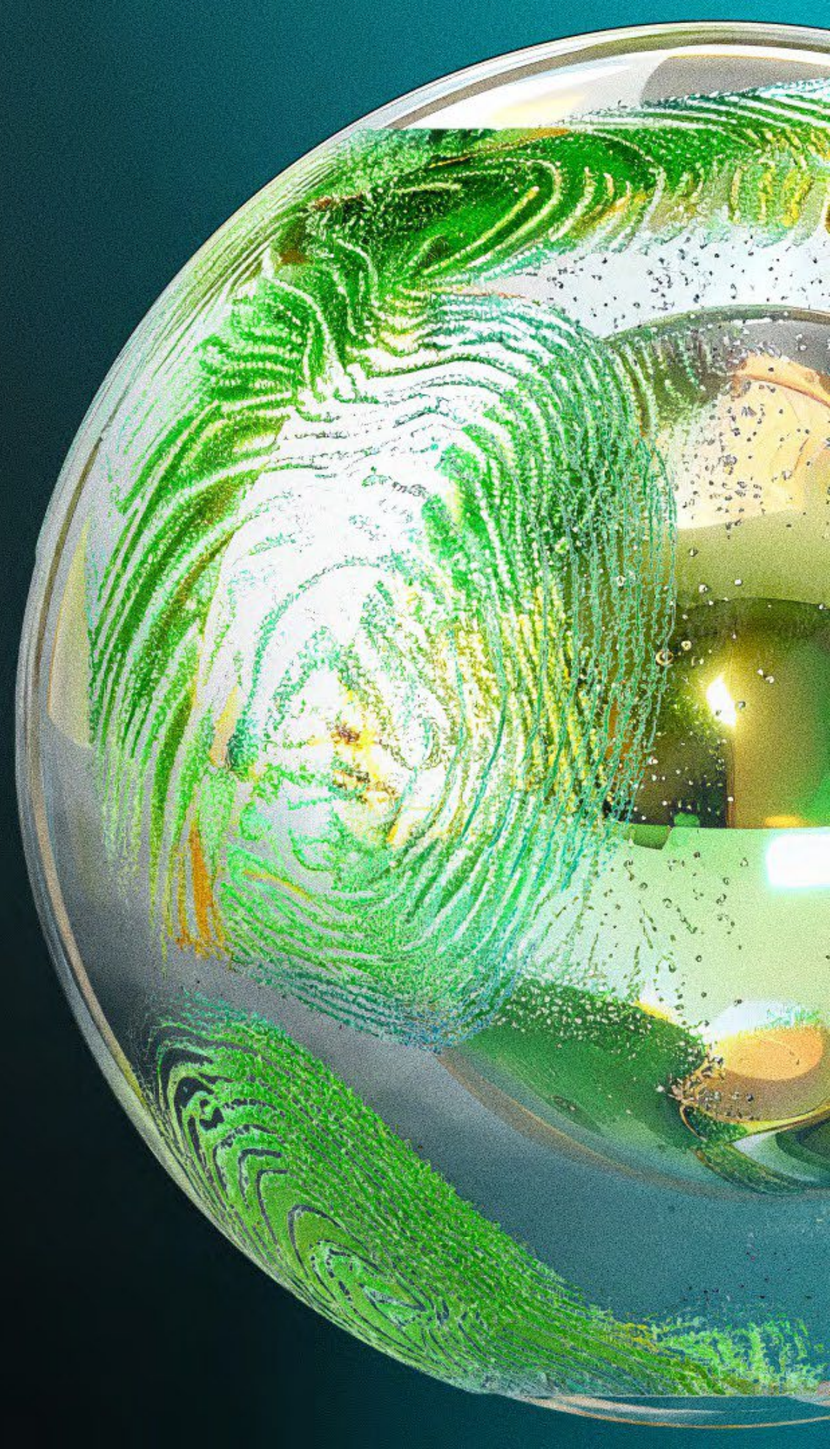
Deloitte.

*Together makes progress*

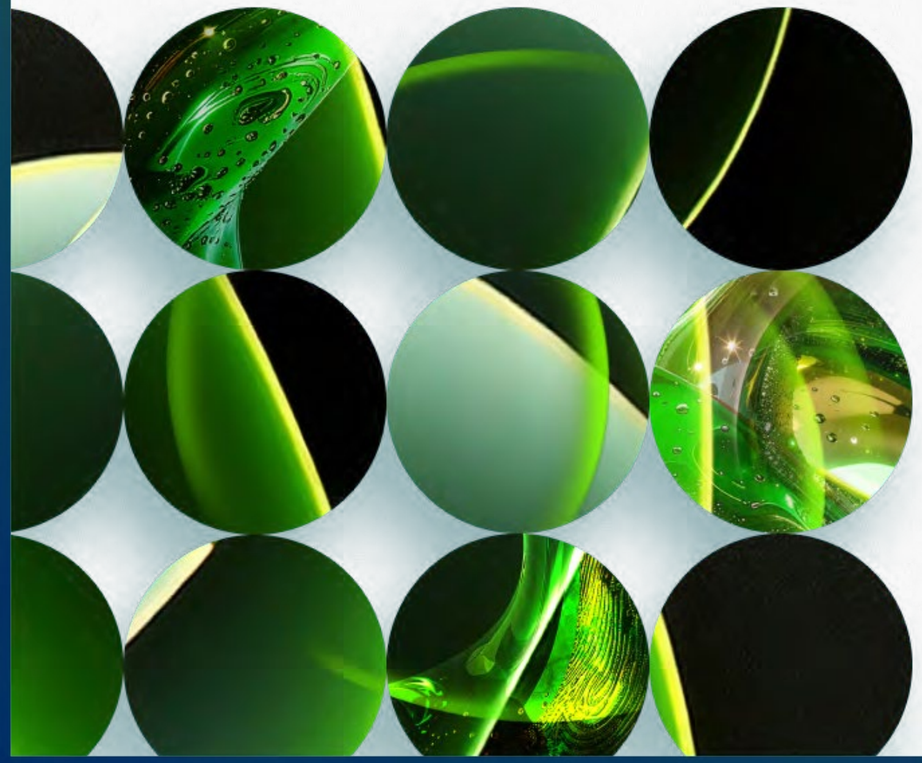
THE GLOBAL FUTURE OF CYBER SURVEY, 5TH EDITION

# 5 PARADOXES SHAPING THE FUTURE OF CYBER

Contradictions at the core of cybersecurity strategy today—and how cyber leaders are navigating them



# Progress and Paradoxes



**In our years conducting this survey, we've documented the steady progress of cyber capabilities in increasingly treacherous conditions. The threat landscape has evolved considerably in that time. But survey respondents have so far responded with a steady hand, bolstered by executive support and funding, to successfully defend against a rising tide of cyber risks.**

So we were excited to dive into this year's survey data to learn what more than 1,000 of the world's cyber and business leaders had to say about the current environment—and what's next. What did we find? A series of fundamental paradoxes—data points that at first appear to contradict one another, but upon further investigation may offer richer, more useful insights into what cyber decision makers are up against and how they're responding to a complex, shifting marketplace.

Maybe it shouldn't be surprising to discover seeming paradoxes and contradictions at the heart of a cyber-focused survey conducted in late 2025. Because the past few years have been marked by so much change (not just in the threat landscape, but in the tools and technologies used on both sides of the cyber battle) that strategy- and execution-level disconnects may have been inevitable.

Regardless of the reasons for their emergence, these paradoxes warrant the careful attention of anyone who has some responsibility for their organization's cyber strategy, as they may reveal weaknesses or gaps that need to be resolved quickly.

In the following pages, you will find a blend of data-driven insights provided directly by survey respondents along with Deloitte's future-focused observations based on in-depth market interviews and our deep global cyber experience.

We hope these insights help you navigate your own cyber journey. Happy reading.

Emily Mossburg
Deloitte Global Cyber Leader

# What sets Cyber Frontrunners apart

When examining how the cyber market is evolving and how organizations are planning for the future, we have always been particularly interested in leaders' distinguishing characteristics. Deloitte's proprietary cyber maturity index has been a hallmark of previous editions of this report, using survey data to highlight organizations that have successfully executed a defined set of cyber-focused actions. Their insights, behaviors, and practices can be instructive for others seeking to advance their cyber capabilities as quickly and effectively as possible, avoiding the pitfalls and dead ends that others may have already navigated.

Previously, we defined leaders as those who had integrated the highest number of key cyber program elements to reduce risk to their organizations and maintained a steady focus on artificial intelligence (AI). Today, these are simply requirements for any organization that is serious about cybersecurity. Therefore, when thinking about what it takes to be a leader in a market where the baseline has moved, we looked at the data to establish a new frame based on what we discovered.

This latest survey reveals a gap between respondents' confidence in their cyber capabilities and their level of readiness for future cyber challenges—the first paradox examined in this report. In response, we have evolved the Deloitte Cyber Maturity Index, our rating and segmentation of respondents' cyber maturity based on their adoption of leading practices. The updated Index allows us to examine and understand the actions respondents are taking to successfully close that gap, by zeroing in on the respondents with the highest cyber confidence and readiness.

This report identifies three groups based on their levels of confidence and readiness. The "Frontrunner" group scored highest for questions related to both cyber confidence and readiness. Those who scored lower fall incrementally into "Followers" and "Foundation Builder" groups[1]:

| FRONTRUNNERS | FOLLOWERS | FOUNDATION BUILDERS |
|---|---|---|
| 17% | 60% | 24% |

For additional details on the methodology used to categorize survey respondents, please see the Methodology section at the end of this report.

**Five paradoxes**

Frontrunners have made significant progress in deepening key relationships and embedding cyber strategies at the highest levels of their organizations. But the five paradoxes identified here reveal opposing forces that could hinder cyber readiness, execution, platform strategies, impact and stability, today and well into the future.

[1] Note: totals may not add up to 100% due to rounding. This is the reason for the variance and is not an error.

PARADOX #1

# **Cyber confidence is high.**
But are organizations ready?

# Cyber leaders have made significant strides to gain confidence

**Our previous report revealed a growing maturity in cyber capabilities and approaches. Survey respondents largely reported that the Chief Information Security Officer (CISO) role was fully embedded and maturing, cyber strategies were being integrated into many different parts of the organization, there was a growing understanding throughout the C-suite of the role cyber strategy can play in generating real business value, and respondents were increasing their focus on driving positive business outcomes.**

