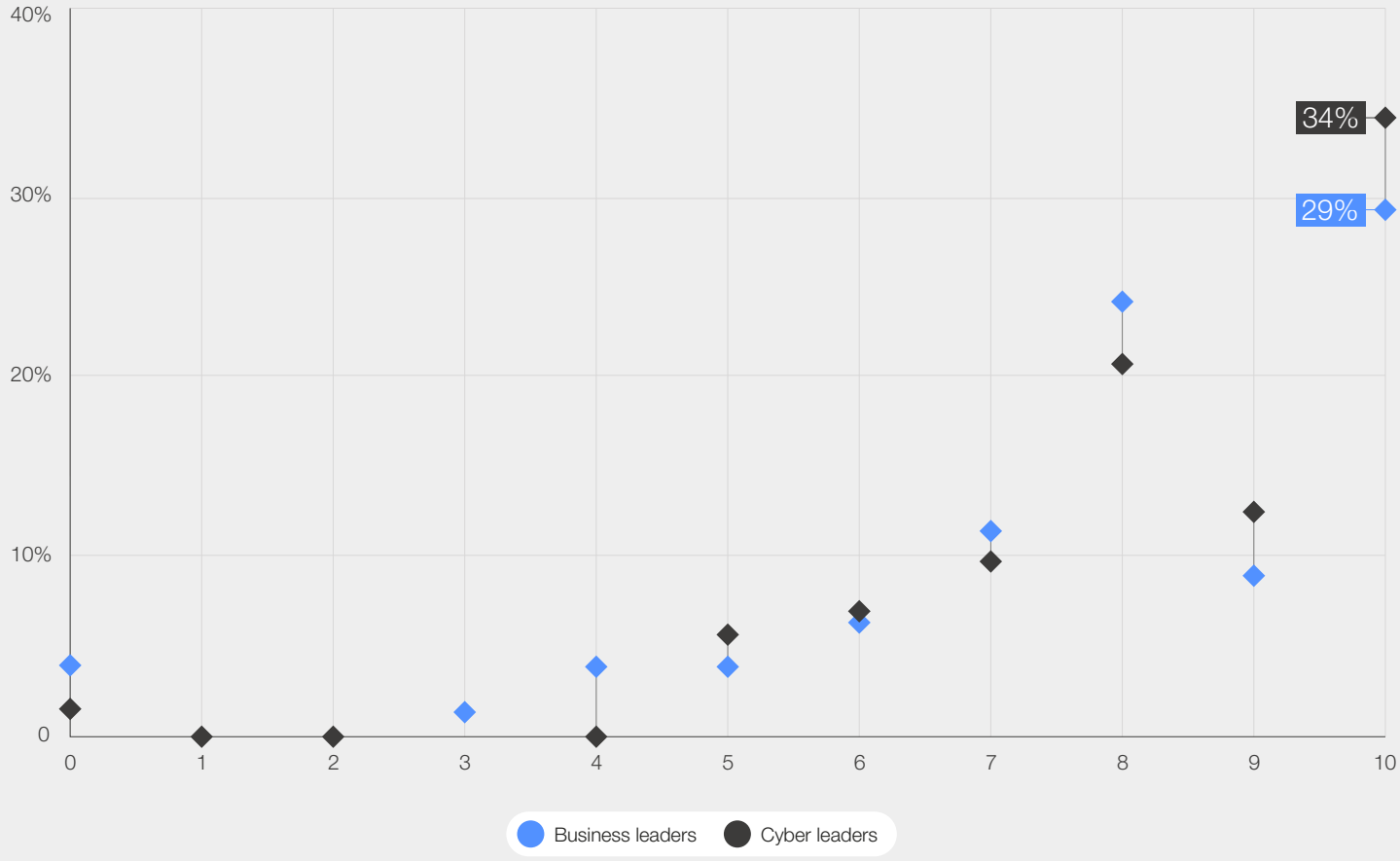
The 2022 Global Cybersecurity Outlook report highlighted how cyber leaders perceive leadership support as a primary challenge in the management of organizational cyber resilience. This year's outlook indicates that a third of all cyber leaders still ranked gaining leadership support as the most challenging aspect of managing cyber resilience. A majority, 94%, of respondents believe, however, that their board of directors has a duty of care when it relates to cybersecurity.

Cybersecurity and the board's duty of care

> **The security staff deserves the same level of trust that you would put in other business leaders. You may not know exactly what is coming, but you should be able to trust that the security leader is directionally right and you understand what their priorities are.**
>
> Remko Vos, Chief Executive Officer, CUJO

Organizational leadership has begun to listen to the concerns of cyber leaders. One interviewed executive explained, "Boards' understanding of their responsibility and duty of care has improved. In larger or regulated firms, this awareness has been helped by the interlocking committees that give several board members quite a bit of exposure to questions of digital transformation, information security, business continuity and cyber resilience."[13]

FIGURE 16 | **My organization's board of directors is able to uphold a duty of care when it comes to cybersecurity**



Cybersecurity and business leaders must learn to effectively translate their cyber risks into enterprise risk.

A primary challenge for cyber executives is shifting from gaining board support to enabling impactful board action. Multiple interviewees brought up the disconnect between how cyber risks are communicated to boards and how boards interpret and translate those risks in the context of overall enterprise risk.

While boards appear to be more cyber aware than before, the questions they are asking about cybersecurity imply that they may not have fully grasped the effect of cyber risk on enterprise risk. In addition, many continue to struggle to determine which questions are best suited to assessing information provided by their cybersecurity teams and enabling informed and risk-based decisions.

As one interviewee stated, "Being able to clearly describe the key operational risks and, as part of this, the key cyber-related risks, and then having the link between these risks and the operational or technical controls is important. This allows business leaders to gauge whether they know what their risks are and whether the organization is doing the right thing to protect itself."[14]

The difficulties cyber leaders report in communicating with business leadership demonstrate a comprehension gap between security issues and business impacts. Cybersecurity and business leaders must learn to effectively translate their cyber risks into enterprise risk, and into the right operational and tactical measures to mitigate those risks.

