Deloitte.

2023 Global Future of Cyber Survey

Building long-term value by putting cyber at the heart of the business

The answer is cyber

Today, we are seeing the emergence of powerful new attitudes when it comes to cyber. Leaders are looking at cyber through a sharp, new lens—one that reveals the inherent business value that can come by embedding cyber. Not only across the enterprise, but as a crucial part of a powerful growth strategy.

No longer just an obligation or a collection of tech-focused hygiene practices, cyber has grown into a critical function for helping businesses deliver outcomes, and the results of Deloitte's 2023 Future of Cyber Survey illuminate this. This year's global survey—Deloitte's largest cyber survey to date—polled leaders across industries in order to get a clearer picture of where cyber stands and where it is going. What we discovered is that cyber's profile as an enabler is growing. Among organizations of all sizes, cyber is consistently earning a place on the agenda, becoming a focal point for business-critical initiatives and investment.

We are excited about the future of cyber, and I invite you to join us in exploring some of the key findings in this report. In addition to data derived from the survey results, the report also includes observations and insights taken directly from survey respondents, as well as additional Deloitte insights on cyber, cloud, and other technologies enabling the future of business.

Stay well,

Emily Mossburg,
Deloitte Global Cyber Leader

What's inside

Cyber beyond

Building long-term value by putting cyber at the heart of the business

The future of cyber is coming into sharper focus as organizations worldwide begin to look beyond the tech-centric and threat focus toward the potential positive outcomes they can achieve by deeply integrating cyber thinking and cyber actions across their businesses.

The world is increasingly interconnected, bringing about new risks alongside the new growth opportunities. Digital technologies, exponential growth of data, and evolving business needs are expanding attack threat surfaces and bringing new challenges that elevate cyber as a strategic business issue. Collaboration across cyber, risk management, and business units is critical to neutralizing cyberthreats, protecting business value, and sustaining customer trust.

In recent years, many enterprise leaders were focusing on the continued transition to digital business processes, as well as their technology environments and the rapid evolution of the cyber threat landscape. In fact, managing hybrid IT and digital transformation have emerged as two of the greatest challenges businesses face—solidifying complexity as the new norm for the enterprise.[1]

Today, a new reality is taking shape, based on Deloitte's 2023 Global Future of Cyber Survey, which asked hundreds of leaders across industries and across the globe to share their views on cyber threats, enterprise activities, and the future. The survey included C-suite executives across the enterprise, as well as other senior leaders with responsibility for IT, security, and risk. This new reality is grounded by the following findings.

Cyber is evolving into a distinct functional area of the business, transcending its traditional IT roots and becoming an essential part of the framework for delivering business outcomes.

Relationship transformation

"We're starting to see a far more significant focus on cybersecurity as an enterprise business risk. Across the organization, there is a significant shift in partnership in viewing cybersecurity as a core ingredient of our transformation and not a side garnish or afterthought. We're doing a lot in terms of embedding cyber—whether it's DevSecOps or in product development—where we're starting to co-create with the (internal) partners to make sure that we're building things securely. It's like cultural transformation."

—Allan Cockriel, Group CIO/CISO, Shell

Organizations increasingly recognize the role cyber plays in enabling broad business success.

Looking ahead to 2023 and beyond, cyber is growing far beyond its technology roots. For many organizations, cyber now weaves more tightly into business operations, outcomes, and opportunities. Cyber is more than technology-focused. It is foundational. Among cyber decision-makers across an organization, it has become part of the structure of the business, an embedded element for supporting business ambitions.

Just as cyber threats shifted from an IT problem to a business problem, we also now see a shift in cyber strategies from IT to the business—ultimately to support strategic business objectives and growth. Cyber as a business priority is becoming more evident at the board level. In this year's survey, 70% of respondents reported that cyber was on their board's agenda on a regular basis, either monthly or quarterly. This clearly demonstrates that cyber has earned an important seat at the table where high-level, strategic business decisions are made.

Organizations increasingly recognize the role cyber plays in enabling broad business success.

An overwhelming majority of survey respondents identified a strong connection between cyber and business impact—with 86% reporting that cyber initiatives made a significant, positive contribution on at least one key business priority. And most organizations are looking to build on that value proposition, with 58% planning to increase their cyber investment in the next year.

70%

Reported that cyber was on their board's agenda on a regular basis, either monthly or quarterly.

Savvy boards

"Boards clearly care about cybersecurity, and they will allocate resources at an impressive level. Boards are now educated enough to identify where is their competent security leadership and where is someone who's buying their way out of the problem. And as they recognize the difference, it's going to change the senior executives' and board's tolerance."

—CISO, Consumer Organization

Despite cyber's potential as a business enabler, the ability to leverage it effectively can be inconsistent across organizations. Some organizations have emerged as clear leaders, defining a path to value for others to follow.

As part of this year's survey, Deloitte identified high-performing, cyber-mature organizations based on their level of cyber planning, their engagement on cyber at the board level, and the level of strategic action they have taken on cyber. These organizations are fully implementing actions that are important for cyber hygiene, including: an operational and strategic plan, an action plan to continuously improve the organization's information security, and a cyber risk program to monitor and track the security posture of partners and suppliers.

These organizations, especially, are making the connection between cyber efforts and business value. They are more likely to report that cyber initiatives made a positive impact to a large extent on:

- Brand reputation
- Customer and digital trust
- Operational stability, including the supply chain and partner ecosystem
- Revenue

Organizations with high cyber maturity also are more likely to report that cyber brings value to key business strategies—providing the organization with confidence to try new things, increasing business agility, and enabling efficiency. And they are more likely to report seeing very high value from the third-party cyber services that they engage.

Moving the business forward
"Projects, initiatives, business objectives can't be met without thinking through information security and privacy impacts, and having that embedded into the appropriate processes. We're brought in during the ideation phase as it relates to business components and aspects. Our strategy is 100% focused on supporting the business, recognizing that cyber and privacy do not exist without the business. We want to ensure that we are meaningfully contributing to moving the business forward, driving growth, and doing so in a manner that's compliant and secure."

—Arno Van Der Walt, SVP and CISO, Marriott

54%

Companies with US$5 billion or more in revenue are spending more than US$250 million annually on cyber

71%

Companies with US$500 million to US$5 billion in revenue are spending less than US$250 million annually on cyber

How we developed the insights

Methodology

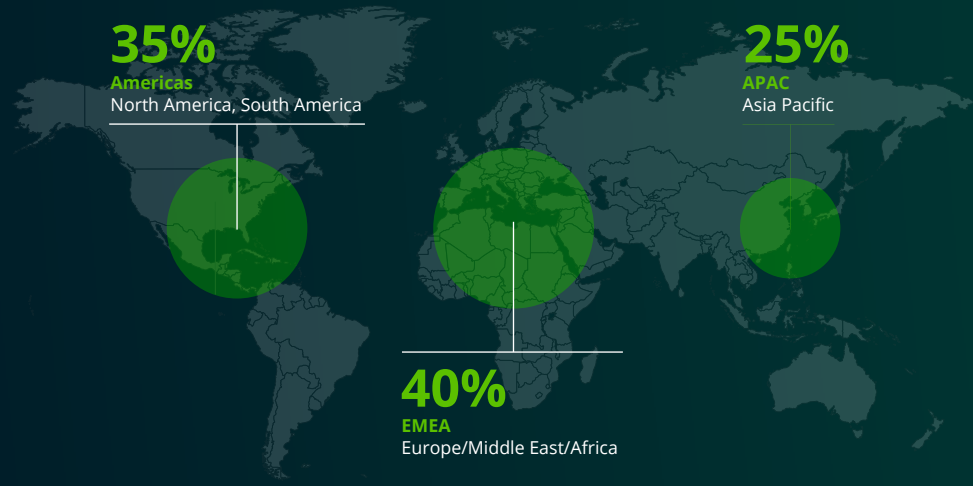
Deloitte designed its 2023 Global Future of Cyber Survey based on the complexity of today's business and technology landscape, focusing on the needs of enterprise leaders who may recognize the importance of cyber yet struggle to harness its value. Deloitte based its research on a survey of more than 1,000 cyber decision-makers at the director level or higher (C-suite executives and C-suite direct reports), across 20 countries and limited to organizations with at least 1,000 employees and US$500 million in annual revenue.

To accurately capture the increased impact that cyber has on businesses today, we nearly doubled the sample size from the 2021 research, from almost 600 respondents to 1,110. Deloitte also conducted in-depth interviews with a number of senior cyber decision-makers across various industries and geographies, to glean more detailed insights and to help validate our observations. Our approach covered every aspect relevant to the future of cyber, from strategy to tactics to culture to technology implementation.

At the core of this research, we focused our intentions and efforts on:

- Exploring how cyber has changed since Deloitte's 2021 report
- Applying a forward-thinking lens, to help bring the future of cyber into sharper focus
- Understanding the business value and impact of cyber that organizations are experiencing, and the distinct actions leading organizations are taking to gain more value from cyber

Headquarters locations of the organizations we surveyed



The future is cyber

In addition to providing essential context for how cyber has evolved over the past two years, we developed a view on cyber maturity to understand the business impact that leading organizations make when they adopt more mature cyber strategies.