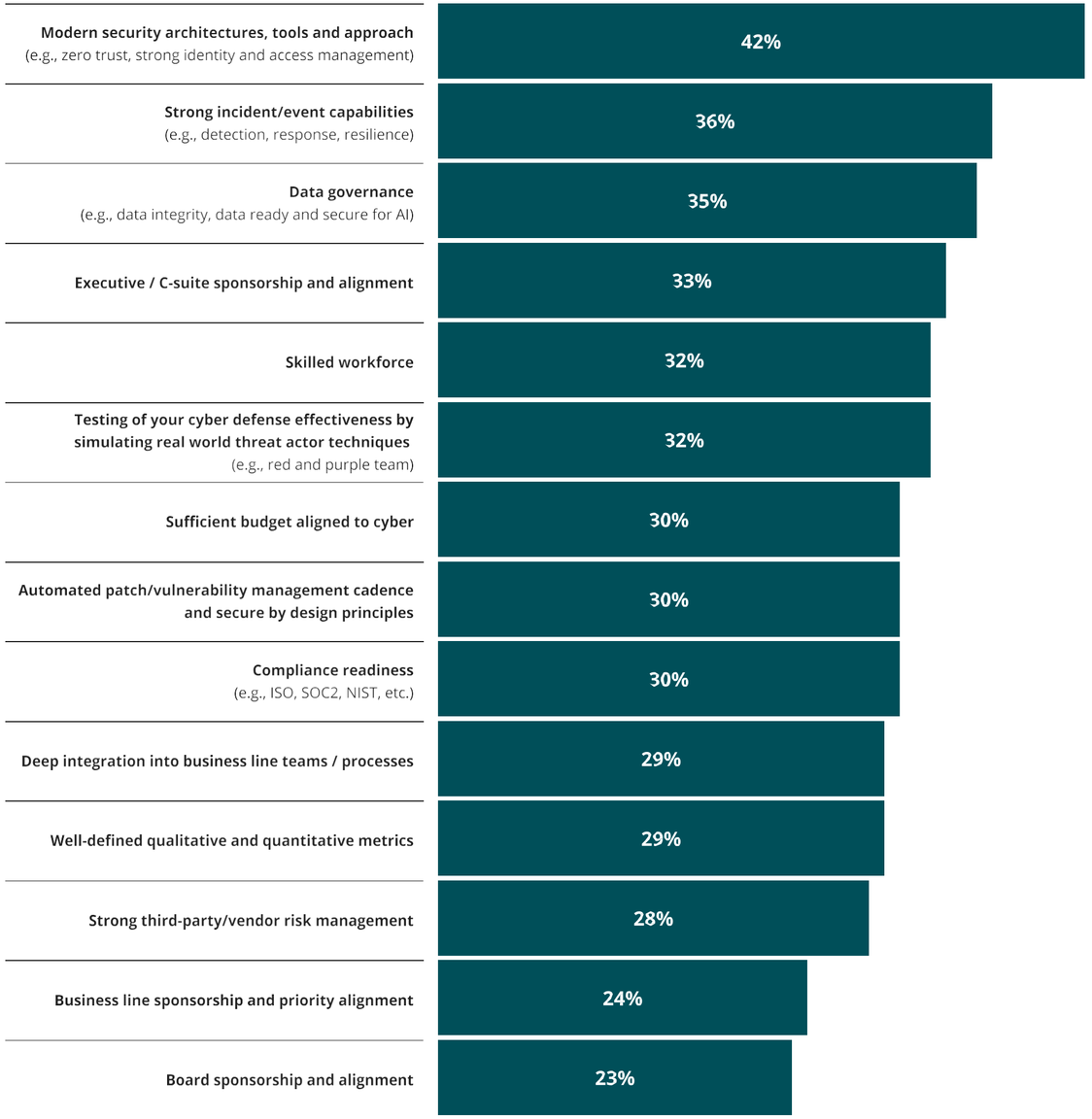
In this edition of the survey, the majority of respondents (85%) say they are somewhat or very confident in their organizations' cybersecurity strategy, citing modern security architectures, strong incident response capabilities, data governance, and other factors shown in the figure at right.

They also report having strong support from the C-suite, and ready access to the budgets they need to stay a step ahead. This support is increasingly evident in cyber's integration into the business cycle—a combined 54% of respondents say they have either fully integrated cyber into their broader business and technology strategy plans or are actively building cyber requirements into their forward-looking strategy.

There are plenty of reasons respondents have earned their confidence. But are some more confident than they should be?

## Top Contributors to Organization Cyber Confidence

Q. Which of the following contributes most to your organization's cyber confidence today?




Total (n=1,058)

PARADOX #1

# There is still concern that organizations may not be ready for future threats

**To determine respondents' cyber readiness, they were presented with a list of cybersecurity-related actions and asked to what extent those actions have been implemented in their organizations.**

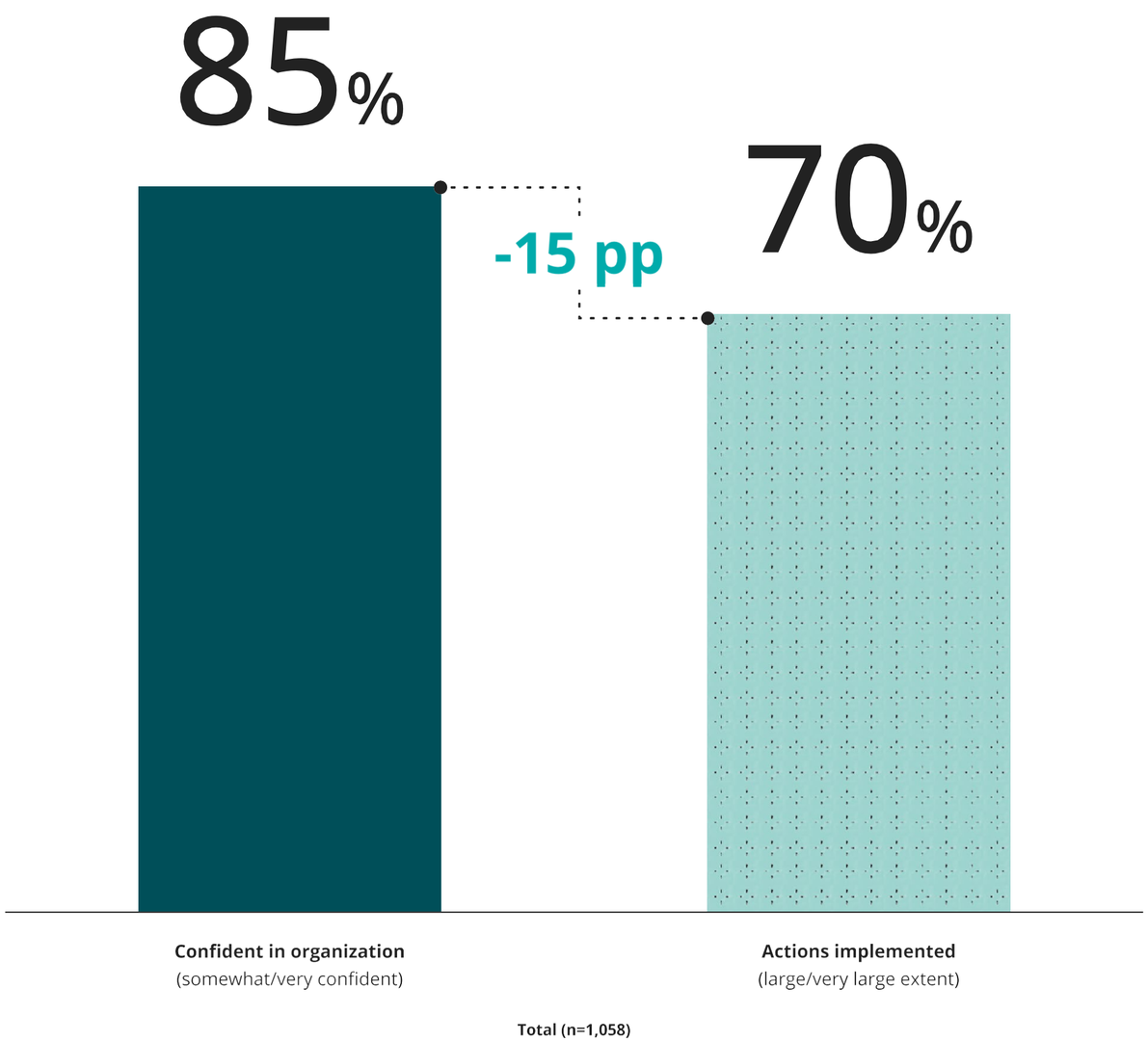
On average, 70% of respondents had implemented all of them to a very large or large extent, indicating a high level of readiness. When this is compared to survey data that measures their confidence in having cybersecurity strategies in place, a notable gap is revealed: On average, respondents report that they are 15 percentage points more cyber confident than cyber ready.

"We get the right level of investment, we get the leadership engagement we need, and we have the right tools and processes," says a CISO at a healthcare company. "But as with any large organization, it's one thing to be confident in your ability to understand the inherent risk and threat environment. It's another thing to be able to say universally that we've got every 'i' dotted and every 't' crossed such that there's no chance that we can have a significant incident."

## Confidence vs implementation gap

**Extent of Implementation in Cybersecurity Related Actions**

Qa. How confident are you that your organization has each of the following cybersecurity strategies in place? (average of all responses)
Qb. To what extent have each of the following cybersecurity related actions been implemented in your organization? (average of all responses)



Respondents have the board-level sponsorship and funding they need. They're confident in the work their organizations have accomplished to date. So why aren't they reporting higher levels of cyber readiness as they prepare for future threats and challenges? Four survey findings in particular offer clues:

### Inadequate business alignment

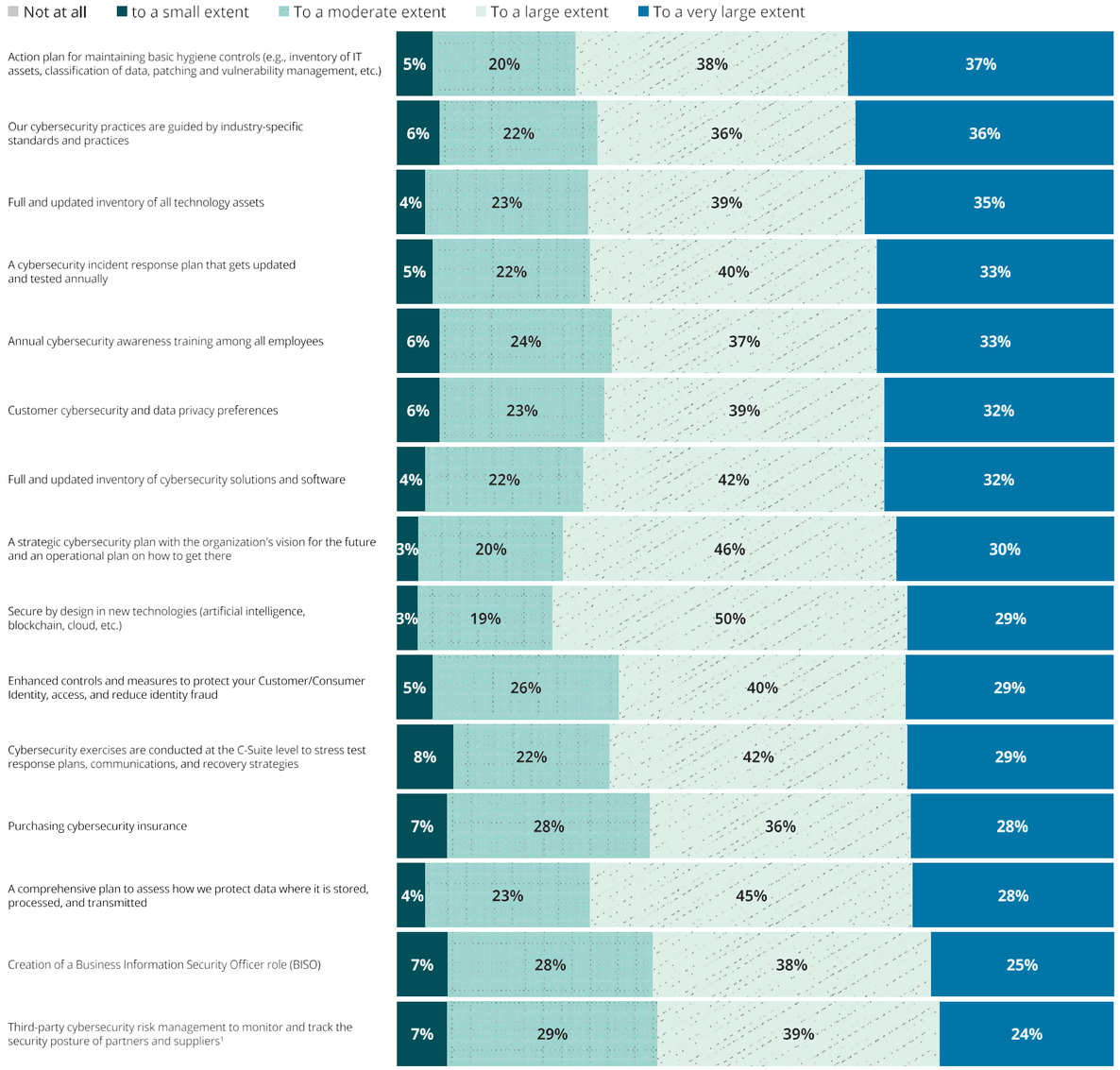
Many respondents report that their organizations have yet to create a Business Information Security Office (BISO) role, which is increasingly recognized as a core feature of mature cyber strategies. Only 63% of respondents have implemented the role to a large/very large extent, suggesting that many organizations do not have the mechanisms in place to connect their business domains to cybersecurity, risk and resilience operations.