Here, the Forum's Principles for Board Governance of Cyber Risk offers common principles on which cyber leaders and business leaders can build. In order to shrink the board-level understanding of cyber risk, security leaders should help their boards to:

- Understand the economic drivers and impact of cyber risk – by reporting cyber risk in financial, economic and operational terms, not just in technical terms
- Align cyber-risk management with business needs – by identifying how cyber-risk management and resilience help to meet business objectives

For corporate directors, and business leaders, the principles counsel them to:

- Incorporate cybersecurity expertise into board governance
- Encourage systemic resilience and collaboration[15]

2.3 Cyber talent management

Cyber talent recruitment and retention continues to be a substantial obstacle for all organizations, as seen in both the 2022 and 2023 Global Cybersecurity Outlook reports. The perception gap between business and cyber leaders, however, has narrowed significantly, signalling alignment on the realities of the cyber labour market.

The 2022 Outlook report found that 10% of cyber leaders indicated they lacked the critical people and skills needed to deal with a cyberattack. No business leaders indicated that deficit.

Reponses to the same question in this year's Outlook report show that 10% of business leaders and 13% of cyber leaders feel that they have critical gaps in skilled personnel. The increases among both groups most likely indicate increased awareness of the talent gap rather than a worsening of the talent problem.

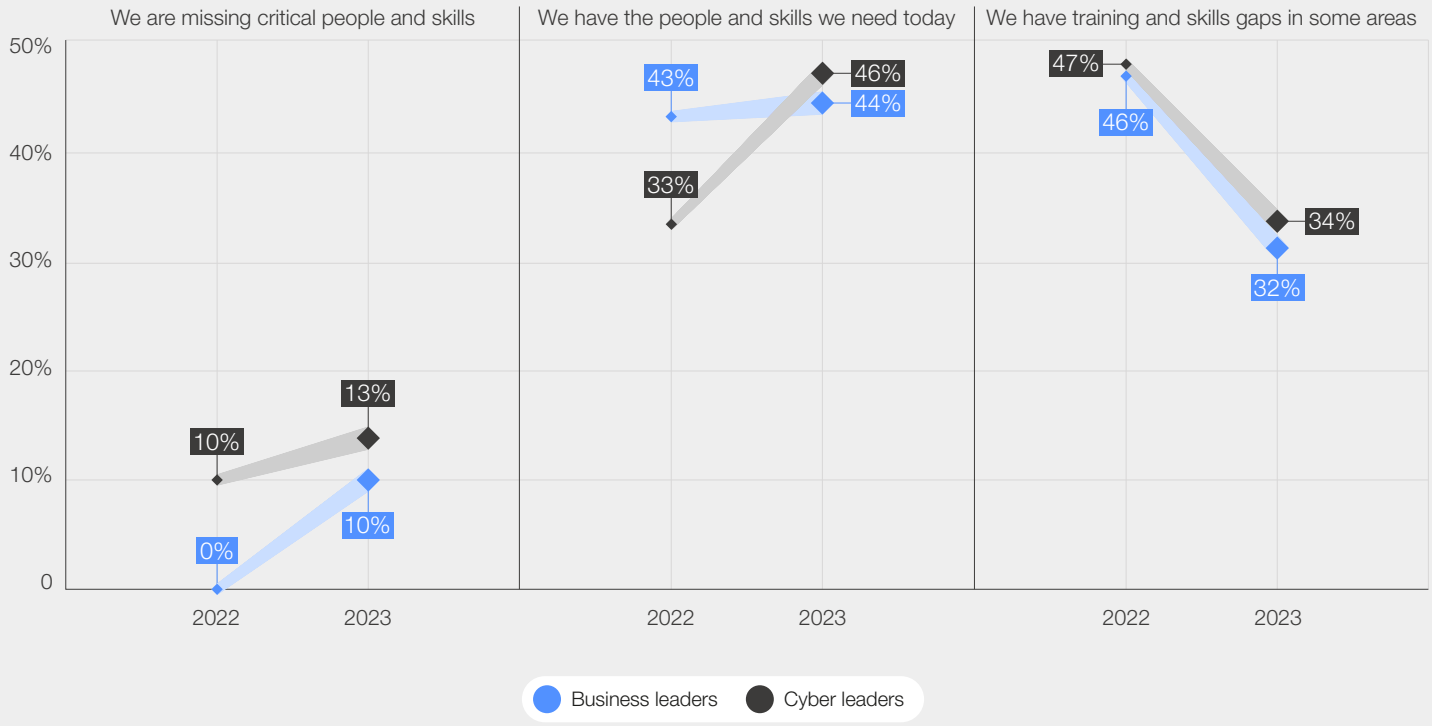
More than half of organization leaders in industries that provide or make heavy use of technology services (including those in the information technology and telecommunications industries) reported they have the skills needed today. In contrast, the industries that reported a lack of critical people and skills were mainly critical infrastructure industries – including energy utilities – and the public sector. The scale of the challenge in critical infrastructure, where specialized skills are often needed, is a concern. It will be difficult for many companies to solve the talent gap on their own and solutions are likely to require partnerships.

FIGURE 17 **Does your organization have the skills needed to respond to and recover from a cyberattack?**

FIGURE 18 | **The cybersecurity skills gap by industry**

In this year's Cybersecurity Outlook research, 59% of business leaders and 64% of cyber leaders ranked talent recruitment and retention as a key challenge for managing cyber resilience. Additionally, less than half of respondents reported having the people and skills needed today to respond to cyberattacks. The level of shared understanding on this topic makes it more likely that steps can be taken to solve the challenge of creating and retaining cyber talent.

FIGURE 19 | **The message is getting through (year-on-year alignment in business and security views on the skills gap)**



3 A way ahead

Boosting cyber resilience starts with improving communication between cyber and business leaders.