By separating high-cyber-maturity organizations from their medium- and low-cyber-maturity counterparts, we can identify a distinct class of cyber leaders and more fully understand the extent to which cyber underpins business success and value.

Today, *cyber* means *business*, and it is difficult to overstate the importance of cyber as a foundational and integral business imperative. For any enterprise, the future of cyber will be shaped by the C-suite and the board's commitment, and by the business value that the entire organization can envision with cyber. Altogether, the results of our research show a new dynamic emerging as the CISO and the rest of the C-suite, along with the board, work in partnership to lead the business and enable innovation—together.

Put another way, cyber should be embedded across the broader business strategy. It should be included in every functional area, as an essential ingredient for success—to drive continuous business value, not simply mitigate risks to IT.

Demonstrating impact

"Where we minimize risk, we can clearly articulate where and how we have made an impact and how we've allowed operations to continue in a smooth and effective way—especially relative to our business partners that in many cases have had either operational or integration challenges."

—CISO, Consumer Organization

Looking at how the landscape has evolved

Since our previous report in the last quarter of 2021, global industries have continued to navigate constant disruption on multiple fronts, while adjusting their priorities, business initiatives, and capabilities accordingly.

Both the 2021 survey and this latest survey asked respondents about their organizations' digital transformation priorities—to help identify which technologies were important to the organization and would, therefore, need to be considered as part of future cyber strategies.

Compared to companies' top two priorities in 2021, cloud moved from the #2 spot to the #1 spot, displacing data analytics. Operational technology/industrial control systems and artificial intelligence/cognitive computing remained in the top five, moving up slightly. Joining the top-5 list this year is newcomer 5G, reflecting the growing role of the standard in organizations' business ambitions.

The continued importance of cloud brings with it the complex cyber considerations that are inherent in hosting data and applications off premises and often across various environments. While cloud—and cyber cloud—maturity varies considerably, findings in our recent Future of Cloud Survey suggest that many organizations are overcoming those concerns and achieving highly positive outcomes for risk-related cloud use cases. In fact, 83% of organizations say their cloud investments are driving positive outcomes in terms of mitigating business and regulatory risk.[2] This is a positive signal regarding maturing cyber cloud capabilities, shared responsibility models, and data privacy programs being put into place.

Digital transformation priorities

Then and now.

The role of cyber

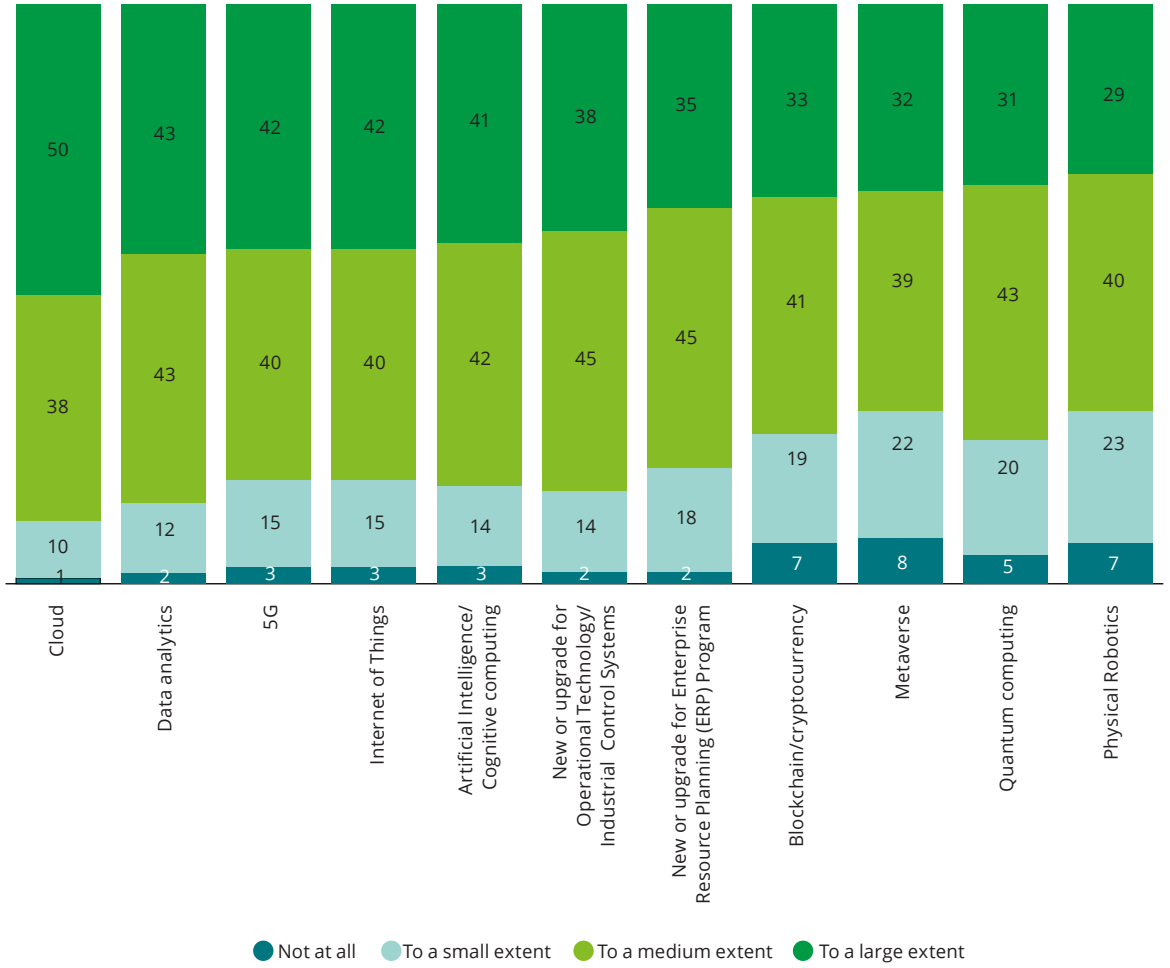
As part of our latest Global Future of Cyber survey, we asked about the role that cyber plays in each of these leading digital transformation initiatives. The results are clear: executives see cyber playing a crucial role for all digital transformation priorities, especially when it comes to cloud, data analytics, and 5G (Figure 1).

While digital priorities and emerging technologies have evolved, so too have the effects of cyber incidents on organizations we analyzed. Even as the organization's focus shifts to the positive benefits and long-term business value that cyber readiness can bring, it is important to keep sight of cyber's core ability to counter cyber threats, mitigating negative business consequences and risks.

Figure 1: Cyber in the spotlight

Cyber is expected to play a leading role in companies' digital transformation initiatives

(Percentages may not add up to 100% due to rounding.)



At the top

"Everyone is having this (cyber) topping the agenda, and they are incorporating that in the design of the strategies, in the design of the budgets, and in the design of their solutions."