### Third-party cyber risk management capabilities remain underused

While respondents report relying on a large and growing number of technology vendors, when asked about the extent to which they've incorporated third-party cybersecurity risk management capabilities to monitor and track the security posture of their organization, they rate it lowest among a long list of other cybersecurity-related actions.  Only 65% of respondents report having implemented these capabilities to a large/very large extent, revealing a potentially significant unmitigated risk.

## Extent of Implementation in Cybersecurity Related Actions

Q1. To what extent have each of the following cybersecurity related actions been implemented in your organization?




1 Note: totals may not add up to 100% due to rounding. This is the reason for the variance and is not an error.

### Skills gaps driving workforce worries

When respondents were asked to rank the top factors limiting their ability to be agile and address cyber issues, the lack of a skilled workforce appears at or near the top of the list. Among those surveyed, the greatest proportion of respondents rank this as their top limiting factor. Out of fifteen potential challenges, 10% of respondents ranked it first, highlighting the importance of workforce skills in ensuring cyber readiness.

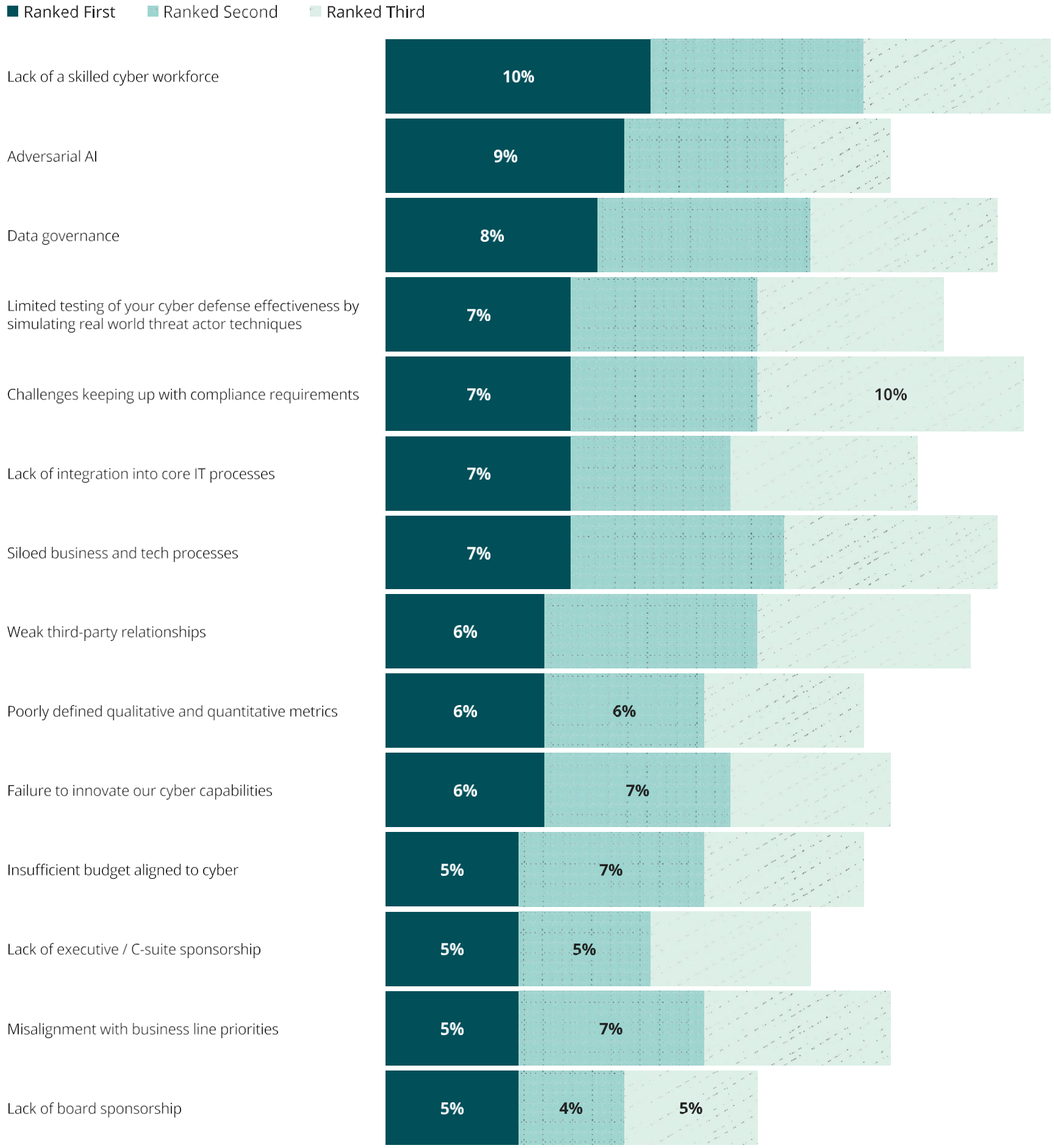
### Evolving threat environment

Adversarial AI occurs when a threat actor targets vulnerabilities in AI systems and/or uses advanced AI techniques to perpetrate their attack. Social engineering, deepfakes, synthetic identity, misinformation, and data poisoning are all examples of adversarial AI, which respondents identify as the second leading factor limiting their ability to be agile when addressing cyber issues. This suggests that respondents are concerned about their ability to adapt to a quickly shifting technology environment and the unpredictable (or unknown) threats AI is likely to introduce, affecting their readiness.

“There are AI systems out there that can morph themselves after you detect them and begin fighting them as a piece of malware,” says the VP, Global Security at a medical technology company. “And then they morph themselves into a different type of malware. Now you’re talking about attacks at scale. We need to respond in an automated way in order to defend against that: If our adversaries stage an agentic AI attack swarm, we need to have an equally sophisticated AI-enabled defense swarm that’s able to learn their attack patterns.”

**Top Limiting Factors to Address Cyber Issues (Ranked First)**

Q. Which of the following most limits your organization’s ability to be agile and adjust to/address cyber issues? Rank the top 3 limiting factors.




Total (n=1,058)

# Unpacking the paradox

**The cyber confidence-readiness gap is perhaps best understood in the context of the journey from strategy and vision to execution. After spending years successfully shoring up executive-level support and funding for cyber initiatives, as well as designing and executing strategy-level cyber planning along with their peers in the business, respondents have yet to push cyber principles, processes, and technologies deeper throughout the organization. They're confident that they can help the organization move forward on cyber issues, but they haven't yet put the mechanisms in place that they know are required to ensure readiness.**

What are the next steps for leaders seeking to translate strategy-level successes into front-line execution? Both our survey findings and in-depth interviews with respondents, especially those who rank high in both confidence and readiness, point to several critical milestones.

### Consider putting BISOs on the agenda

BISOs can function as the liaison between cybersecurity functions and the business. For organizations looking to turn smart cyber strategies into business-level execution, there may be no more important role. In fact, many organizations report embedding security architects and BISO roles to stay closely aligned with product, DevOps, and architecture teams. Given the previous focus on strategy, it should perhaps not be surprising that to date, less attention has been paid to BISOs.

The BISO role may not be a good fit for all organizations, although achieving tight integration between the business and technology processes and functions is relevant for all. Smaller organizations (or those that are highly centralized) may be better positioned to use alternatives such as agile pods that include security professionals, rather than create a new role.

### Tap into providers' strategic capabilities

Third parties are often engaged to take on and/or automate the type of tedious, time-intensive work that organizations don't have the resources to handle on their own. As organizations ramp up their capabilities, and these relationships mature, they can evolve into even more valuable, strategy-based engagements. Third parties are a critical part of a strong cyber posture.

### On emerging threats, find the balance between concern and actual risk

While respondents' concerns about adversarial AI appear to be high in the survey, Deloitte's client experience suggests that these worries may be inflated relative to the actual risks posed today. In our interviews with select respondents, they indicated apprehension over the relatively unknown nature of adversarial AI. While they have experience addressing "known unknowns," they are understandably less comfortable facing "*unknown* unknowns."

Adversarial AI warrants care and attention from leaders with cyber responsibilities, but focusing on known, addressable challenges such as unintended data exposure and misuse of sensitive data in GenAI environments may have a greater impact today. Don't let fear overwhelm reason in addressing adversarial AI—instead, investigate it further to understand what level of investment is justified while maintaining a steady focus on other, more immediate challenges.

> "**We get the right level of investment, we get the leadership engagement we need, and we have the right tools and processes.** But as with any large organization, it's one thing to be confident in your ability to understand the inherent risk and threat environment. It's another thing to be able to say universally that we've got every 'i' dotted and every 't' crossed such that there's no chance that we can have a significant incident."
>
> **— CISO, Healthcare**

PARADOX #2

# **The executive team believes in and prioritizes cyber strategy.** Cyber doesn’t have the same level of influence elsewhere.

# Top business leadership is on board

**Cyber is a clear priority for businesses—at the highest levels. This was a key finding in our previous survey, and our latest data shows continued strength in executive level sponsorship of cyber priorities.**

Frontrunners set themselves apart by having CISOs with strong relationships at the very top: the overall C-suite, CEO, and the board (>90%). In comparison, CISOs in Follower organizations are reported to have strong relationships with the board and CIO (80% each). Among Foundation Builders, CISOs have the strongest relationships with CIOs (72%).

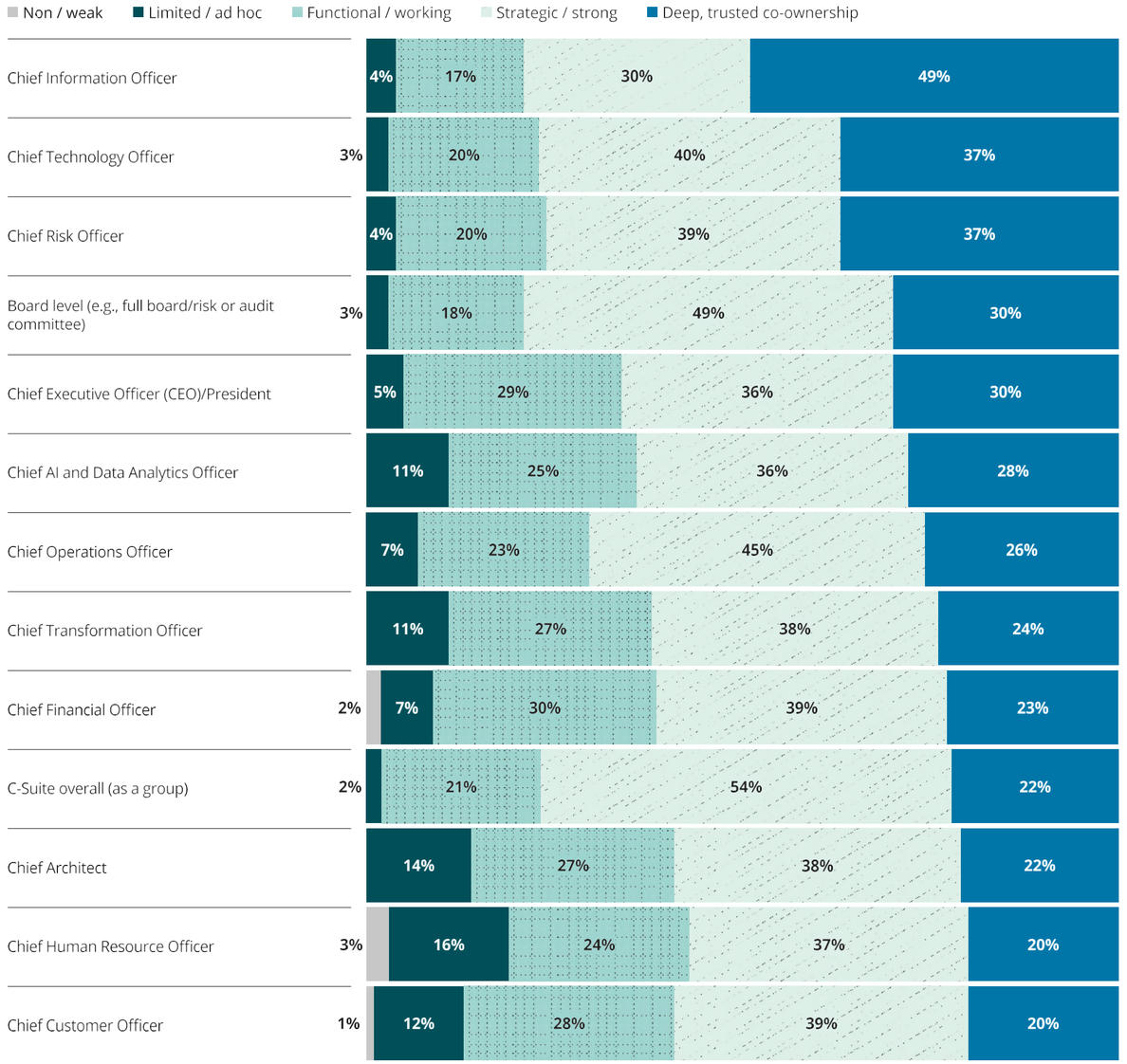
This year, cyber continues to be a C-suite business priority. Most respondents say their organization's CISO has a strong relationship with the CEO (66%), and even more (76%) say the same for the C-suite overall—key elements for ensuring an organization's readiness to meet future cyber challenges.