3.1 Improving communication

> **The role of the chief information security officer (CISO) is one of the most dynamic careers. We secure entire organizations as they evolve with new technologies in an increasingly digital environment. This means the CISO has a role in supporting the transformational change of a business's technology, culture and organizational structures.**
>
> Daniel Bariusso, Chief Information Security Officer, Banco Santander

17%
of security executives are concerned about the level of cyber resilience in their business.

In this year's report, 17% of security executives expressed concern about the level of cyber resilience in their business. This was up slightly from 13% of security executives the year before. Conversely, the increased level of awareness of cyber risk among business executives led to a marked increase in concern, from 16% to 27%. This might be due to a better understanding by business leaders of the damage that can be done to their business operations, commercial relationships and reputation by a major cyberattack.

Survey responses for this report indicate that the increased concern among business executives could also be driven by regulatory demands for increased board-level accountability for cyber-risk management. For example, in late 2022 the United States Securities and Exchange Commission (SEC) created rules that make cyber-risk reporting and business resilience planning a vital component of effective board management.[16]

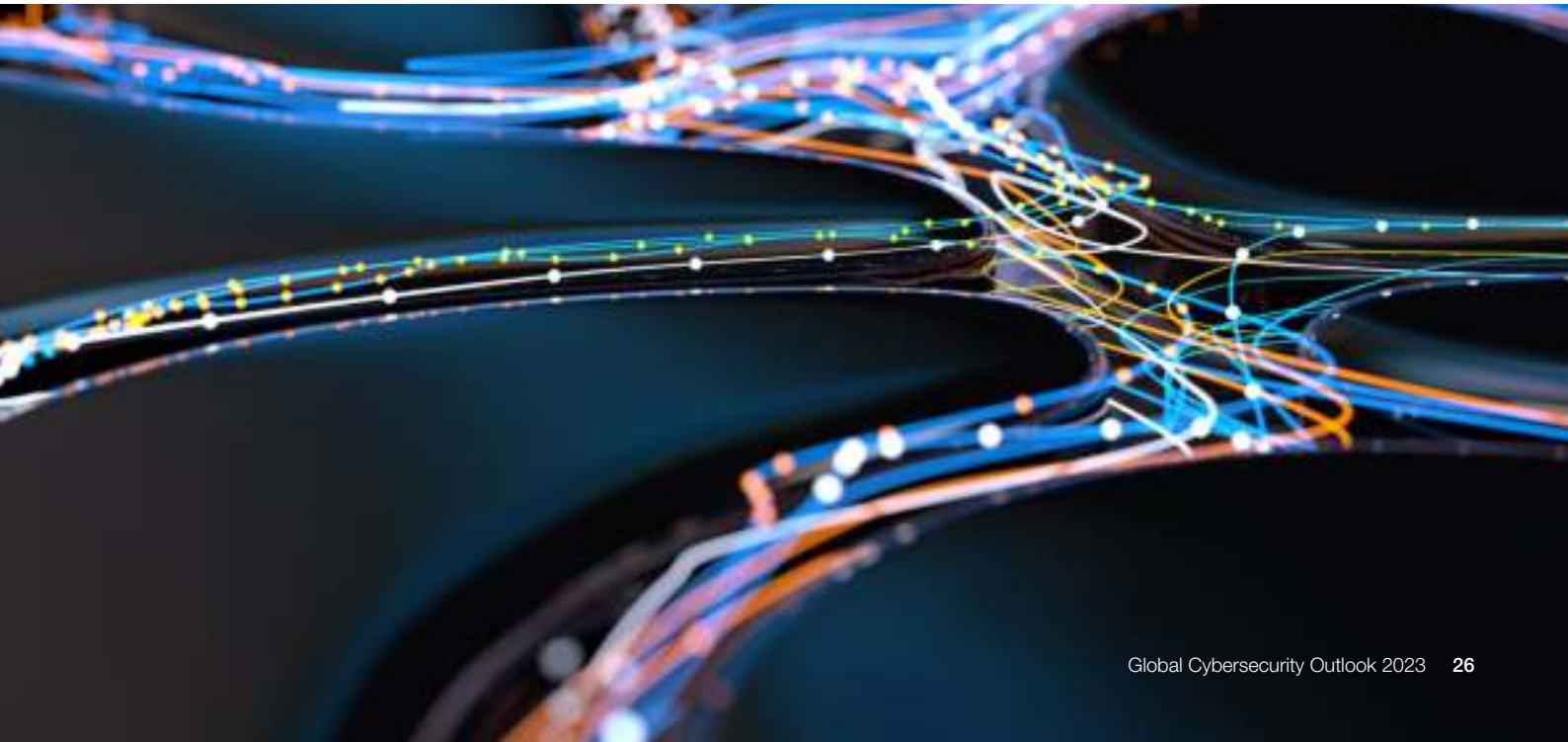
Lost in translation?

Security leaders and business leaders sometimes have difficulty translating cyber-risk information into mitigating actions in their organization. Security leaders who reported they were successful in translating risk to mitigation regularly demonstrated a capacity to make technical data comprehensible and relevant for organizational leaders.

The difficulty in translating cyberthreats to operational risk is a barrier to collaboration between security executives and business leaders. Commonplace terms such as "ransomware" can be explained to boards more easily, but mapping cybercrime campaigns or threat actors to the targeting of particular assets and resources is complicated.