—CISO, Financial Services Organization

Insights on incidents and impact

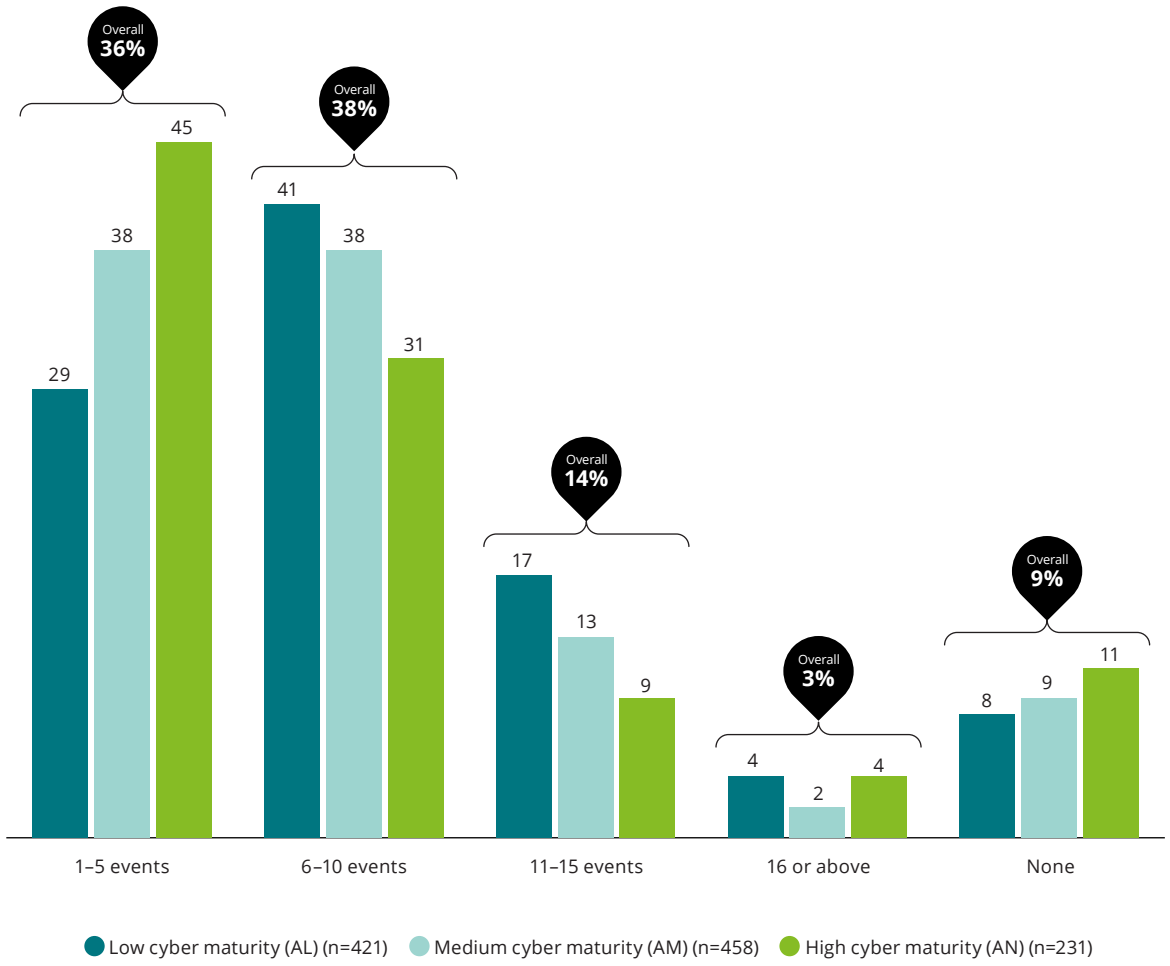
The frequency of cyber incidents or breaches has been growing, with 91% of organizations reporting at least one, compared to 88% in the 2021 survey. A multitude of actors, sources, tools, and techniques are part of the cyber concerns for organizations. High-maturity organizations seem more concerned about cyber criminals and terrorists, as well as phishing, malware, and ransomware attacks. Low- and medium-maturity companies have greater concern about denial-of-service attacks. It is worth noting that organizations with low maturity report experiencing more significant cybersecurity events (Figure 2).

91%

Organizations reporting at least one cyber incident or breach.

Figure 2: Number of significant cybersecurity events

(Precentage)



Meanwhile, operational disruption continues to be the most significant impact of cyber incidents, although loss of revenue and loss of customer trust jumped in the rankings—to second and third place—with 56% of respondents reporting that they suffered related consequences to a moderate or large extent. One potential hypothesis in play here: Organizations with a higher level of maturity may view the impacts differently, as they have a deeper understanding of what is actually happening in their business. Less mature organizations may be evaluating theoretical impacts. Regardless, high-maturity organizations do appear to be reaping significantly more positive benefits from cyber initiatives—including improved brand reputation and trust, operational benefits, and financial benefits. Low- and medium-maturity groups seem more likely to gain benefits around brand reputation and improving trust, as opposed to other areas.

In the context of these significant impacts, the need for a risk-based cyber strategy—across the organization's ecosystem of cyber strategies, solutions, and controls—is ever more important for the future of cyber. A zero trust architecture can enable modern enterprise environments by strengthening security posture, simplifying security management, and improving end-user experience. And the journey to zero trust requires a strategy aligned to business outcomes plus significant effort and planning, including addressing foundational cyber issues, automating manual processes, and planning for transformational changes to the security organization, the technology landscape, and the enterprise itself.[3]

Figure 3: Feeling the pain
Cyber incidents and breaches are resulting in the following negative consequences for organizations
(Based on frequency of top 2 ranking in 2021, top 2 box selection in 2023)

Negative consequences resulting from cyber incidents and breaches	2021 (Rank)	2023 (Rank)	2023 (Percent)
Operational disruption *(including supply chain/or partner ecosystem)*	1	1	58%
Loss of revenue	9	2	56%
Loss of customer trust/negative brand impact	4	3	56%
Reputational loss	5	4	55%
Defunding of a strategic initiative	N/A	5	55%
Loss of confidence in tech integrity	N/A	6	55%
Negative talent recruitment/retention impact	8	7	54%
Intellectual property theft	2	8	54%
Drop in share price	3	9	52%
Regulatory fines	7	10	52%
Change in leadership	5	N/A	N/A

More than zero
A zero trust implementation is much more than a technological implementation, it is also a business and cultural transformation that is dependent on culture, communications, and awareness.

A comprehensive zero trust implementation should address a number of elements, including governance (architecture and operations), enablers such as analytics and automation, and core domains such as identities, data, and devices.

56%
Respondents reporting that they suffered related consequences to a moderate or large extent.

Understanding what it means to be cyber mature

In today's environment of heightened cyber importance, we drew from our experience working with thousands of organizations worldwide to segment respondents according to their cyber maturity.

Maturity at any size, in any industry

In looking across the three groups, we dug into their broader characteristics to identify any trends or traits for maturity. All three of the segments (low, medium, high) spanned industries as well as organization size and revenue—indicating that maturity level may not be significantly dependent on a company's industry or size.

Defining maturity

To define cyber maturity and identify the high performers who are shaping the future of cyber, we used three sets of leading practices to rate organizations:

Robust cyber planning, indicated by the presence of strategic, operational, and tactical plans to defend against and respond to cyber threats

Key cyber activities, such as qualitative and quantitative risk assessment, industry benchmarking, and incident-response scenario planning

Effective board engagement, exemplified by organizations whose boards address cyber-related issues on a regular basis

A closer look at maturity groups

By assigning point values to each set of leading practices, we were able to segment the surveyed organizations into three groups:

38%

Low cyber maturity organizations, adhering to none of the sets of leading practices

41%

Medium cyber maturity organizations, adhering to 1 of the sets of leading practices

21%

High cyber maturity organizations, adhering to 2–3 sets of leading practices

Connecting maturity to value, for the entire enterprise

Crucially, the three leading practices that we identified—cyber planning, activities, and board involvement—hinge on stakeholders recognizing the importance of cyber responsibility and engagement across the whole organization.

While CISOs can serve as organizational champions for cyber, many of these leading practices only become possible through enterprisewide engagement.

That can take the form of:

- Having a governing body that comprises *IT and senior business* leaders to oversee the cyber program
- Conducting incident-response scenario planning and simulation at the organizational and/or board level
- Regularly providing cyber updates to the board, to secure funding
- Annual cyber awareness training among all employees

The high-maturity organizations that we identified recognize the effectiveness of distributing cyber responsibilities throughout the organization. Such efforts align with Deloitte's common guidance of embedding cyber professionals within business units, or at least having someone in each business unit with a clear responsibility for coordinating with the cyber team. They are 31% less likely to cite inadequate governance across their organization as a top challenge in managing cyber (35% for low cyber maturity vs. 34% for medium cyber maturity vs. 22% for high cyber maturity).