The majority of CISOs report to the CEO (28%) or CIO (33%), giving them a direct line to the executive leadership team. The greatest proportion of respondents say they have either fully integrated cyber into their broader business and technology strategy plans or are actively building cyber requirements into their forward-looking strategy (54%). Frontrunners are significantly more likely to have cyber as the co-owner or driver of strategy and budget for both the core IT stack (61%) and core business strategy (57%) compared to Followers (43% and 29% respectively) and Foundation Builders (31% and 15% respectively).

While cyber initiatives enjoy widespread support at the top levels of their organization, respondents struggle to expand their reach into everyday execution-level processes and decision making.

**Relationship Strength Between CISO and Other Business Leaders**

Q. Thinking about your organization's CISO (or equivalent security leader), how strong is their working relationship with each of the following?




**Total (n=1,039)***

*Excludes don't know

# Cyber influence has yet to expand from vision to execution

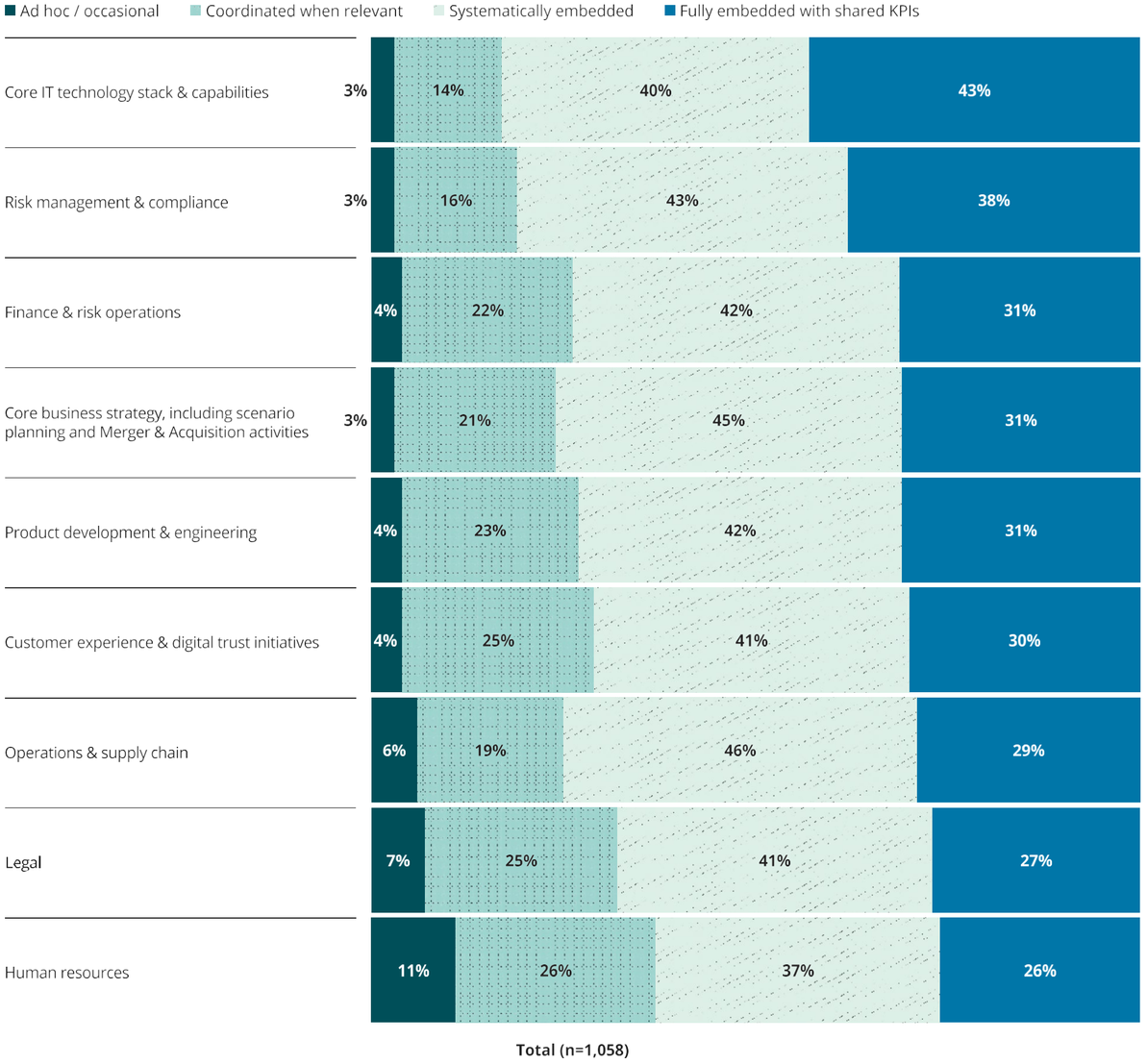
**While there is generally strong cyber alignment within the C-suite, the next step for many organizations is the systemic integration of cyber into critical business unit and technology functions.**

Business-line execution is one key factor in the successful deployment of cyber strategies. Respondents indicated that among nine domains, cyber had the most influence on strategy and processes related to core IT and risk management. In both areas, more than 80% of respondents say that key indicators of strong alignment between business and cyber practices are in place. Outside of this sphere of influence, cyber has less of an impact on core business strategy and other functions. Meanwhile, the majority of Frontrunners say their organizations are fully integrating cyber into their broader strategy. They are also significantly more likely to have all the mechanisms in place to connect cyber to business strategy, especially in enterprise risk management strategy (96%).

"The CISO's goal is to be able to make the shift from being very tactical and technical to being more aligned with the business through a new methodology," says the Group CISO at a financial services company. "That new methodology should allow them to conduct threat modeling and risk assessment on the business revenue value chains, which is what really matters to business leaders."

**Extent Organization Connects Cyber to Other Domains**

Q. To what extent is your organization connecting cyber to each of the following domains in planning and day-to-day decision-making?




**Total (n=1,058)**

Additionally, cyber has yet to significantly influence technological product development. While DevSecOps has achieved peak maturity, and 78% of respondents say that cyber leaders in their organizations are formally integrated into DevSecOps practices, only 40% believe there's true joint ownership with shared key indicators. Frontrunners significantly outpace Followers in having tighter joint ownership across DevSecOps by 22 percentage points (61% versus 39%), as well as across solution design & threat modeling (52% versus 26% of Followers) and tech stack guardrails (51% versus 28% of Followers).

This could be the result of cyber's current lack of influence with leaders who "own" organizational control mechanisms, such as the CTO and Chief Architect. These are important strategic relationships that hold the keys to driving deeper integration into product engineering, application design, and security functions.

Today, CISOs don't have the reporting structures and relationships in place to address this lack of influence. For example, by looking at reporting lines, we can get a sense of relationship strength. Only 37% of CISOs have a deep and trusted relationship with the CTO, despite the CTO being a critical partner for technology development and execution. Similarly, just 22% report a deep, trusted relationship with the Chief Architect—the role responsible for shaping the organization's future technical foundation. These findings echo and reinforce the vision-to-implementation gap identified in the previous confidence-readiness paradox.

> "The CISO's goal is to be able to make the shift **from being very tactical and technical to being more aligned with the business** through a new methodology. That new methodology should allow them to conduct threat modeling and risk assessment on the business revenue value chains, which is what really matters to business leaders."
>
> **— Group CISO, Financial Services**

# Unpacking the paradox

**Cyber initiatives enjoy widespread support at the top levels. At the same time, cyber is less integrated with core business functions that expand their reach into everyday execution-level processes and decision making. Here are some of the most important steps for shifting this dynamic:**

## Get cyber at every table

Most organizations have a cyber foundation. For example, DevSecOps principles and processes are widely adopted. But for cyber to be truly embedded into technology architectures, systems need to be architected with true co-ownership and shared performance indicators across engineering and security leaders. That's the promise of secure by design approaches, which incorporate security principles into systems from the start. Implementation requires more than a strong cyber posture or a checkbox mentality, however. Enterprise architecture with embedded security principles requires the organization to shift from a "following the process" mindset to working toward shared outcomes such as engineering for agility and resilience. To accomplish all this, cyber needs to be included as part of the process as early as possible, throughout the organization.

## Get serious about the CISO-Chief Architect relationship

Today, CISOs don't have the strong, strategy-level relationships with Chief Architects that are required to drive the integration of cyber principles and practices into product engineering, application design, and technology functionality. As in any relationship, these connections won't strengthen on their own—CISOs need to develop a plan for establishing stronger bonds with these critical stakeholders to ensure that cybersecurity measures are built directly into solutions developed in the future.

"We used to have a centralized enterprise architecture team that reported into the head of technology that got federated out under the last CTO… So we lost some of the momentum there…my team built an architecture security review board…they started it by saying, hey, this is a place where you can come and get advice," says the CISO at a healthcare company.

A stronger CISO-Chief Architect relationship could unlock important benefits for the organization. For example, nearly half of respondents believe that an integration between enterprise architecture and cybersecurity would significantly benefit IT/ops recovery time in both the short and long term. They also identify enhanced threat intelligence and application security as leading benefits. These are all areas requiring buy-in and active support from the Chief Architect.

### Match organizational priorities to their owners

Where do your organization's mission-critical priorities lie today—and which leaders have primary responsibility for managing those priorities? The answers can serve as a practical map to the next most important relationships for CISOs and others with cyber responsibilities. If the organization is activating a new customer-focused strategy, cyber needs to be in the conversation, on everything from customer data issues, customer experience, privacy, and more. These are the core business relationships that can be instrumental in extending cyber's reach beyond strategy and into core business operations. The impact can be significant. Sixty-one percent of CISOs in Frontrunner organizations have joint ownership in the development of IT operating standards. They're also ahead of the pack in delivering advisory support on solution design and threat modeling—52% of Frontrunner CISOs are engaged in these initiatives.

### Step up the soft skills

CISOs and other cyber leaders typically rise to their positions based on their strong technical and strategic capabilities. But their ability to successfully make inroads with other parts of the organization—a key feature of these cyber roles—depends in no small part on so-called "soft skills" that may have been less relevant in their previous positions. Are they good listeners and communicators? Can they establish common ground with colleagues and with other leaders? These skills have a direct impact on their ability to convince others that cyber is a business enabler rather than an inconvenient obstacle.