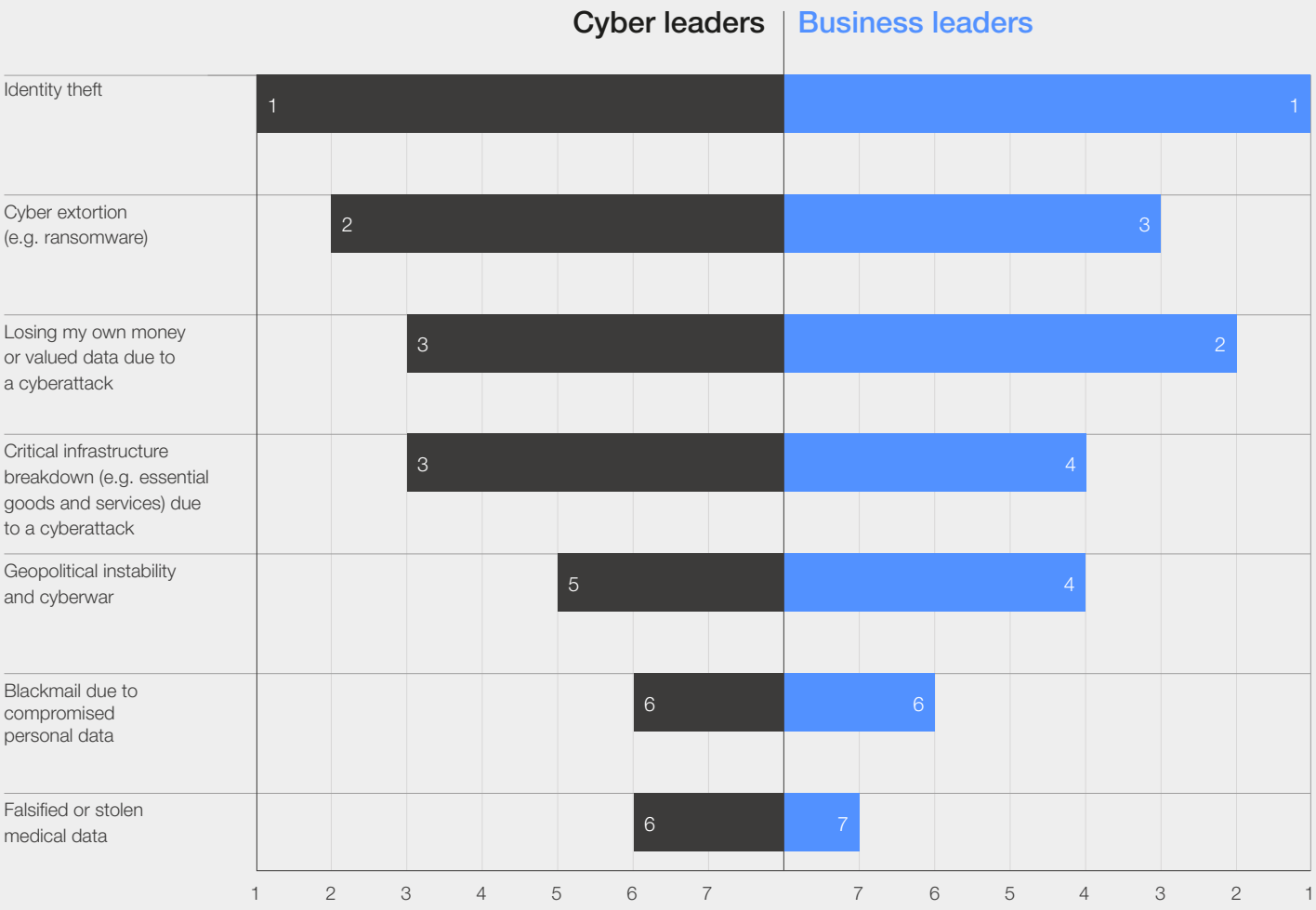
It has also proven difficult to quantify and assess cyber risk. Costs are often expressed in "average" terms when referring to a breach, but this may not be appropriate for an individual organization assessing its own risk.

Many organizations have too many assets on their network to identify the key risk points, or even to map their assets. This makes it difficult to assess where and how much money should be spent. Without a way to clearly map risks to value-creating assets or processes, as well as a plan of action arising from this, it is hard to quantify and justify the resources that should be allocated to mitigating them.



Shared starting points

FIGURE 20 **What cyber risk are you most concerned about when it comes to your personal cybersecurity?**



It can be useful to find a shared starting point for the conversation between security and business executives on cyber risk.

As mentioned earlier in this report, business leaders are often well-practised in adapting their organizations to geopolitical change. The research for this paper also indicates that security leaders and organizational leaders share the same concerns about their personal cybersecurity.

When considering personal risks, organizational leaders and security executives are most concerned about becoming victims of identity theft (ranked first) or cyber extortion and theft of data or money (ranked second and third by each cohort). So there are shared reference points at the macro level (geopolitics) and the micro level (personal digital security) that can be an entry point to a discussion on organizational and business cybersecurity.

Explaining return on investment in cybersecurity

During the World Economic Forum's Cybersecurity Outlook Series of workshops in 2022, participants noted the difficulty of translating investment in cybersecurity into clear returns for the board, with one representative participant saying, "The three things board members are interested in are risk, opportunities and investment in cost. In cybersecurity, we talk about the cost a lot, but we need to better respond to the question, 'What is the return?' That is something we struggled with in cybersecurity. How do I know this is a good investment across the myriad of things that I could potentially be invested in? How can we improve at making effective metrics to help boards make better-informed decisions?"[17] Effective metrics are ones that a board can translate directly into informed decisions to drive the business.