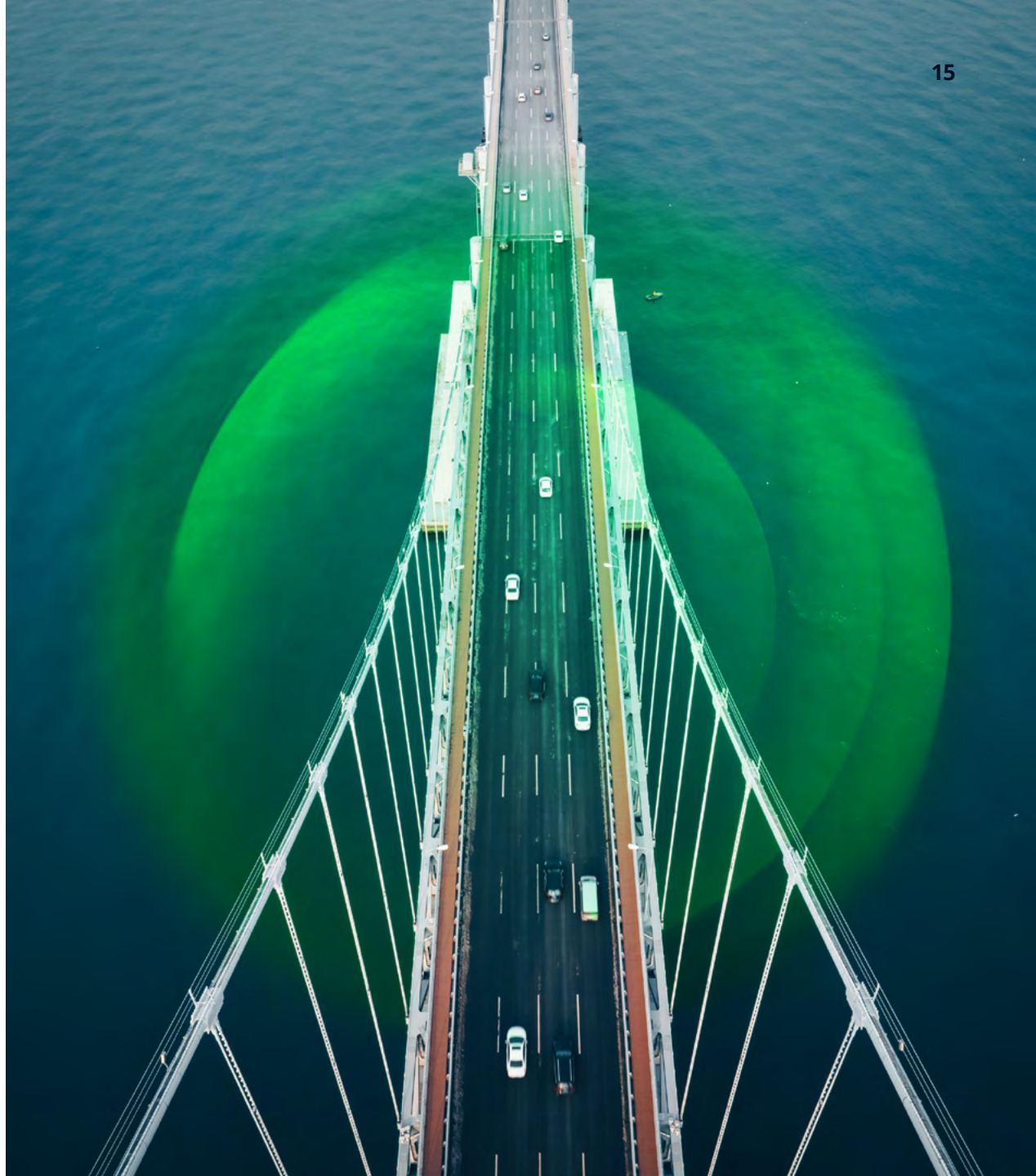
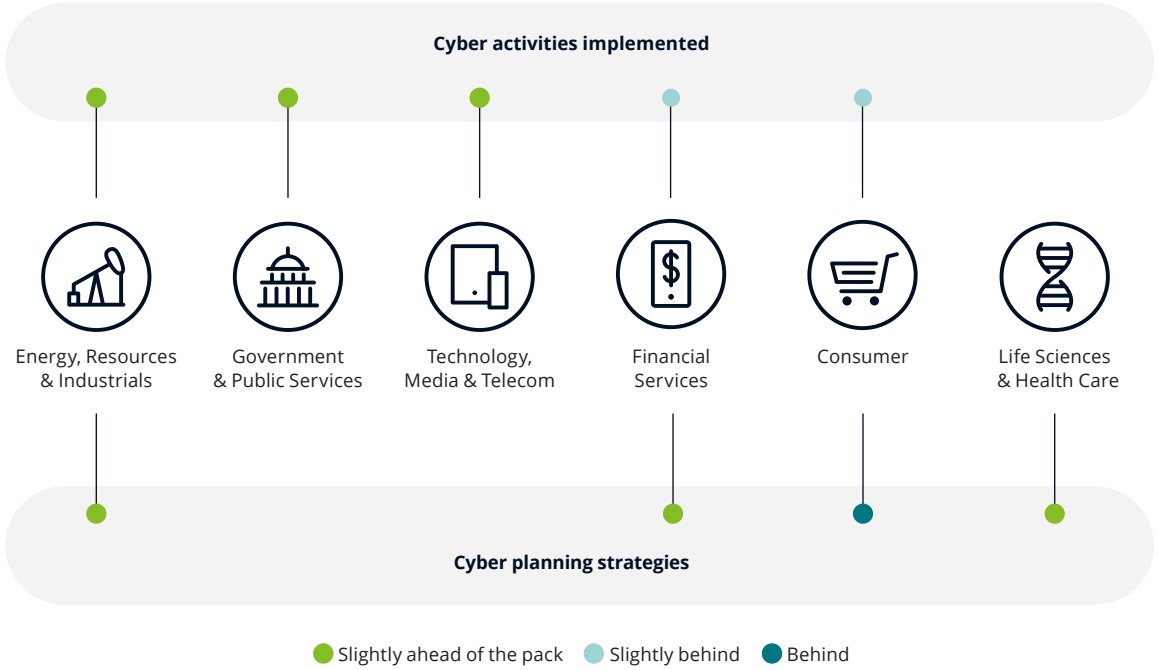


Figure 4: Where industries stand



Examples of cyber planning strategies

- Analyzes and updates cyber plans annually
- Has a governing body composed of senior business and IT leaders, to oversee the cyber program
- Employs risk quantification tools to measure and ensure the return on cyber investments
- Conducts incident-response scenario planning at the organizational and/or board level
- Gets external help/outsourcing to manage cyber initiatives

Examples of cyber activities

- Annual cyber awareness training among all employees
- A cyber incident-response plan that gets updated and tested annually
- Comprehensive plan to assess how to protect data at each step, as to where data is stored, processed, and transmitted
- Cyber risk program to monitor and track the security posture of partners and suppliers
- Ongoing "voice of the customer" input for cyber and data privacy preferences

Industry

Of the six industries included in this study, three of them have five or more cyber activities implemented—slightly higher than the overall average. Those three industries include government/public services (GPS); energy/resources/industrials (ERI); and technology/media/telecom (TMT).

Two industries (ERI and life sciences/health care) have five or more cyber planning strategies implemented, at a level slightly higher than the overall average.

Meanwhile, the financial services industry is implementing four out of eight cyber planning strategies at levels slightly higher than the overall average. That industry, however, is behind the overall average when it comes to cyber activities, with only one activity rising above the overall average.

And our data showed that the consumer industry is slightly behind other industries and the overall average, with seven out of the ten key cyber activities, slightly behind the overall average, and with all of the cyber planning strategies being implemented at levels below the overall average.

Organization size

The research also indicated that companies with 20,000 or more employees are more likely to:

- Understand the importance of business strategies around risk management, digital transformation, digital trust, and technology modernization.
- Recognize the importance of cyber in these business strategies.
- Engage in cyber planning and implementing key cyber activities.

The bottom line

Any organization, regardless of industry or size, can move toward high cyber performance and maturity. Success should not depend solely on your ability to "buy" maturity through increased investments in cyber. Rather, the actions that you take and the culture that you build will be primary factors for improving performance.

The survey defined small companies as those with revenue of US$500 million to US$1 billion. Large companies included organizations with US$10 billion or more in revenue.

Bolstering the business with cyber

Building a bigger business case for cyber

Regardless of an organization's maturity, there is no cyber architecture or approach that can guarantee absolute security and risk mitigation. Instead, the most striking feature of highly cyber-mature organizations is their ability to extract value from their cyber investments.

High performers are doing more when it comes to engaging leadership, planning, and acting—and it appears to be generating more business value from their cyber efforts. In terms of seeing impacts like increased efficiency, resiliency, and agility, those highly mature organizations are ahead of the pack, and they are recognizing benefits that may not be typically associated with cyber.

Generating confidence and much more

More than half of these leaders (55%) reported that cyber provides them with confidence to try new things—compared to 45% for medium-maturity organizations and 40% for low-maturity organizations.

And nearly 70% of highly mature organizations said cyber was making an impact on both enhancing trust and enabling efficiency—significantly higher than the low- and medium-maturity organizations.

Likewise, a majority of highly mature leaders (65%) also cited resilience and agility as benefits of cyber—once again far ahead of their low-maturity and medium-maturity peers (Figure 5).

55%

Highly mature organizations said cyber provides them with confidence to try new things.

Figure 5: Recognizing the bigger potential

Where cyber is making a specific impact on businesses initiatives

(Percentage)