> "We used to have a centralized enterprise architecture team that reported into the head of technology that got federated out under the last CTO… So we lost some of the momentum there…my team built an architecture security review board…they started it by saying, hey, this is a place where you can come and get advice,"
>
> **— CISO, Healthcare**

PARADOX #3

# **“We want fewer vendors.”**
“We need more vendors.”

# Vendor overload

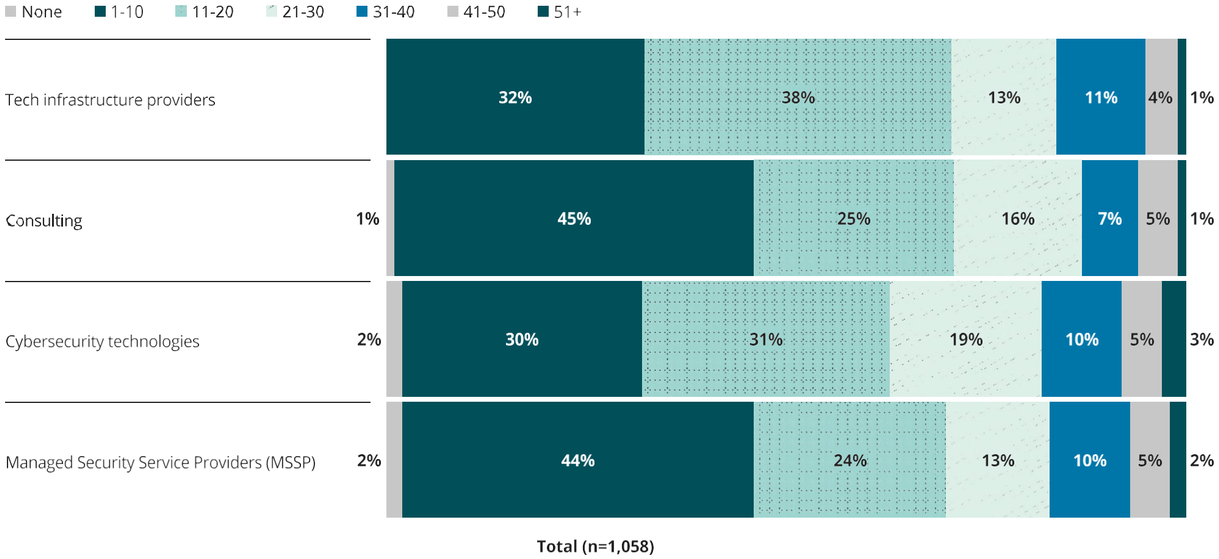
**Ongoing changes in the threat landscape, combined with a constantly evolving set of solutions and technology capabilities, have led cyber professionals to establish relationships with a large and growing number of vendors—with no end in sight.**

Respondents are already working with what appears to be an overwhelming number of vendors to manage—and those numbers are expected to increase in the next three and five years. For tech infrastructure, the greatest proportion (38%) of respondents have 11-20 providers, though 29% have 21 or more.

And while our interviews suggest that many don't necessarily want to increase the number of vendors given growing interest in moving to platforms, there may also be no choice if current technologies don't meet present or future needs. For some organizations, maintaining a large number of vendors (often more than 20) is an intentional strategy for avoiding vendor concentration risk. Even for leaders who would prefer to partner with fewer providers in order to simplify integration and reduce operational complexity, many view consolidation as a path to concentrated risk: A smaller number of players can create single points of failure. There is no one-size-fits-all solution to this dilemma.

**Number of Cyber Partners Across Categories**

Q. How many cyber partners does your organization work with across each of the following categories?




**Total (n=1,058)**

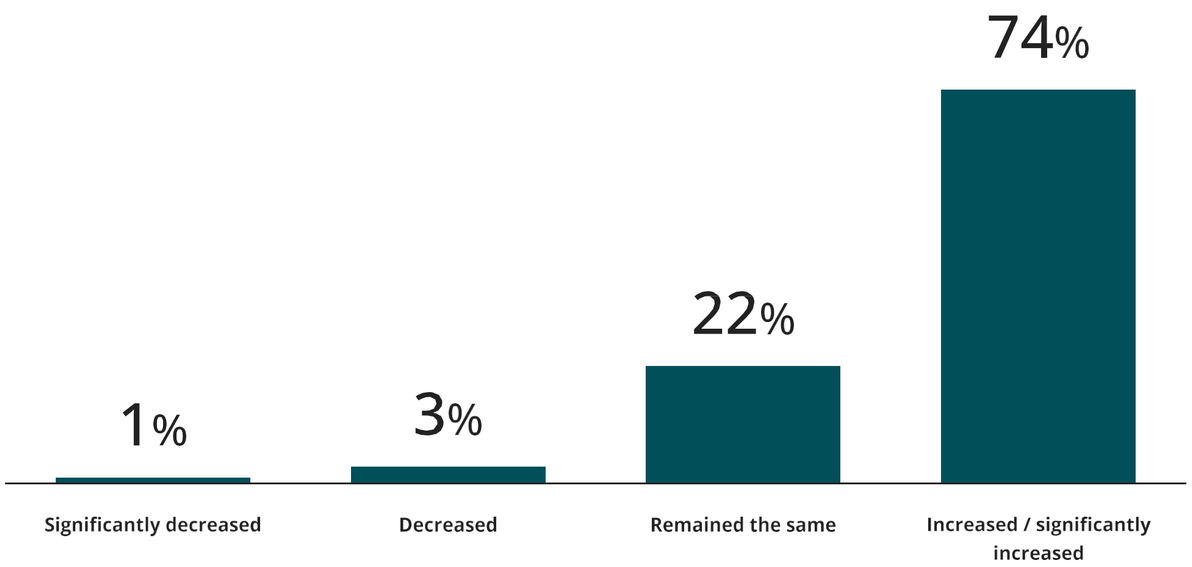
## The vendor portfolio: Large and growing

Despite having large numbers of vendors already in place, survey respondents say vendor totals have increased or significantly increased in the past year, and that they expect to rely on an even greater number of vendors in the next one, three, and five years. Seventy-four percent of respondents say the number of cybersecurity partners their organization works with has increased or significantly increased over the past year.

"We've added new third parties that provide cybersecurity solutions to the firm, and IT has added more partners to manage some of their infrastructure services as well," says the CISO at a financial services company. "It's the same for CIOs—they've also added more solutions and third parties for their application teams." Only 38% expect the number of cyber partners to remain stable over the next year. Most others expect vendors to proliferate in the future: 79% of respondents anticipate the number to increase or significantly increase in the next three years. When respondents are asked about the next five years, this rises to 85%.

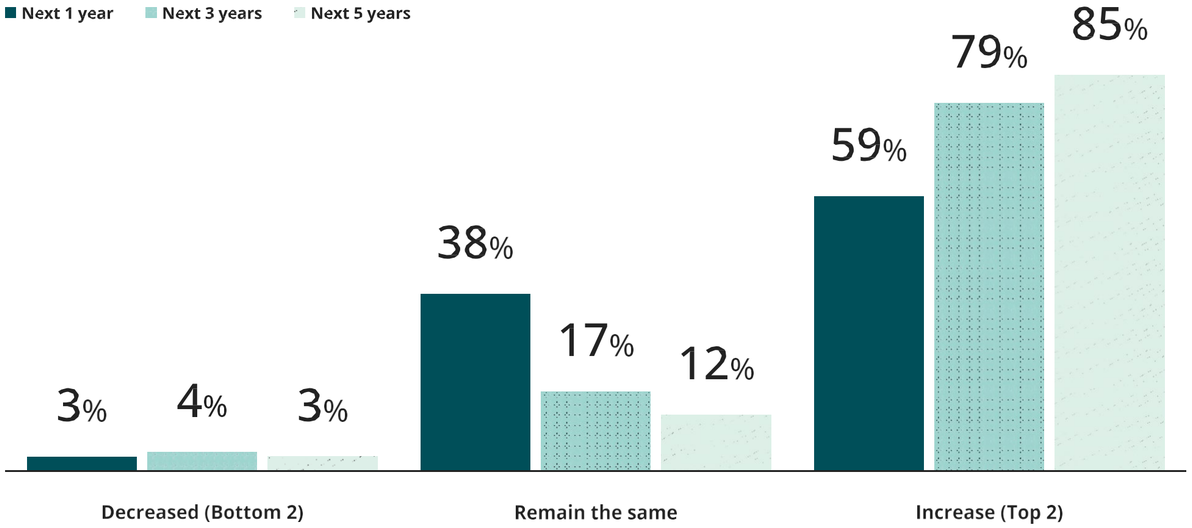
### Change in number of cyber partners in the past year

Q. How has the number of cybersecurity partners your organization works with changed over the past year?




### Anticipated future change in number of cyber partners

Q. And how do you anticipate this changing in the next 1, 3, and 5 years?




Total (n=1,058)

# What’s driving this growth?

**New vendors are being sought out due to AI**

While organizations already have many vendors, one reason they may enter into new strategic relationships is to bring in new technical capabilities or to address emerging risks. AI has been a strong driver of cyber capability upgrades over the past year, with a strong majority of respondents (nearly 75%) updating existing cyber programs to incorporate advanced reasoning capabilities for real-time threat analysis and digital infrastructure monitoring. Seventy-six percent of respondents specified they were engaging cybersecurity vendors that incorporate AI into their services.

**Cyber is not well integrated into the tech stack**

Today, only approximately 30% of respondents believe cyber is highly integrated into the tech stack. This data suggests that redundant architecture patterns may be in place, creating an opportunity for vendor rationalization and consolidation through a more streamlined enterprise architecture. Survey respondents indicate that organizations may be moving in that direction over the next 12-24 months, with integration levels expected to increase by 8 percentage points. We see this same pattern emerging with the move toward more integrated cyber platforms as a mechanism to streamline (and potentially reduce) the vendor ecosystem.

> “**We’ve added new third parties that provide cybersecurity solutions to the firm**, and IT has added more partners to manage some of their infrastructure services as well. It’s the same for CIOs—they’ve also added more solutions and third parties for their application teams.”
>
> **— Group CISO, Financial Services**

# Respondents report 5X growth in moving toward integrated cyber platforms, from 2024 to 2026.

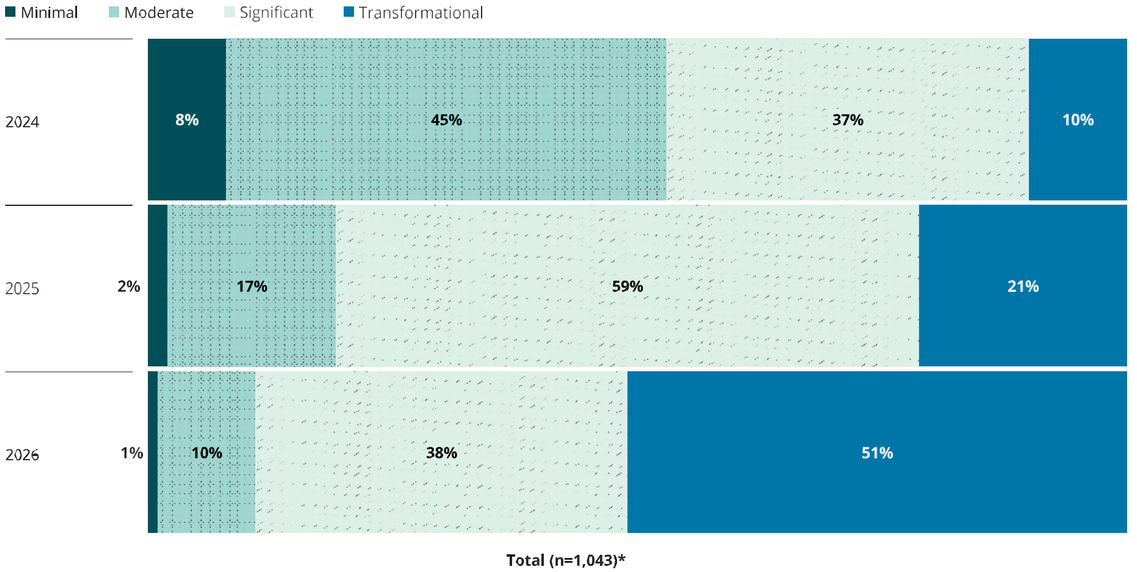
**In our previous survey (2024), only 10% of respondents said their organizations were driving toward integrated cyber platforms in a transformational way. In 2025, that percentage more than doubled to 21%—and 51% of respondents expect these integrated platforms to be transformational in 2026, reflecting a significant momentum shift in the direction of integrated platforms. Among Frontrunners, this shift is even more pronounced: 64% reported a significant/transformational move in 2024, and 94% expect the same in 2026.**

What accounts for this shift in momentum toward consolidated cyber platforms? Traditional drivers such as reduced complexity and lower total cost of ownership are likely behind these decisions—some companies would rather move to a single "good-enough" platform rather than manage a collection of best-in-class providers of niche services.