Steps to close the communications gap

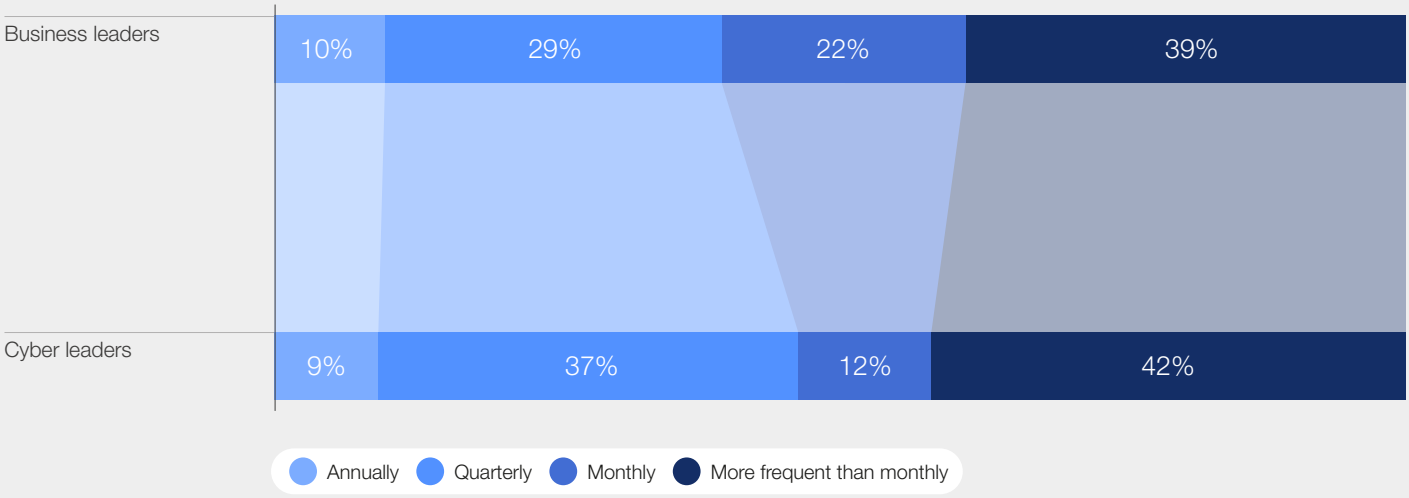
> Boards need to understand the strategic essence of the message from security teams and what that means for corporate governance and investment decisions in security and elsewhere.

Cyber leaders should actively work to close the communication gap with their non-technical audiences so that the relevance of their recommendations is understood and incorporated into risk-management strategies.

The challenge was clearly described by a business executive interviewee: "Cyber leaders remain, in general, weak at presenting the cybersecurity problem in terms that board-level executives can understand and act on. It's also true that boards need to have questions they can ask to assess what their cyber leaders are telling them. However, the message from cybersecurity experts is still too technical and the data they are providing is too 'scattered'. Lots of data [is] flying around and, while the environment can't be made less complex, boards need to understand the strategic essence of the message being received from security teams and what that means for corporate governance and investment decisions in security and elsewhere."[18]

Effective communication is the basis for success in any cyber-resilience programme. Cybersecurity leaders should use less technical jargon when speaking with business leaders. Boards of directors should help cybersecurity leaders understand what assets and processes must be prioritized for protection. Boards should then make themselves accountable for these priorities once they are set because cybersecurity resources are rarely sufficient to effectively defend all parts of an organization all of the time.