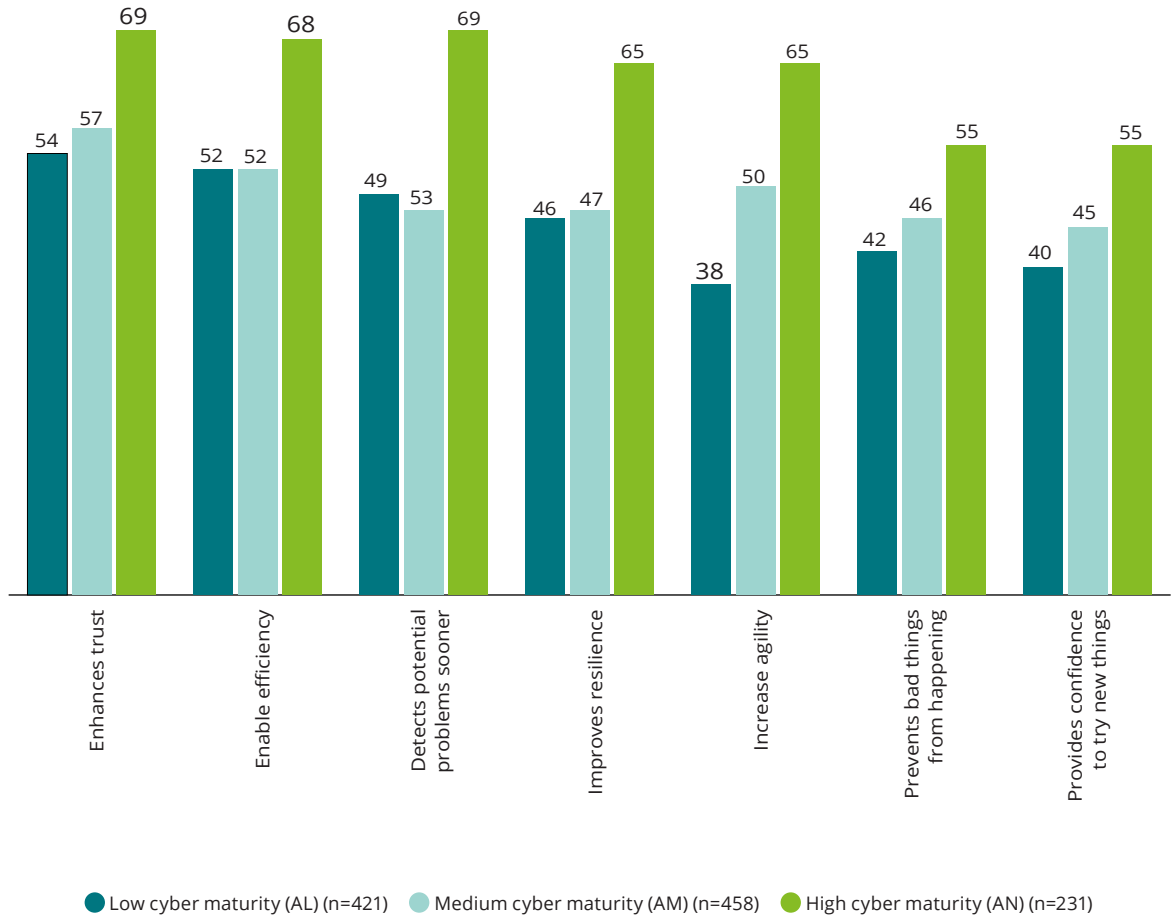
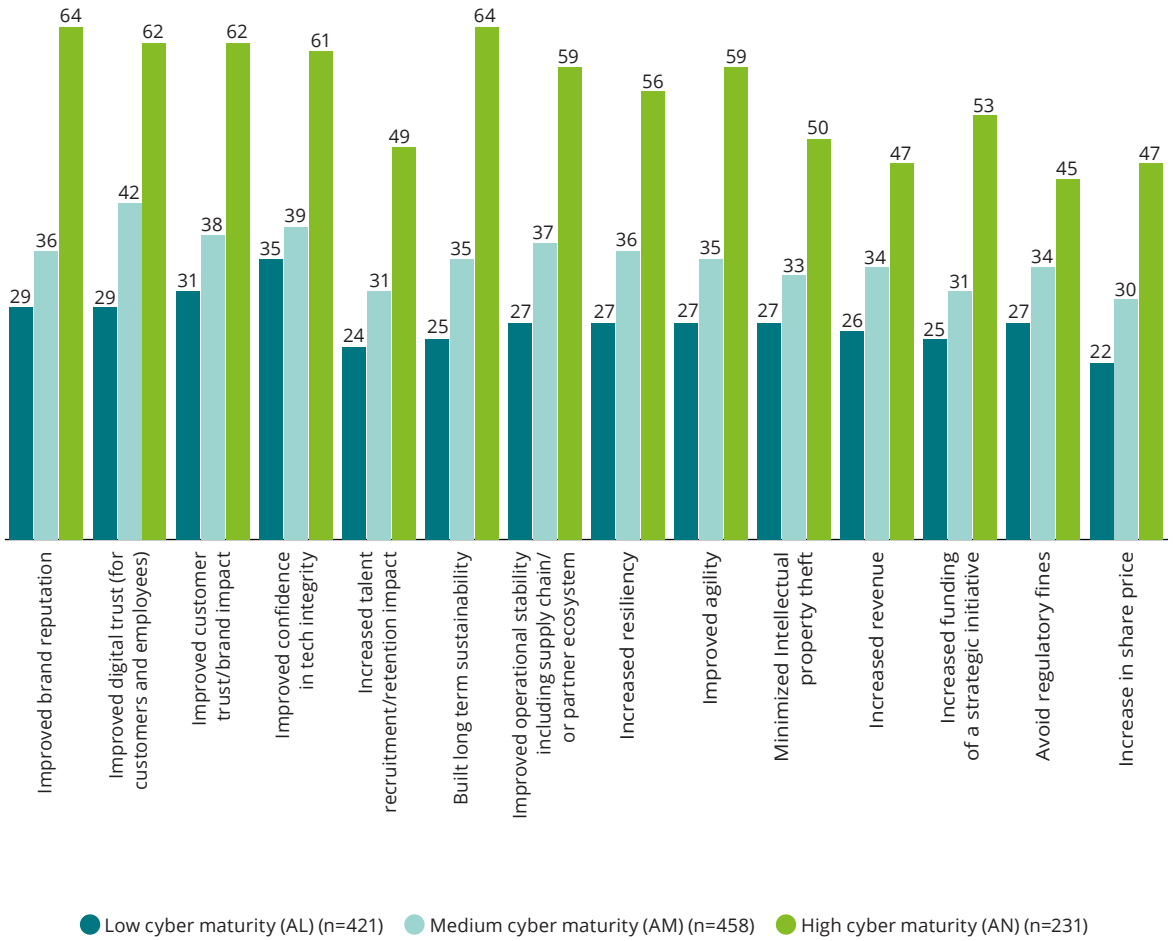


Figure 6: Reaping real benefits

Cyber initiatives are making a positive contribution in the following areas

(Percentage)



The highest-performing organizations also were more likely to report positive contributions from their cyber initiatives in areas such as improved brand reputation (64%), increased revenue (47%), improved operational stability involving the supply chain and partner ecosystem (59%), talent recruitment and retention (49%), long-term sustainability (64%), improved customer trust and brand impact (62%).

Trust is an issue of paramount importance when it comes to cyber. As an "ecosystem" that can help deliver outcomes, trust needs to be built with all of your human stakeholders. A trusting workforce, for example, achieves 2x improved customer satisfaction, and customers who trust a brand are 88% more likely to buy again. Building customer trust also affects partners and improves up to 4x market capitalization, with trusted companies ultimately outperforming their peers by up to 400%.

And based on the data from our 2023 Global Future of Cyber Survey, global organizations can clearly see the connection to benefits including trust. While organizations that are investing in cyber are seeing significant gains across a range of value measures, the highest performers get more of that value across every strategic measure (Figure 6).

Customer expectations

"The customer—my personal guess—is not willing to pay a lot extra for cybersecurity (in our products). They will *expect* to have it. It will be a *differentiator*."

—CISO, Automotive Organization

400%

Building customer trust affects partners and improves market capitalization, with trusted companies ultimately outperforming their peers.

One other area in which highly mature cyber organizations exceeded their peers in the low and medium group: the value they are seeing from using third-party cyber services.

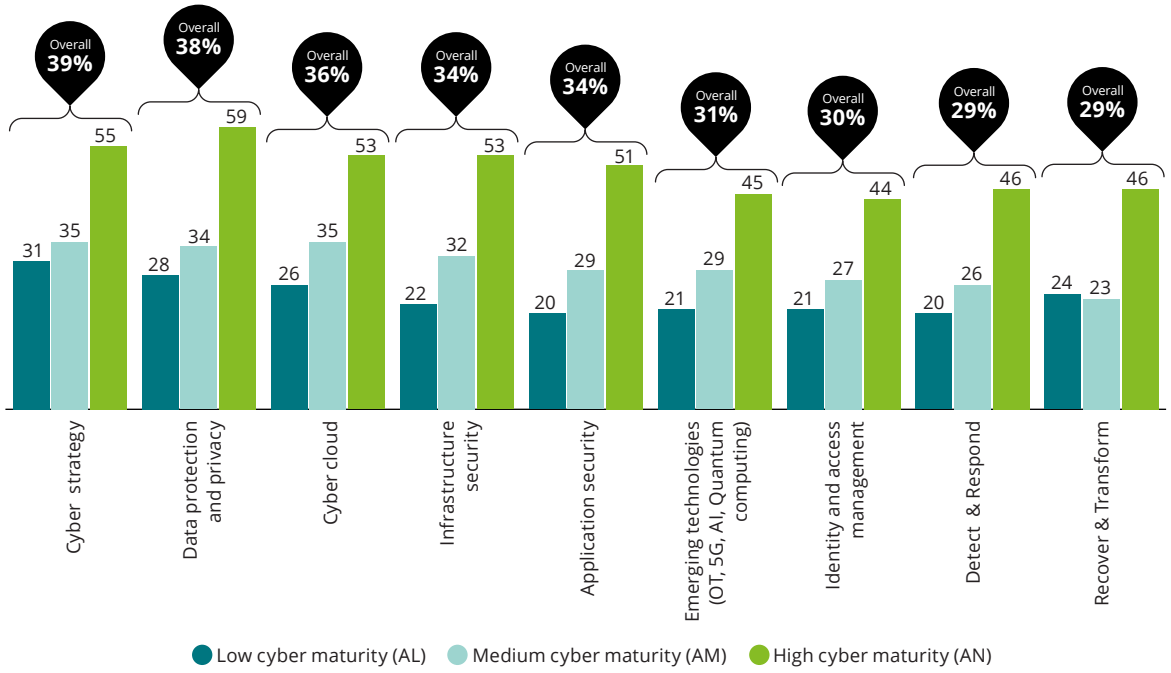
A majority of these high performers reported measurable value when it came to third-party services for cyber strategy, data protection and privacy, cyber cloud, infrastructure security, and application security. Meanwhile, a minority of low- and medium-maturity companies reported value across those areas.