Other drivers may be at work here too, starting with AI. Cyber and technology leaders alike know that AI requires consistent, normalized data to be effective, and platforms are well positioned to deliver it. For those pursuing agentic AI strategies, these platforms typically offer the standardized data models required to build agentic workflows.

**Extent Organization is Driving Towards Integrated Platforms for Cyber Activities**

Q. To what extent is your organization driving towards an integrated platform for your cyber activities in the past year, this year, in the next year?




**Total (n=1,043)***

*Excludes don't know

# Unpacking the paradox

**Is vendor proliferation inevitable? It may seem that way today, as the threat environment remains fluid and new tools and capabilities are required to address those threats quickly. Equipped with ample budgets and executive support, respondents simply keep adding to their arsenal of providers.**

In this context, it's easy to understand the growing appeal of platforms—especially those that require less overhead to administer, incorporate many of the same tools and capabilities offered by niche providers, and are capable of integrating different technologies at a lower total cost of ownership.

As organizations seek to gain control over vendor proliferation fueled by AI and poorly integrated architectures, here are some of the actions they should consider today:

### Assess vendors to identify their real value—and their untapped potential

Vendors are a critical component of any organization's cyber strategy today. Does your organization have a clear, up-to-date understanding of exactly how they're serving the organization today, where different vendors may have overlapping capabilities, or where they could be providing additional value? It's virtually impossible to know without having a structured approach to vendor assessment that is strategic, intentional, risk-based, and disciplined.

### Use enterprise architecture principles to assess mission-critical vendors versus redundancies

While organizations may have added new vendors to address immediate risks across different business lines and geographies over time, that can also lead to redundancies. AI is just one recent example of well-meaning vendor expansion. Organizations can get a handle on which vendors are mission-critical and where they may be able to consolidate by working closely with enterprise architecture teams, flagging redundant capabilities, and looking for opportunities to rationalize, integrate, and consolidate.

### Look beyond the cost and efficiency benefits of platforms

Platform growth is being driven by a number of factors including cost and efficiency, AI enablement, data transformation, and agentic workflow reimagination. At a moment when interest in agentic AI is surging, platforms can deliver standards, controls, and integration capabilities as well as support vendor consolidation and optimization strategies.

PARADOX #4

# **Cyber breaches remain steady and persistent.**
Their business impact is contained.

# Cyber breaches are here to stay

**Respondents continue to report a high number of incidents. Seventy-eight percent publicly reported at least one breach in 2025, compared to 91% in 2024. Nearly a third reported 6-10 breaches in 2025, compared to 40% in 2024. While the number of reported breaches decreased year over year, it continues to be on the higher side.**

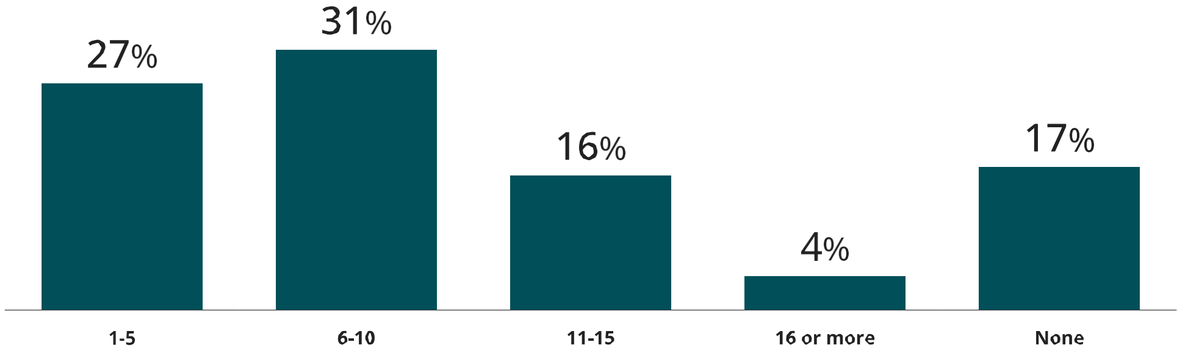
We can also assume that some cyber breaches go unreported, especially among organizations that may not have the capabilities in place to identify and report such incidents.

Respondents are concerned about a familiar group of threat actors, starting with cybersecurity criminals (30%), cybersecurity terrorists (15%), and hacktivists (10%). The tools and technologies these threat actors use are equally familiar: Ransomware (20%), malware (15%), and data exfiltration (14%) are once again top concerns. However, this year's findings reveal a notable new entrant: The misuse of AI is now tied for fourth place as a new area of concern.

> "**Compromises of systems, applications, and environments will happen.** If you try to prevent every compromise, it's going to be very hard to get business done in the company. The goal is to build your program so that if a system is compromised, you see it as quickly as possible—immediately contain it and eradicate it before it has a bigger impact."
>
> **— Global CIO, Healthcare**

## Publicly Reported Security Breaches*

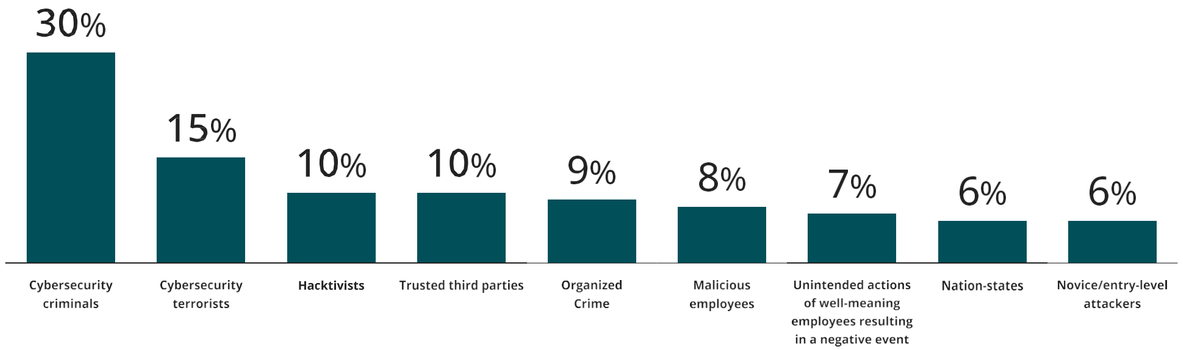
Q. In the last year, how many cybersecurity breaches has your organization publicly reported?




* Note: Does not total 100% given 5% of respondents are private companies that do not have a public reporting obligation.

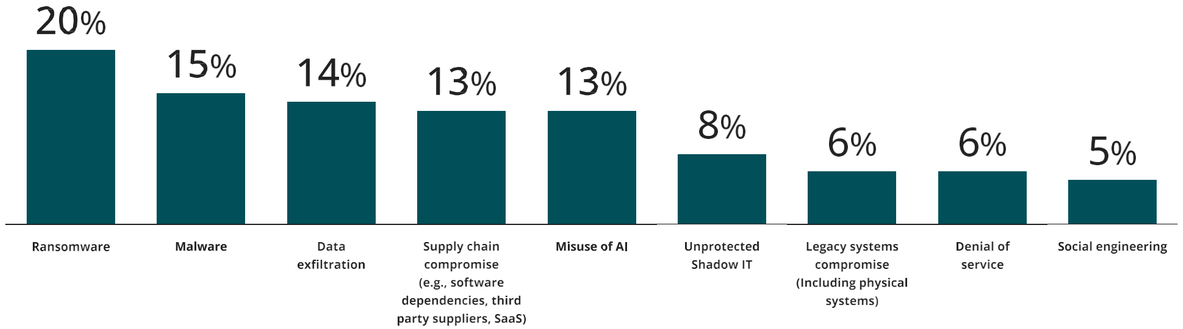
## Most Concerning Cybersecurity Threat Source - Actors / Sources

Q. What is the single biggest cybersecurity threat source that your organization is most concerned about?




## Most Concerning Cybersecurity Threat Source - Tools / Techniques

Q. What is the single biggest cybersecurity threat source that your organization is most concerned about?




Total (n=1,058)

# Businesses have so far successfully minimized the impact of breaches

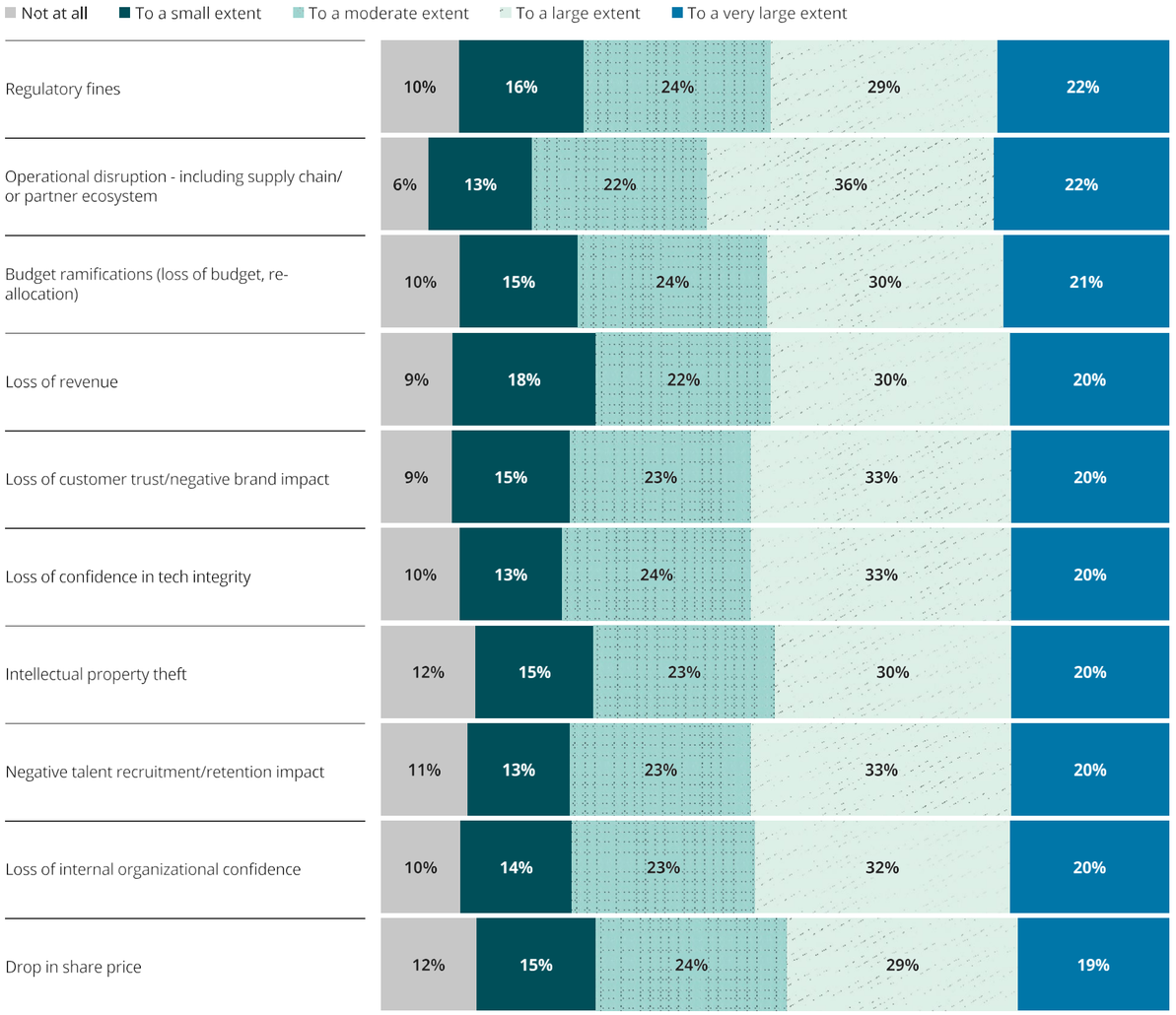
**Despite the significant number of cyber breaches, on average 52% of respondents say that negative consequences have to a large/very large extent affected their organizations due to cybersecurity incidents across a range of potential impacts. Last year, this figure was 64%.**

That's not to downplay the impact. Operational disruption is the leading consequence of cybersecurity incidents, with 58% saying their organizations suffered large/very large disruptions in operations, affecting their supply chains and partner ecosystems. A year ago however, the same impact was felt by 66% of respondents, suggesting that organizations have gotten better at managing negative consequences. "Compromises of systems, applications, and environments will happen," says the Global CIO at a healthcare company. "If you try to prevent every compromise, it's going to be very hard to get business done in the company. The goal is to build your program so that if a system is compromised, you see it as quickly as possible—immediately contain it and eradicate it before it has a bigger impact."