FIGURE 21 **Frequency of meetings**

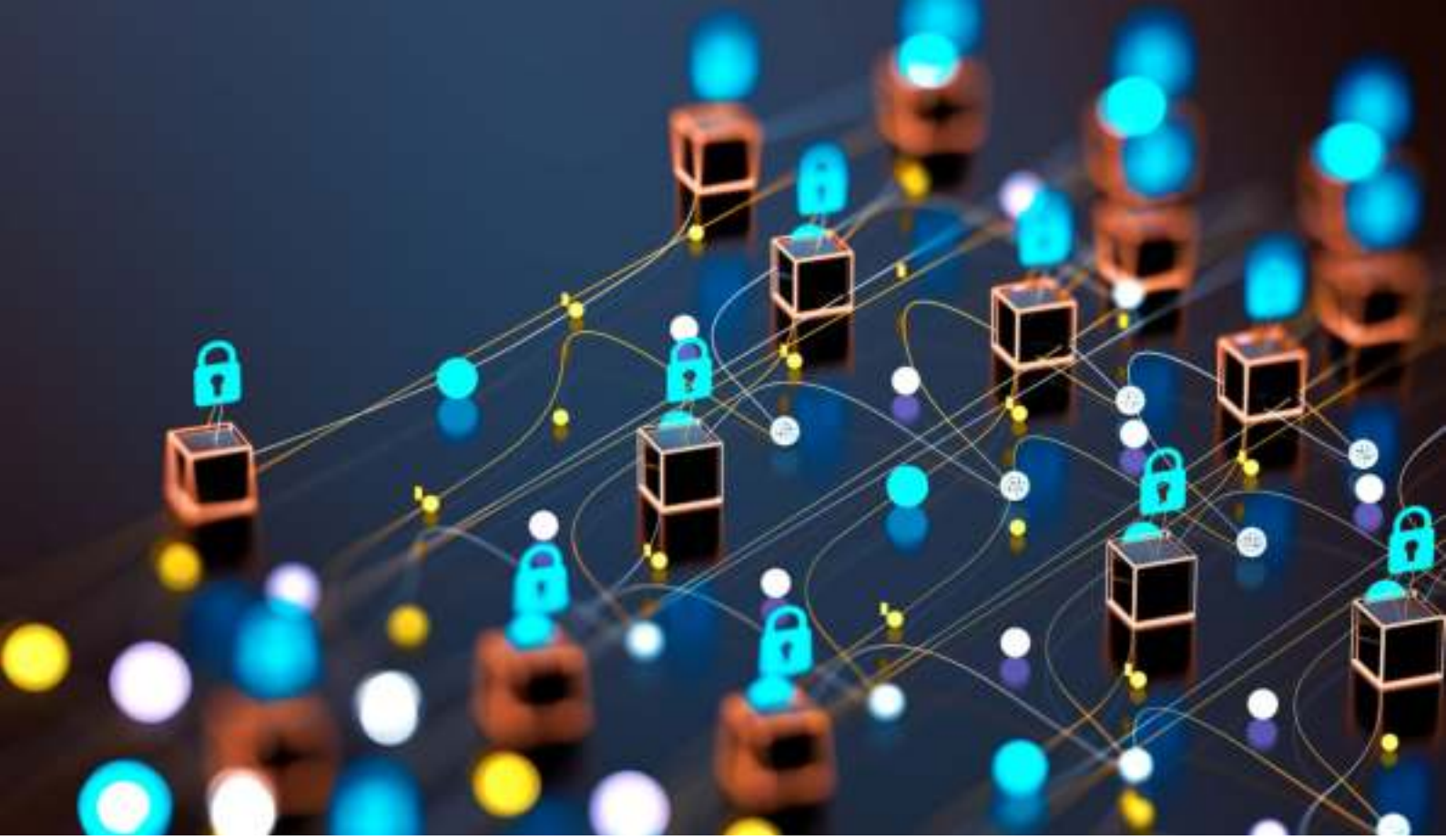


3.2 Reviewing organizational design

Organizational structures play an important role in embedding cyber-risk management across an organization. They shape the frequency and quality of cyber-risk discussions, and can create opportunities for improved clarity, context and understanding between security and business teams. As one participant at the World Economic Forum's 2022 Cyber Outlook Series of workshops highlighted with regard to organizational and reporting structures: "I report to the CEO, which is a huge advantage; we have portfolio companies where cybersecurity is still in IT. Not having direct reporting to the board is a big disadvantage. Reporting should come from the person responsible for it."[19]

That participant was not alone in their opinion that the most senior cybersecurity executives should report directly to CEOs. Another respondent opined that by having the CISO report directly to the CEO, budgeting conflicts between security initiatives and technology enablement might be avoided.[20]

As observed in the 2023 Global Cybersecurity Outlook survey results, only 25% of all respondents indicated that the most senior cybersecurity executive in their organization reports directly to the CEO. However, other security executives pointed to the importance of the chief information officer (CIO) as a champion for cybersecurity across a business. There is no single approach to making this work, but it is important that security executives have access to senior business leadership.



3.3 Building security culture

A security culture starts with awareness and includes everyone. Increased employee awareness about cyberattacks was cited by cyber leaders who took part in the survey as the most positive influence on an organization's cyber-resilience approach in the next 12 months. An organization's cyber capabilities grow with its employees' understanding of cyber risks and their personal role and responsibility in helping to manage them.

Organizational leaders should consider pushing more accountability for operational cyber requirements onto business leaders. As an example of how this can change an organization's security culture, one interviewee explained that their organization previously granted cybersecurity control exceptions without considering how those exceptions could increase their cyber risk. To address this, it is establishing a new executive committee to review exceptions. "Now if you need an exception, you will have to come in front of the CTO, CIO and CISO to defend your case ... the business might not immediately be ready for the mitigation controls and the path forward, but now I am looking for a mindset shift. When you need to stand in front of three executives, your preparations have to be completely different. We need this to drive cultural shifts towards security."[21]

The cybersecurity team, if used thoughtfully, can provide vital insights that help embed cyber-risk methodologies in an organization. For example, one security executive interviewed for this report identified their organization's human resources team as being considerably more likely to open suspicious attachments than other parts of the organization. Further investigation revealed that staff in this team had no secure portal in which to access job applications from external candidates and were thus required to open large numbers of resumés that arrived as email attachments. The volume of attachments processed by this team increased the likelihood of a malware-infected attachment being opened. This allowed the security executive to make an organizational recommendation, that the human resources team be provided with an online portal for job application submissions to reduce the risk of opening malicious files that could severely damage the wider company.

This high-value consultative approach can be taken when boards give security executives the time and space to step away from their daily role of surveillance and response to act as an adviser to the rest of the organization.

Where possible, security should be focused on higher-order topics that are more specialized than basic operations. Cyber leaders should contribute cybersecurity requirements that business units can incorporate into their key performance indicators (KPIs), after which all leaders must demand real enforcement, real consequences and real incentives to achieve the agreed-upon KPIs. Meaningful incentive structures make change happen.

"The cybersecurity team, if used thoughtfully, can provide vital insights that help embed cyber-risk methodologies in an organization.

3.4 Closing the cyber talent gap

> **People think that cybersecurity is something that's highly technical. Yes, some roles require deep technical expertise, but cybersecurity is a vast domain and making an organization cyber resilient also requires generalist roles that need a broader skillset, from education and awareness to policy writing, governance and others. We need more people in the both the technical and generalist roles.**
>
> Bobby Ford, Senior Vice-President and Chief Security Officer, Hewlett Packard Enterprise

2.27m
Shortfall between supply and demand for cybersecurity experts in 2021

As indicated in the previous section, talent recruitment and retention continue to be a key challenge for managing cyber resilience. The shortfall between supply and demand for cybersecurity experts was estimated at 2.27 million in 2021.[22]

Currently, organizations are competing for talent by paying more to the same small pool of people. This exacerbates the staff shortage by creating a high turnover of cybersecurity experts from company to company. Paying more is a stopgap that will not solve the longer-term problem.

More needs to be done to increase the flow of cybersecurity talent into the workforce. This has been a consistently difficult problem to solve, but it is also an area with possibilities for real progress.

New and inventive projects are being launched every year. A significant number of organizations understand that cybersecurity touches on many areas of their activity and making an organization cyber resilient requires a wide range of skill sets. Respondents to the surveys as well as participants in the interviews and workshops consistently argued that the academic and professional disciplines that lend themselves to cyber-resilience skills are much broader than many people realize and are certainly not limited to computer science or engineering. The soft skills for cyber roles can come from disciplines such as economics, law, psychology, sociology, communications and media studies.

Expanding the talent pool

A broad solution to increase the supply of cyber professionals is to expand and promote inclusion and diversity efforts within cyber recruitment. Underrepresented groups in cybersecurity such as women, people of colour and those with informal educations have been continually discouraged from technical careers through societal expectations and perceptions of cybersecurity work culture.

This is not a simple solution. As a first step, it requires broadening the narrative about who can work in cybersecurity so that people with non-technical backgrounds, as well as those outside of the traditional education system and from underrepresented groups, understand that there are currently roles for them as well and that it is possible to retrain for technical roles in the near future.

Many cybersecurity roles can be learned on the job or through apprenticeships. Democratizing access to cybersecurity career paths has the potential to be a social good, supporting reskilling of sections of the workforce.