Importantly, to take advantage of the value that third-party cyber services can bring, organizations should consider ways they can manage their growing services ecosystems and the inherent complexity (Figure 7).

Figure 7: Getting value with vendors

Where companies are reporting seeing value from third-party cyber services

(Percentage)



Lessons to learn: Following the leaders

Given the ability of these high-performing organizations to extract significant business wide benefits from their cyber investments, other organizations should look to the example set by cyber-mature companies—using it as a set of guideposts for achieving broader enterprise engagement on cyber.

Based on the success that these high-maturity organizations have derived from cyber, it may be time for your business to take a deeper dive into questions such as:

Do we have the right technology and partner ecosystem in place—and how can we manage a growing, complex network of third parties?

Are we investing in the right ways and in the right areas—and do we have the right framework in place to understand how and where cyber is adding value across the organization?

Are we investing in the right ways and in the right areas—and do we have the right "value frame" in place to understand how and where cyber is adding value across the organization?

Key insights to shape the future of cyber: Five areas of focus

1 Multidirectional engagement

As we have already noted, high-performing organizations engage the entire organization in cyber activities. While high-maturity organizations, by definition, leverage more cyber leading practices than their medium- and low-maturity counterparts, the disparities in organizational engagement are among the starkest.

Leadership. High-maturity organizations are nearly three times as likely as low-maturity organizations, and nearly twice as likely as medium-maturity organizations, to have a governing body comprising senior business and IT leaders, to oversee their cyber programs (60% high vs. 36% medium, 22% low).

Scenario planning. Similarly, high-maturity organizations are three times as likely as low-maturity organizations, and twice as likely as medium-maturity organizations, to conduct incident-response scenario planning at the organizational and/or board level (60% high vs. 30% medium, 20% low).

2 Criticality to digital transformation initiatives

High-maturity organizations are much more likely to value cyber as central to key digital transformation priorities (Figure 8).

Adoption of these digital transformation priorities is essential to ensuring operational agility and business success. But each carries significant cyber risks, and high-maturity organizations may be especially attuned to that reality.

For example, AI can be an enabler of cyber strategies and companies' digital business ambitions, but it also introduces the potential for cyber risk that can come with any digital technology. Beyond the leading practices we have highlighted here, our recent State of AI in the Enterprise survey report also underscores how engaging in specific risk-mitigation steps can also help drive better outcomes, such as cost reduction and entry into new markets. AI-related risks represent an issue of high importance to organizations. It also found explainability and transparency in AI decisions, data privacy or consent mismanagement, and safety concerns about AI systems, among others, all loom large as ethical risks that concern organizations.[5]

Managing these risks can have a major impact on an organization's AI efforts. In fact, the AI survey found that 50% of respondents cited management of AI-related risks as one of the top inhibitors to scaling AI projects. Despite such sentiments, only 33% of respondents have aligned their AI risk management with their organization's broader risk management efforts. However, 33% of high-outcome surveyed organizations and 29% of low-outcome surveyed organizations do engage outside vendors to independently audit their AI systems.

Aiming for results with AI

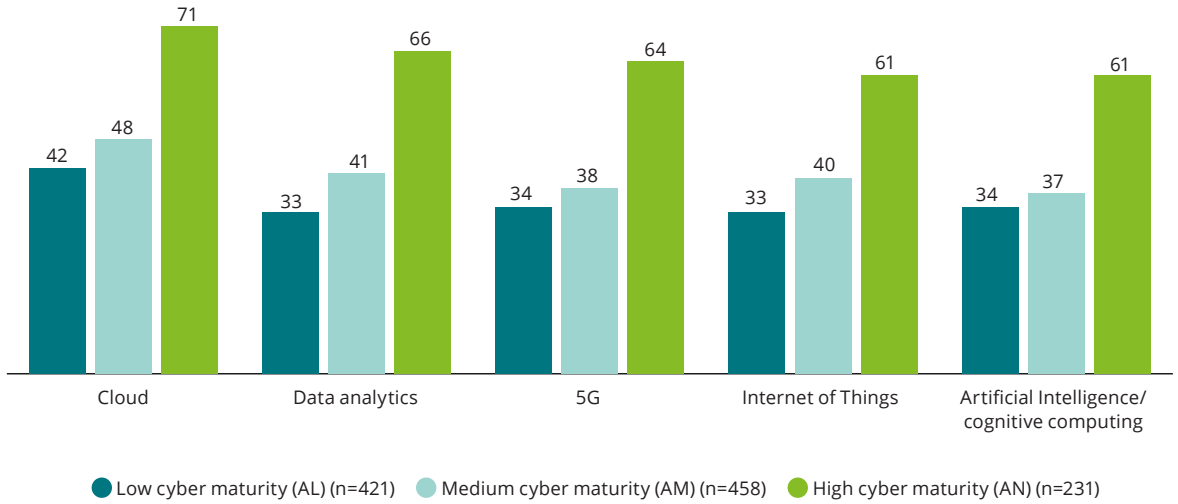
"But in a nutshell we are promoting our knowledge and awareness (about cyber), as well as quantum computing and metaverse—AI too—while approaching cybersecurity as the enabler for the business."

—Mesfer Almesfer, CISO, NEOM

Figure 8: Evolving with cyber

How each maturity group views cyber's importance to specific digital transformation initiatives

(Percentage)



3 Robust planning

Planning is proving to be paramount for creating cyber strategies that effectively mitigate risk and drive business value. And the high-performing organizations identified in this report appear to be abundantly aware of planning's importance (Figure 9).

Highly cyber-mature organizations are more likely to have robust plans in place, with elements that may include:

- **A cybersecurity incident-response plan** that gets updated and tested annually (87% of high-maturity organizations)
- **An operational and strategic plan** to defend against cyber threats (91%)
- **A comprehensive plan to assess how it protects data** in each step, covering where that data is stored, processed, and transmitted (88%)

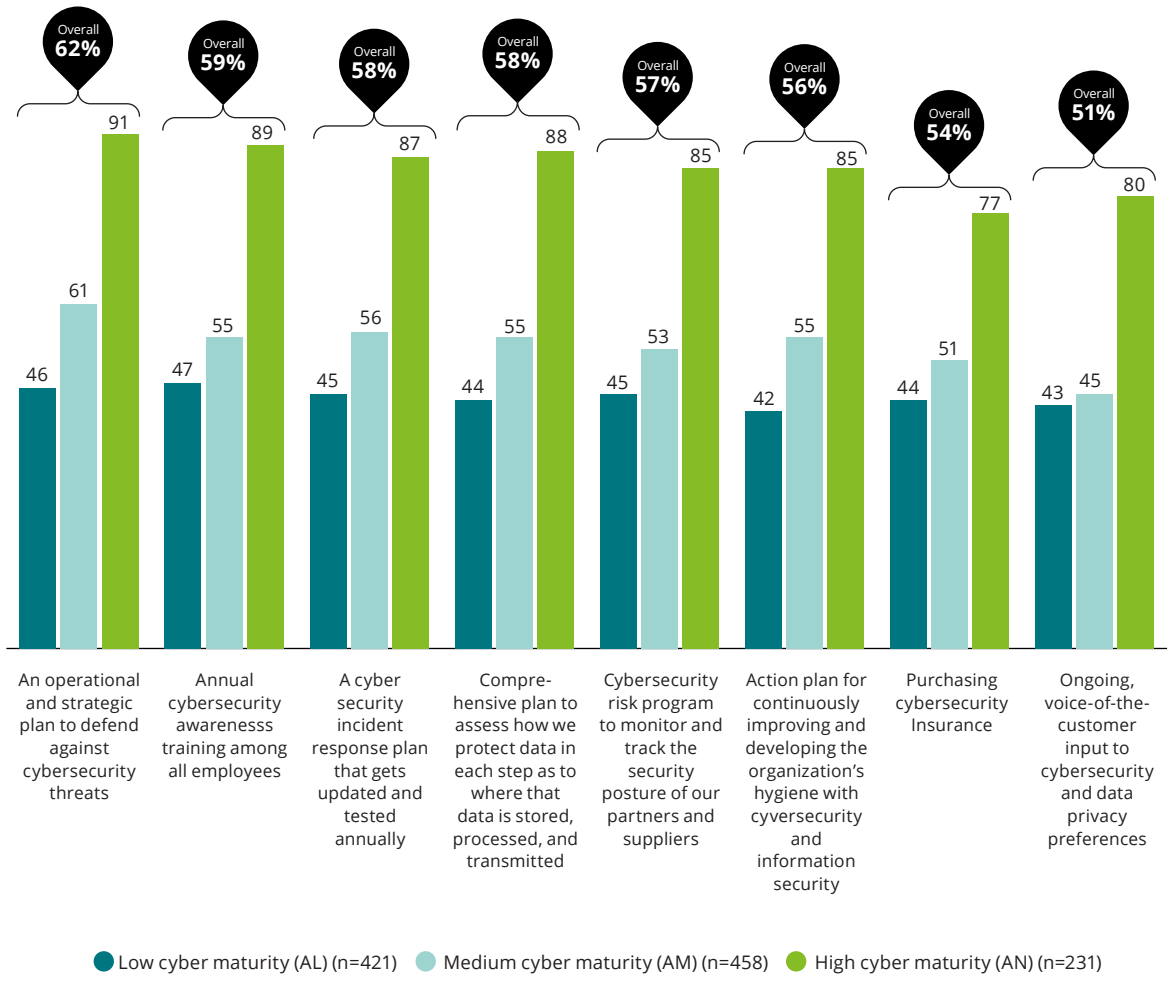
91%

High-maturity organizations an operational and strategic plan to defend against cyber threats.