Frontrunners especially reflect this pattern. Mature threat intelligence may allow them to report higher numbers of breaches than their peers. Twenty-six percent of Frontrunners reported 11+ cyber breaches in the last year, versus 19% of Followers, and 20% of Foundation Builders. Despite reporting more incidents, Frontrunners are equally likely to report negative consequences from cyber incidents as Followers.

**Extent Organization has Suffered Consequences from Cybersecurity Incidents / Breaches**

Q. To what extent has your organization suffered negative consequences in each of the following areas due to cybersecurity incidents or breaches?




**Total (n=823)***

*Excludes don't know

# Unpacking the paradox

*Something* is working. That's the most obvious conclusion to be reached from this positive paradox. Against a rising tide of threats, respondents have been able to successfully contain the negative consequences associated with a cyber incident.

But they can't afford to be lulled into complacency by their success. Here are some practical ways to help extend this encouraging trend:

### Increasing reports of breaches? Don't overcorrect

An increase in the number of reported breaches can in fact reflect strong cyber practices, showing that healthy threat detection and response capabilities are in place and being followed. In either case, closer analysis is warranted. Breach volume alone is not a useful indicator without insights into what is being detected, how quickly it is being detected, and what impact the breaches are likely to have on the business.

Consider focusing less on breach counts, and more on patterns and outcomes. Is an increase in breaches driven by faster detection of many low-impact incidents? That can be a positive sign pointing to improving maturity. Is the increase tied to recurring attack paths, prolonged dwell time, or operational disruption? Without this type of context, leaders risk overcorrecting through unnecessary controls—or underestimating their exposure to pressing risks.

### Low reports of breaches? Look closer

Similarly, if your organization isn't reporting breaches, this could be a good sign—or it could be the symptom of an insufficient ability to detect them. As a result, your organization may not have sufficient monitoring and analytics capabilities in place to identify malicious activities and breaches, and could still be susceptible to dormant sleeper attacks.

### Relentlessly pursue resilience

Sixty-seven percent of respondents are proactively pursuing scenario-planning exercises to link cyber to business strategy—one key element (among many) for building resilience. These exercises also help clarify the value of cyber to the organization. Is it primarily a revenue driver? Revenue protector? Or is it focused on avoiding disruptions and the costs they incur? Scenario planning should unfold at a pace that matches the rapid evolution of the threats the organization faces.

PARADOX #5

# **Year-to-year cyber budgets are stable.**
The cyber environment is wildly unstable.

# Steady, stable, supported spending

**Respondents who can make the business case for investment are likely to secure the funding they need.**

"When there's a good, well-thought-out justification and solid business case, it's usually going to get funded," says the Global CIO at a healthcare company. Cybersecurity budgets are expected to increase incrementally over the next year, with few significant changes in distribution across business priorities—perhaps due to planned multi-year investments and shared ownership across business, IT, and risk management functions. Frontrunners investing in cyber initiatives are far more likely than peers to expect tangible business outcomes, especially in these areas:

- Efficiency, agility, and strategy
- Trust, confidence, and resiliency
- Customer value

More than 90% of Frontrunners anticipate gains in each area.

A strong majority of respondents (85%) report that they've increased cyber budgets year over year—and even more (88%) plan to increase their budgets over the next 12 months. For some, these increases are significant: Eight percent of respondents expect 12-month spending levels to increase by more than 25%, and more than a third anticipate increases between 10-25% of their organizations' total cyber budget today, including IT, business, enterprise risk, and other sources.

Notably, respondents anticipate budget sources[1] to remain relatively stable over the next 12-24 months, focusing on:

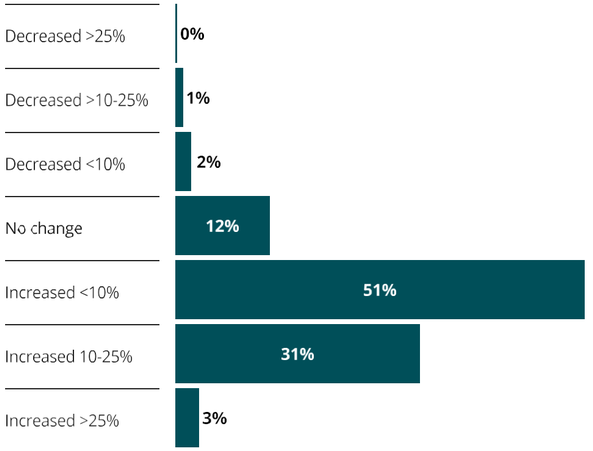
| CENTRAL IT BUDGET | BUSINESS | ENTERPRISE RISK |
|---|---|---|
| 43% | 30% | 26% |

[1] Note: totals may not add up to 100% due to rounding. Also, the remaining share pertains to 'Others'.

## Organization Cybersecurity Budget

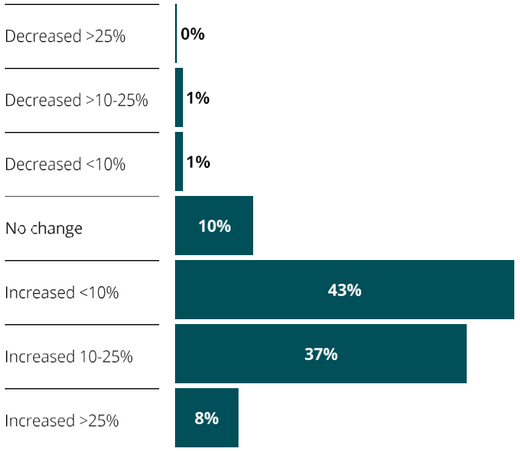
Qa. Compared to last fiscal year, how much did your organization's total cyber budget (including IT and any other sources) change?
Qb. Thinking about next the next 12 months, you expect your organization's cyber budget (including IT and any other sources) to...

### Change vs Previous Year




**Total (n=1,058)**

### Expected Change in Next 12 Months




**Total (n=1,058)**

Nearly all of those we surveyed have budgeted for multi-year cyber investments—only 7% don't, instead focusing on a single-year cycle. "Our programs tend to be 2-3 years, but budgets go year by year," says the Global CIO at a healthcare company. "I have long-term aspirations, and the programs might be long-term, but the budgets are still getting set every year."

Of the multi-year plans, the majority proportion of the cyber budget (61%) extends for 1-2 years:

**One year beyond current cycle:**

**35% of cyber budget**

**Two years beyond current cycle:**

**26% of cyber budget**

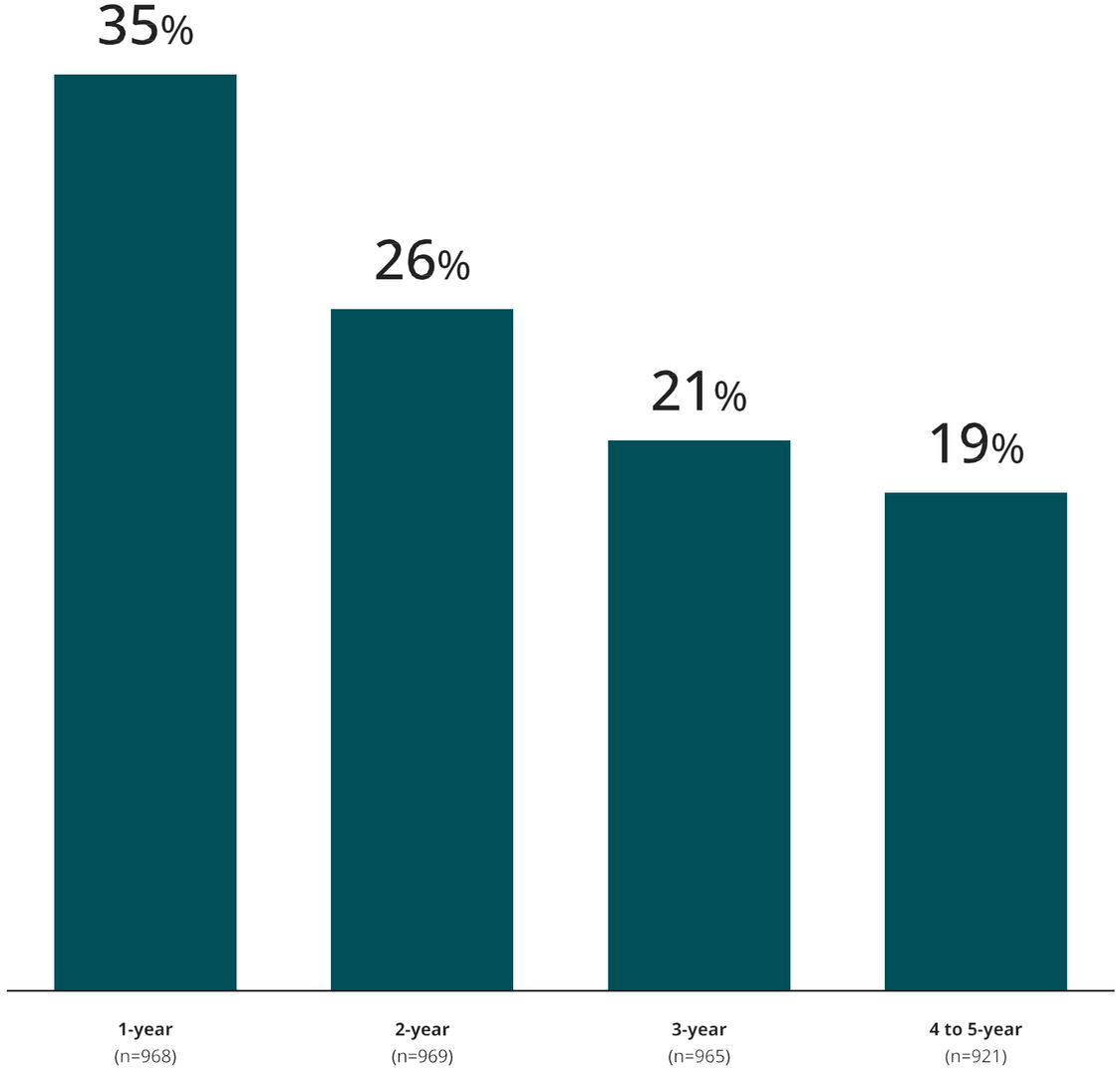
Nineteen percent of the cyber budget is allocated to multi-year investments over the next 4–5 years.

Program-level priorities aren't shifting significantly, and neither are spend categories. In fact, survey respondents indicate that their current budget allocations will be identical in the following year, with threat detection and response in the lead at 20%. After that, infrastructure security, data/identity/application security, and strategy/governance/compliance are the leading spending categories, in that order.