However, capitalizing on the increased interest in cybersecurity is also likely to require greater collaboration between organizations. Even high-quality apprenticeship and training programmes run by individual organizations, such as the Absa Cybersecurity Academy in South Africa,[23] have encountered difficulties scaling to large numbers.

Diversity and talent pipelines can be further improved if organizations build relationships with civil society organizations such as Girls Who Code in the US and Africa Teen Geeks in South Africa. It's also possible to open the recruiting process by focusing more on skills and experience rather than four-year degrees.

As cyberthreats evolve and expand, so must the talent pool that engages with them. As argued in October 2022 by experts from the Tech for Good Institute, the Tifa Foundation and the United Nations University Institution: "Designing and implementing appropriate cybersecurity solutions … demands non-technical competencies such as business, management, legal, policy and diplomacy."[24] The need for these competencies grows as "socio-technical threats such as social engineering and online abuse are increasingly prolific".[25]

Social inclusion and diversity issues should not be decoupled from the discussion of cyber talent development. Many skills projects are successful because they focus on diversity of professional or lived experience. Diversity is not a "nice-to-have" addition to a cyber-skills programme but something that is likely to influence the programme's success and also strengthen the cyber resilience of an organization to the highest degree. Employing a range of people with diverse opinions, backgrounds, experiences and identities leads to

> Traits such as curiosity, problem-solving and critical thinking are vital for cyber professionals.

stronger outcomes and produces greater insights in any setting, including cybersecurity.

Understanding the broad spectrum of skills needed to be cyber resilient in the current cyber landscape can help enable organizations to expand their hiring pools.

Work conducted by the World Economic Forum and its partners in 2021 identified four concrete steps taken by organizations that prioritize diversity, equity and inclusion. These steps should be seen as the minimum for organizations seeking to attract and retain a diverse workforce that will increase their cyber resilience:

- Ensure that leaders actively support diversity, equity and inclusion across the organization.
- Create opportunities for everyone to publish, write and engage in public speaking.[26]
- Treat all employees as individuals, provide opportunities for them to express themselves, create a safe space and acknowledge their contributions.
- Prioritize retention and development opportunities for diverse staff members. Employee retention is essential to increase diversity at higher organizational levels.

Once hired, organizations can train professionals to become effective cyber employees. Technology can always be taught, but traits such as curiosity, problem-solving and critical thinking are vital for cyber professionals. Organizations should therefore seek these traits even when recruiting experienced talent. As a Forum article says, "Professionals cannot be static in their knowledge to succeed in this field."[27]

Conclusion

The 2023 Global Cybersecurity Outlook study showed that the profound disconnect between how cyber leaders and business leaders perceive cyber issues – a core finding of the 2022 edition of this report – has begun to close.

Both security leaders and business leaders needed to adapt and change their mindsets to make this possible.

When we compare this year's findings with the 2022 edition of this report, business leaders are more aware of the threat landscape and cyber leaders made more frequent appearances before their board of directors. Both groups have a clearer view of the strengths and weaknesses of their organizations' cyber capabilities, and cyber issues are more integrated into enterprise risk management and now receive more board-level support.

However, the study also revealed that cyber and business leaders still have a great deal of work to do to truly understand each other, articulate the risk cyber issues pose to their business and translate that into meaningful management and mitigation measures. As the cyber landscape promises to become more complex in the coming years, it is critical that organizations work to resolve this now if they are to build systemic cyber resilience for the long term.

Fortunately, building long-term capability is in the interest of all executives. As one leader stated, "There is value in providing business leaders with access to cyber-issue information. Business leader roles such as CRO, BoD and CEO evaluate risks over a long time frame, and this long-term strategic focus can help overcome the tendency to focus less on cyber response and more on cyber resilience."[28]

Yet, the 2023 Global Cybersecurity Outlook study illustrated that time is both the most valuable asset and a stubborn adversary in this regard. The results indicated that the tenure for cyber leaders is often short and the turnover of cyber talent is high. Furthermore, the dynamics of the threat landscape frequently focus attention on tactical defence at the expense of extended strategy, horizon planning and investment.

Jacky Fox, Europe Security Lead for professional services firm Accenture, put it this way: "One of the biggest barriers to cyber resilience in many organizations is time. Business leaders broadly understand they need to become more cyber resilient, but they can't snap their fingers to make it happen. They know there is a journey to travel to make their organizations cyber resilient, but time is not on their side."

Breaking that cycle will require concerted communication and a coordinated risk-driven improvement effort across the C-suite. In a cyber environment with such interconnected systemic implications, this is imperative for all public- and private-sector organizations. Encouragingly, it is also a message that is recognized consistently in the Global Cybersecurity Outlook year after year and by leaders across the globe.

Appendix: Methodology

Insights for the Global Cybersecurity Outlook 2023 were gathered from five sources: first, a survey of global organizational leaders; second, a workshop with the World Economic Forum's Cybersecurity Leadership Community and Global Future Council on Cybersecurity in October 2022, as well as workshops conducted during the World Economic Forum's Annual Meeting on Cybersecurity in November 2022; third, a multitude of interviews with experts and bilateral meetings; fourth, the collection of data from reports, research and articles published by the World Economic Forum and reputable third parties. In combination with all of these efforts, the World Economic Forum's team consulted 151 global organizational leaders.

Cyber Outlook Survey

The World Economic Forum's Centre for Cybersecurity and Accenture generated a survey comprised of 27 questions. The questions focused on cybersecurity and cyber-resilience progress, foresight, challenges and perceptions. The survey was administered to global leaders within the following groups: Accenture account teams client counterparts; the Forum's cyber leadership community; the Forum's chief strategy officers community; the Forum's New Champions; and the Forum's Young Global Leaders.

The survey was anonymous and non-attributable to the respondents or their respective organizations. Demographic questions were asked in the survey and included: industry; ranges of number of employees in the respondent's organization; annual revenue ranges of the respondent's organization; country in which the respondent's organization is headquartered; and the respondent's job title. There were a total of 117 responses from 32 countries and 22 industries.