> "When there's a good, well-thought-out justification and solid business case, **it's usually going to get funded.**"
>
> **— Global CIO, Healthcare**

**Cyber Budget Allocation to Multi-Year Investments***

Q. What portion of this year's cyber budget is explicitly tied to multi-year investments?




*Note: excludes those who don't have multi-year investments (n=71)

PARADOX #5

# The cyber landscape is anything but stable and predictable

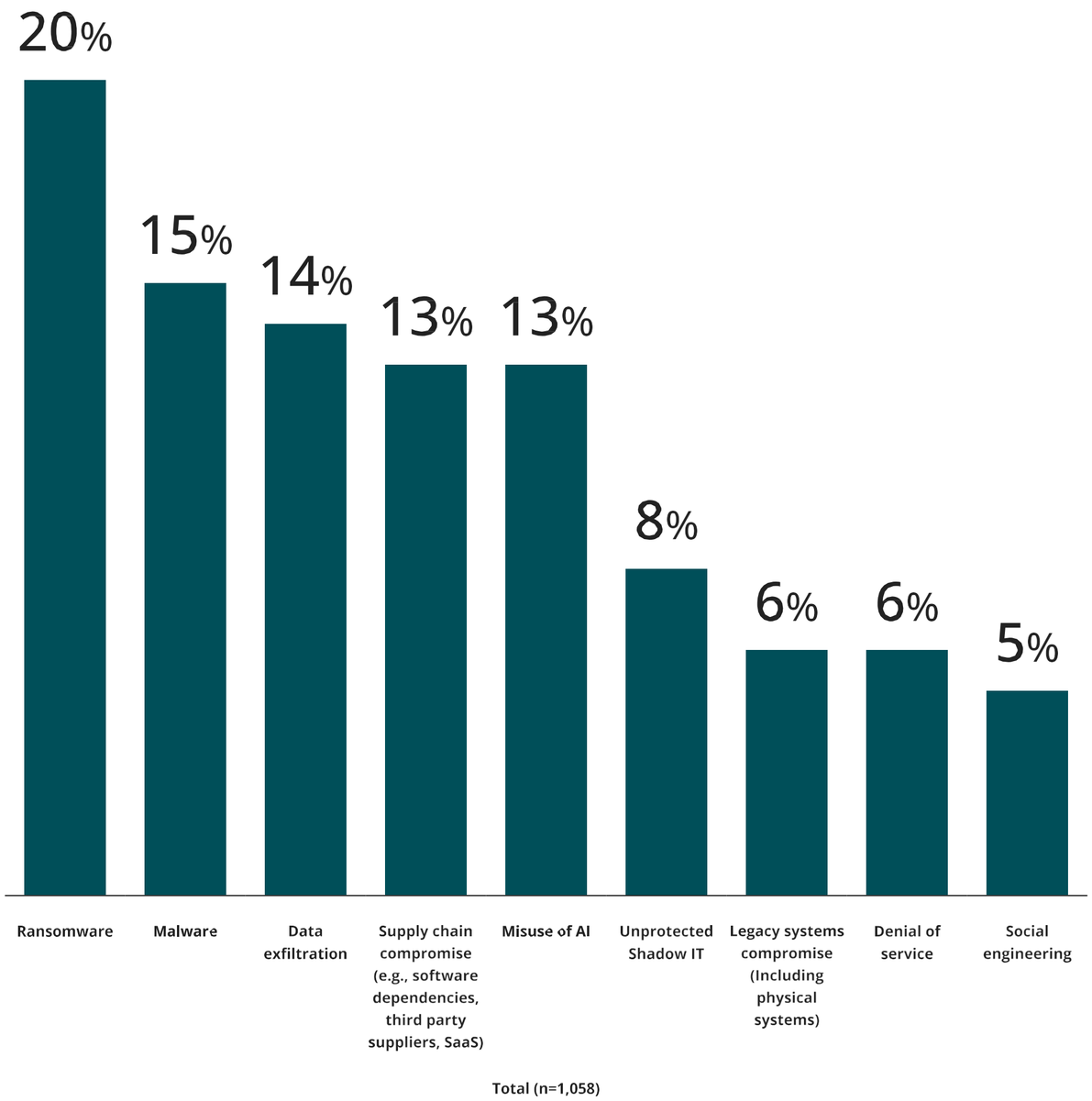
Consider how quickly the cyber landscape has shifted already solely due to one factor: the rapid advance of GenAI capabilities. Only two or three years ago, few were seriously discussing the need to make immediate investments in GenAI capabilities, much less acting on it. Today, almost three quarters (72%) of respondents have incorporated new generative reasoning approaches into their existing AI capabilities across almost a dozen cyber initiatives. This was an unpredictable, largely unplanned development that virtually no static budgets could have accounted for.

Threats are changing, too. “Misuse of AI” was not on the list of threats identified by respondents only three years ago, for example. Now it’s a top five concern, alongside ransomware, malware, and data exfiltration—and it requires new approaches. Applying traditional controls to AI is not sufficient. For example, non-deterministic AI systems require highly specific guardrails to defend against threats such as prompt hacking. This represents a new level of complexity that organizations should be addressing today.

> “**Our programs tend to be 2-3 years, but budgets go year by year.** I have long-term aspirations, and the programs might be long-term, but the budgets are still getting set every year.”
>
> **— Global CIO, Healthcare**

**Most Concerning Cybersecurity Threat Source - Tools / Techniques**

Q. What is the single biggest cybersecurity threat source that your organization is most concerned about?



# Unpacking the paradox

**It's natural for any organization to seek predictability and stability, especially when it comes to budgets.**

It's widely understood that technology budgets overall will need to change significantly due to the quickly shifting nature of technology advances. But even in that context, investments in cyber defenses are different given the profoundly disruptive potential of cyber risks. For example, while AI adoption is widely viewed as a source of greater efficiency and lower costs in most parts of the organization, in cyber environments it could have the opposite effect, as threat actors turn AI to their advantage in new ways. Cyber leaders may be able to optimize their cybersecurity budgets by using AI, but they may also need to ramp up their usage considerably to defend against an array of evolving threats.

How can they accomplish this when they're locked into steady, predictable funding levels (enviable as this scenario may be)?

### Build flexibility into the cyber budget

Think of this as funding the unexpected—preserving 10-20% (for example) of the annual cyber budget to make agile investments in new capabilities as they emerge, or to respond to unpredictable threats as they unfold.

### Rethink multi-year budgeting

What if multi-year budgets are simply too constrictive? Consider adopting rolling forecasts, or continuous budgeting approaches as alternatives to standard multi-year budget strategies.

### Shift the budgeting mindset

Your organization's finance leaders and budget decision makers may not fully appreciate the unique challenges cybersecurity presents to budget planning. If so, it may be time for an organizational mindset shift—an opportunity to brief these leaders on the cyber landscape and develop innovative new approaches to budgeting together. When cyber leaders are able to quantify cyber risks the organization is facing in financial terms, these conversations can gain more urgency and focus. For example, when one part of the organization carries a higher risk profile than others—one with a correspondingly large potential financial impact—a more significant investment in that area may be warranted.

# The upside of paradox

**The paradoxes uncovered in this survey reveal new opportunities: Those who are able to resolve them will put themselves in position to close the gap between vision and execution.**

Many of the conditions required to spark this type of transformational change in cyber strategy and execution are in place today. Those responsible for driving overall strategy understand cyber's importance to achieving the organization's top goals—and they're ready to support cyber strategies with robust funding. Meanwhile, CISOs and other leaders with cybersecurity responsibilities have carefully cultivated the strategies, processes, and structures needed to defend their organizations against a rising tide of cyber threats.

Now is the time to combine all these key elements in a way that creates an even stronger, far-reaching, truly integrated cyber culture mechanism that is ready for future challenges. This will require a change agent—and if you're reading this report, that role likely falls to you. Start by viewing your organization through the lens of the paradoxes we've uncovered here, pinpointing which are most relevant to the organization, and working with your peers to unravel them.

**If you would like a closer look at the details of this research, want to discuss any of the insights in the report, or want to further explore their potential impact on your organization and its goals, we are happy to help.**

## Authors

Diana Kearns-Manolatos
Emily Mossburg
Kelly Nelson
Iram Parveen

## Acknowledgements

Volker Burgers
Evan Carvouni
Jonathan Chan
Tim Corder
Felix De Andres
Miguel Olias De Lima
Jason Frame
Javier Francisco
John Gelinne
Tanneasha Gordon
Rob Jacoby
Jimmy Joseph
Daphne Lucas
Tara Mahoutchian Mortazie
David Mapgaonkar
Jeffrey Minick
Stephanie Montalvo
Will Nelson
Jose Pela Neto
Sean Peasley
Anand Raghawa Prasad
Frank Santucci
Jennifer A. Sullivan

## Contacts

Stéphane Hurtaud
Partner,
Cyber Leader
shurtaud@deloitte.lu
+352 451 454 434

Maxime Verac
Partner,
Cyber Strategy & Transformation
mverac@deloitte.lu
+352 451 454 258

Maurice Schubert
Partner,
Cyber Defense & Resilience
mschubert@deloitte.lu
+352 273 315 256

Laureline Senequier
Partner,
Cyber Governance & Compliance
lsenequier@deloitte.lu
+352 451 454 422

# Methodology

The 5th Edition of the Deloitte Global Future of Cyber survey draws on data from 1,058 business and technology leaders in 43 countries across 5 industries and 23 sectors.

The analysis also draws on executive interviews with 9 C-suite leaders who are knowledgeable about cyber trends.

This year's survey report includes three categories for respondents based on their levels of confidence and readiness:

**Frontrunners** scored highest for being somewhat/very confident for questions related to both cyber confidence and readiness actions, covering issues such as:

- Use of risk quantification tools to measure the impact of cybersecurity investments
- Degree to which they are addressing third-party risks across their digital supply chain
- Development of a cybersecurity incident response plan that gets updated and tested annually
- Alignment between cybersecurity practices and industry-specific standards and practices
- *…and many more*

**Followers** scored on average in the mid-range for these same questions on cyber confidence and readiness.

**Foundation Builders** reflected the lowest confidence and/or readiness levels.

**This cybersecurity confidence and action Index was created by determining how many cybersecurity actions out of 15 a respondent took to a very large extent and how many cybersecurity strategies out of the 8 in which they are very confident.**

# Inadequate business alignment

**Implementation readiness—Q1**

If a respondent was considered to match very large extent/ completely in:

**10-15 actions** .....they were assigned a weight of 3.
**4-9 actions** .....they were assigned a weight of 2.
**0-3 actions** .....they were assigned a weight of 1.

**Confidence—Q2**

If a respondent was considered to match very confident in:

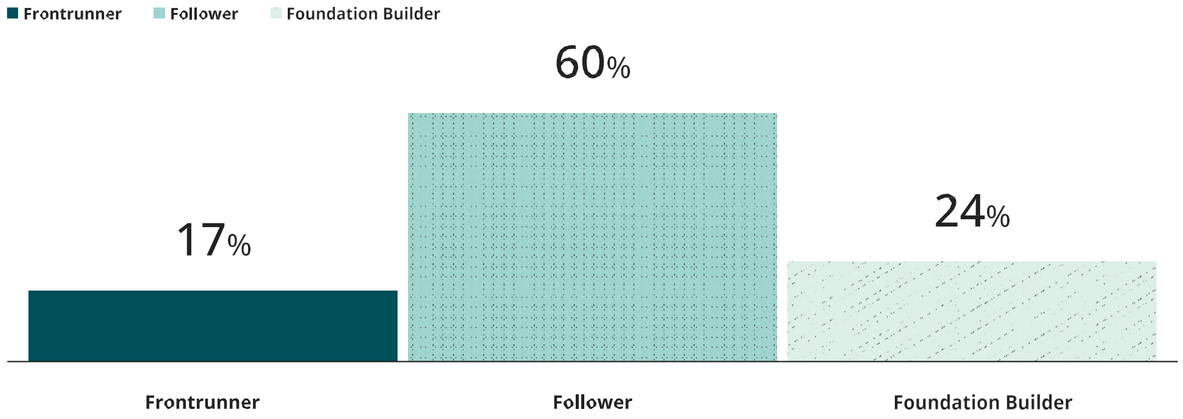
**5-8 strategies** .....they were assigned a weight of 3.
**3-4 strategies** .....they were assigned a weight of 2.
**0-2 strategies** .....they were assigned a weight of 1.

Both weights were added to get a total calculation on confidence and implementation of cybersecurity strategies and actions.

- If a respondent got a total calculation of 5-6, they were classified as a Frontrunner
- If a respondent got a total calculation of 3-4, they were classified as a Follower
- If a respondent got a total calculation of 2, they were classified as a Foundation Builder

**Frontrunners are the respondents who have mastered the first paradox in this report. Their experiences offer valuable insights into the actions organizations can take to successfully address the other paradoxes identified in this report.**

**Confidence and implementation index (% of total)***




*Note: totals may not add up to 100% due to rounding. This is the reason for the variance and is not an error.

| N=1,058 | Frontrunner | Follower | Foundation Builder |
|---|---|---|---|
| Sum of weights for confidence strategies and implementation actions (min: 2, max: 6) | 5-6 | 3-4 | 2 |
| Base size | 176 | 631 | 251 |
| Percentage of total sample | 17% | 60% | 24% |

# Disclaimer