Except for one percentage slider (ranging from 0–100%) and seven sentiment responses (ranging from 1 to 10 where 1 is "strongly disagree", 5 is "neither agree nor disagree" and 10 is "strongly agree"), all survey questions provided respondents with a list of pre-populated answers from which they could select. Where appropriate, a text box labelled "other" was available to permit the addition of responses not included in the pre-populated responses. Three questions asked respondents to rank their responses, which also permitted respondents to create and rank their own unique responses using a text box input.

Cyber Outlook Series

The Forum Centre for Cybersecurity hosted a series of workshops in 2022 as part of its Cyber Outlook Series sessions, with the goal of creating opportunities for unique peer-level exchanges on key cybersecurity issues among members of various leadership communities. This series included a workshop to test the validity of the Global Cybersecurity Outlook survey results. During 2022, the Forum actively engaged more than 151 members of these communities on the questions raised in this report. The Cyber Outlook Series of workshops were held under the Chatham House Rule; consequently, no information in this report is attributed to a specific member of these communities

Contributors

World Economic Forum

Lead authors

Gretchen Bueermann
Research and Analysis Specialist,
Centre for Cybersecurity, Switzerland

Seán Doyle
Lead, Centre for Cybersecurity, Switzerland

Additional contributors

Daniel Dobrygowski
Head of Governance and Trust,
Centre for Cybersecurity, USA

Akshay Joshi
Head of Industry and Partnerships,
Centre for Cybersecurity, Switzerland

Luna Rohland
Early Careers Programme, Centre for Cybersecurity,
Switzerland.

Accenture

Carlos Aguirre
Security Senior Manager, USA

Taylor Browder
Security Consultant, USA

Jim Pruitt
Principal Director, USA

Michael Rohrs
Security Senior Manager, USA

Lauren Stockton
Security Senior Analyst, USA

Acknowledgements

Harim Jung
Data Analyst, Climate Change Data
Visualisation Org, South Korea

HyoJin Park
Creative Producer, World Economic Forum,
Switzerland

Campbell Powers
Data Fellow, World Economic Forum,
Switzerland; Salesforce, USA

Giovanni Salvi
Data Intelligence Manager,
World Economic Forum, Switzerland

Nicolas Siegenthaler
Video Producer, World Economic Forum,
Switzerland

Editing and design

Laurence Denmark
Designer, Studio Miko

Sophie Ebbage
Designer, Studio Miko

Alison Moore
Editor, Astra Content

Endnotes

1. World Economic Forum, "Systemic Cybersecurity Risk and Role of the Global Community: Managing the Unmanageable", November 2022: https://www3.weforum.org/docs/WEF_GFC_Cybersecurity_2022.pdf.
2. Pipikaite, A., Holla-Maini, A., Ware, B. and Dickinson, M., "Will the Battle for Space Happen on the Ground?", World Economic Forum, 25 May 2022: https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/.
3. World Economic Forum, "Earning Digital Trust: Decision-Making for Trustworthy Technologies", 15 November 2022: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
4. Phone Interview with Seán Doyle, World Economic Forum, 19 September 2022.
5. See Cybersecurity and Infrastructure Security Agency, "Apache Log4j Vulnerability Guidance": https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.
6. Phone Interview with Seán Doyle, World Economic Forum, 13 October 2022.
7. Phone interview with Seán Doyle, World Economic Forum, 9 September 2022.
8. World Economic Forum, "Principles for Board Governance of Cyber Risk", 23 March 2021: https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.
9. World Economic Forum, "Global Cybersecurity Outlook 2022", January 2022: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.
10. Page, C., "Viasat Cyberattack Blamed on Russian Wiper Malware", *TechCrunch,* 31 March 2022: https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper.
11. Tidy, J., "Swedish Coop Supermarkets Shut Due to US Ransomware Cyberattack", BBC News, 3 July 2021: https://www.bbc.com/news/technology-57707530.
12. World Economic Forum, "Systemic Cybersecurity Risk and the Role of the Global Community: Managing the Unmanageable", November 2022: https://www3.weforum.org/docs/WEF_GFC_Cybersecurity_2022.pdf,
13. Phone Interview with Seán Doyle, World Economic Forum, 17 September 2022.
14. Phone Interview with Seán Doyle, World Economic Forum, 14 October 2022.
15. World Economic Forum, "Principles for Board Governance of Cyber Risk", 23 March 2021: https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.
16. World Economic Forum, "Here's What Regulators Will Want Boards to Know About Cybersecurity",24 October 2022: https://www.weforum.org/agenda/2022/10/here-s-what-regulators-will-want-the-board-to-know-about-cybersecurity/.
17. World Economic Forum, Cyber Outlook Series Workshop. Cyber Outlook Series, Virtual, 22 October 2022.
18. Phone Interview with Seán Doyle, World Economic Forum, 6 September 2022.
19. World Economic Forum. Cyber Outlook Series Workshop, Cyber Outlook Series, Virtual, 22 October 2022.
20. Phone Interview with Seán Doyle, World Economic Forum, 10 October 2022.
21. Phone interview with Jim Pruitt, World Economic Forum, 3 October 2022.
22. (ISC) ², "(ISC)² Cybersecurity Workforce Study", 2022: https://www.isc2.org/Research/Workforce-Study.
23. ABSA, "Cybersecurity Academy": https://www.absa.africa/absaafrica/a-force-for-good/cybersecurity-academy/.
24. Christine, D., et al, "Beyond Supply and Demand: Addressing the Multidimensional Workforce Gaps in Cybersecurity", World Economic Forum, 21 October 2022: https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gaps-inclusive-approach-jobs/.
25. Ibid.
26. Pipikaite, A. and Zabierek, L., "Why Cybersecurity Needs a More Diverse and Inclusive Workforce", World Economic Forum, 26 October 2021: https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/.
27. Ibid.
28. Phone Interview with Seán Doyle, World Economic Forum, 18 September 2022.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org