Figure 9: The planning reality, across maturity groups

Organizations that are fully implementing these actions

(Percentage)



4 Appreciating and investing in talent

Cyber issues and activities are ultimately about people—whether it is an attacker trying to exploit vulnerabilities, decision-makers responsible for cyber strategies and tactics, or the frontline employees running digital business processes and cyber programs. Strong talent—in the form of people who are skilled, experienced, and cyber-focused—is a prerequisite for strong performance. Looking beyond traditional talent profiles has become crucial for securing the right people to drive cyber initiatives. For example, a customer experience designer might bring needed insights for cyber initiatives, helping to identify potential vulnerabilities when it comes to transactional processes, data collection, or privacy.

Attracting and retaining talent—the *right* talent—is difficult. Stress and other pressures come naturally with any position of cyber responsibility. And it can be intense. In fact, one respondent interviewed as part of the study—a financial industry leader in the United Kingdom—pointed out that his designation as a "senior responsible manager" means that cyber risk effectively sits with the CISO and that "there could be serious, personal consequences" for certain events. It is also a powerful argument for the inherent business focus of cyber—and how responsibility should transcend a single enterprise role or department.

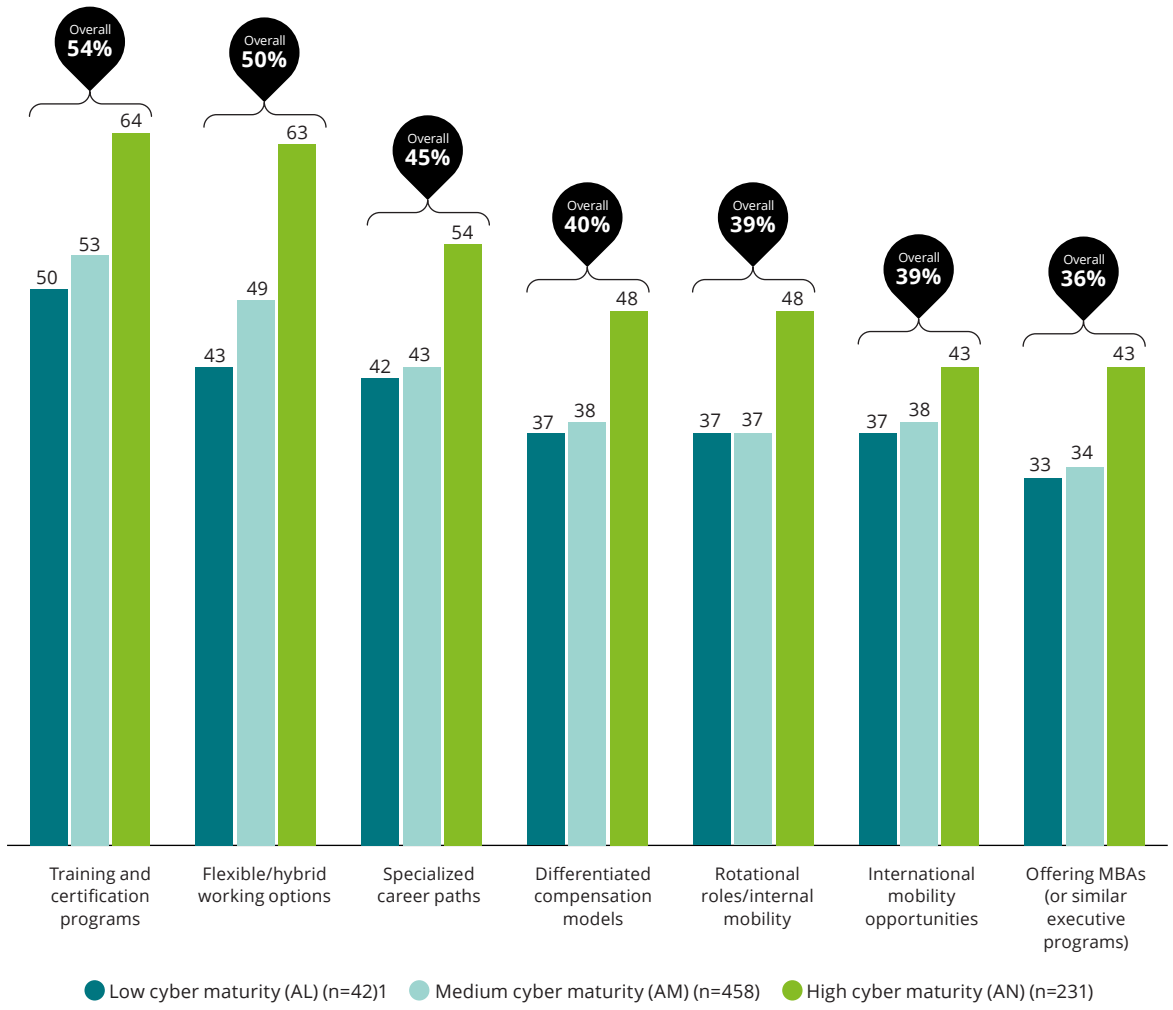
Overall, high-maturity organizations appreciate the importance that experienced talent can bring to cyber efforts, and they are taking meaningful steps to retain valuable talent. High-maturity organizations are significantly more likely to cite a lack of skilled cyber professionals as a top challenge in managing cyber (47% high cyber maturity vs. 38% medium, 37% low).

For more mature organizations, their robust programs may be part of the talent challenge. As they engage more broadly and deeply in cyber-related activities, they may find that they have stretched their teams and capabilities to the maximum, and they may recognize the need to bring in more people with advanced and diverse skills to support their more mature programs.

But are low-maturity organizations *really* not facing the same level of talent challenges—or are they simply not putting enough emphasis on having the right skills in place? If the latter, emphasizing talent acquisition should be a priority—and something that ultimately could help them become more mature organizations (Figure 10).

Figure 10: How they are tapping their talent

Strategies organizations are taking to engage, retain, and develop existing talent



5 A diverse ecosystem of tools and services

As they look to lead in the future of cyber, high-maturity organizations are acutely aware that they cannot do it alone. They must rely on an extended ecosystem of technologies, capabilities, and external offerings to create future-facing cyber capabilities that can also support business value.

Compared with their low- and medium-performing counterparts, these high-performing organizations are more likely to have in place a broad assortment of products and services from third parties (Figure 11), including:

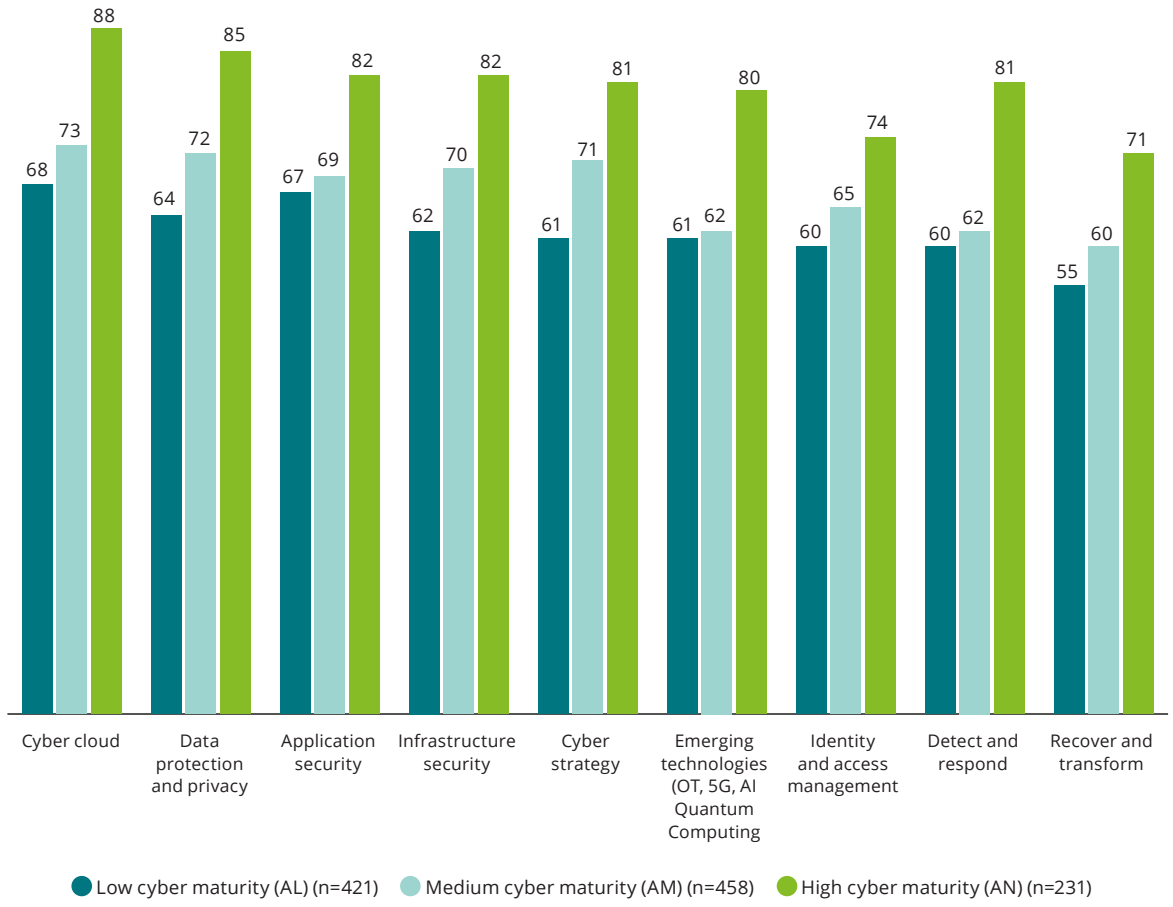
- Application Security
- Cyber Cloud
- Cyber Strategy
- Data Protection and Privacy
- Detect & Respond
- Emerging Technologies (OT, 5G, AI Quantum Computing)
- Identity and Access Management
- Infrastructure Security
- Recover & Transform

While deploying tools and services increases cyber readiness, it also creates a need for strong ecosystem planning, management, and operations. Working with multiple vendors to solve complex, evolving problems—and to run, monitor, and update cyber capabilities as part of an integrated environment—presents its own set of complex needs.

Ironically, the complexity that can come with multiple cyber vendors could provide an entrée to new risks, including breaches. In some situations, consolidating vendor oversight is one way to bring simplicity to the challenge.

As the average number of cyber vendors used is expected to increase in the next two years, so does the case for simplifying and consolidating oversight. One other approach to consider: working with convening bodies, such as industry groups, to better understand technology developments and emerging practices that can influence how you manage your ecosystem.

Figure 11: Relying on others
Organizations are using third-party cyber services providers in these areas



Change in behavior
The use of automated behavior-analytic tools to detect and mitigate potential cyber risk indicators among employees has increased significantly. In this survey, 76% of respondents reported using such tools; in the 2021 survey, 53% reported using them.

Gaining perspective
"A 100% internal strategy doesn't work. It doesn't scale; it doesn't work and it has a tendency that it becomes an ivory tower. We work with a wide range of partners, and this is mainly to get new ideas and to help in guiding us strategically."

—CISO, Automotive Organization

So where do we go from here?

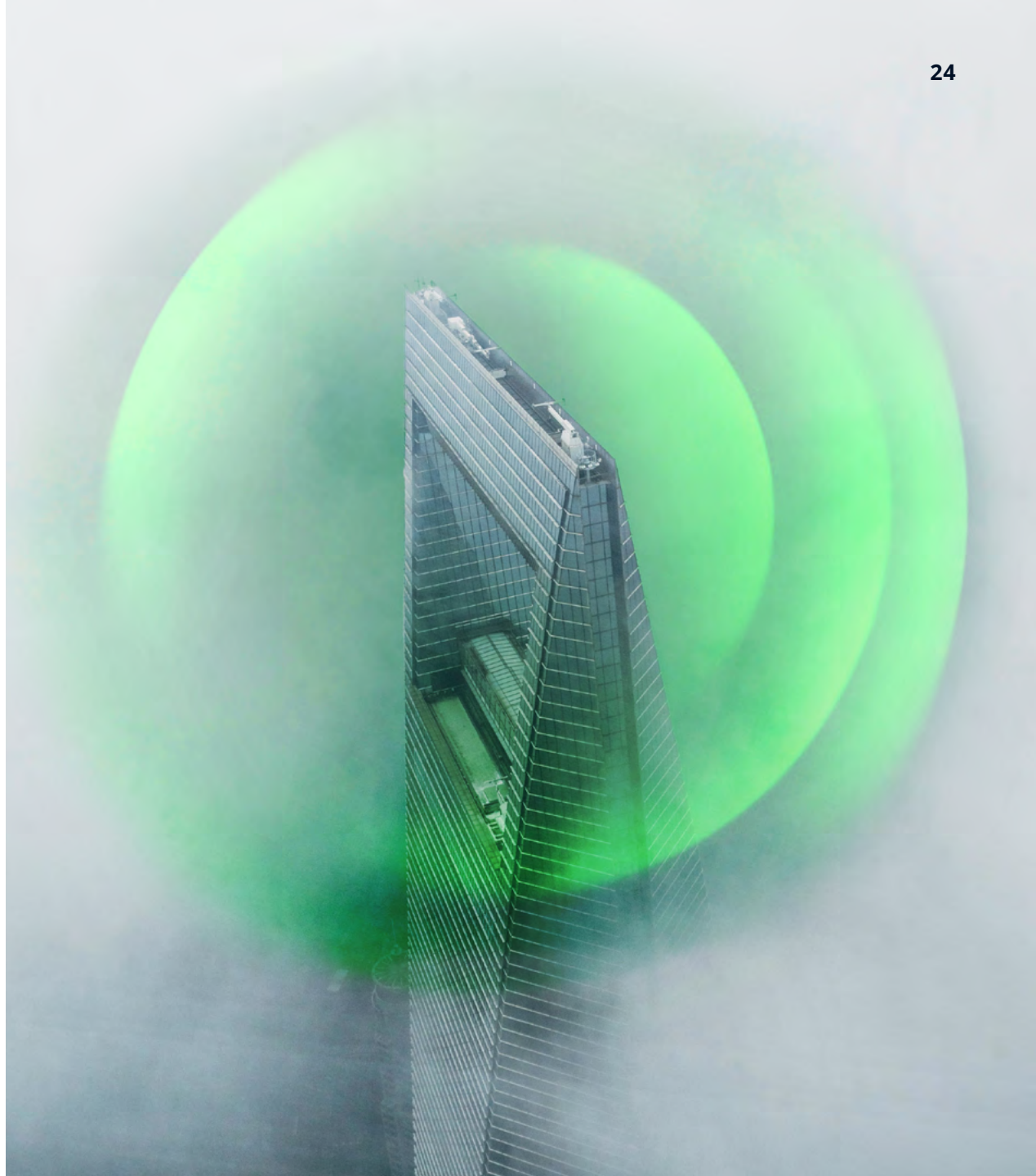
If enterprise leaders expect their businesses to be able to expand and grow, they should expect cyber to be an integral part of their plans. Cyber should also be an integral part of all the tools they will use to support their business ambitions going forward.

The days of "cyber as an afterthought" are gone. And for any business, new technological capabilities will be more effective when strong cyber strategies are part of the picture. Emerging technologies will bring along with them innovative solutions that can support future business models and also present unforeseen challenges on the cyber front. How will you harness these technologies for business value while ensuring that your cyber strategies and investments keep pace?

For starters, a zero trust approach should be central to your efforts involving new technology. By removing the assumption of trust from the security architecture and authenticating every action, user, and device, zero trust helps enable a more robust and resilient security posture. The organizational benefits are complemented by a considerable end-user perk: seamless access to the tools and data needed to work efficiently.

"Zero trust transformation journeys become very complex in large IT estates like ours. We must transform at the pace of business while managing the complexity of an ever-expanding ecosystem of partners looking to connect with a wide range of devices in order to process diverse workloads—all securely."

—Allan Cockriel, Group CIO/CISO, Shell



"We will have a more diverse range of digital solutions, including highly business-specific or data-intensive ones like AI and supercomputing, which require a constant update on how our cyber environment is effectively protected and meets regulatory standards."

—Charlie Huang, Data Protection Officer, BASF

When it comes to adopting innovations, begin with your strategy and understand the technologies available that support that strategy from a cyber perspective—then apply a critical lens. How does the use of a data service or platform, for example, align with your purpose, reinforce your ability to create trust, and open up the organization to risks and threats? From there, work to apply the right solution for the right needs.

Looking ahead

Sensing the risks and opportunities inherent in new technology is one way to keep up with the evolving threat landscape. You do not want your cyber efforts to have to play catch-up with fast-moving tech trends. The less prepared you are for technological change, the less prepared you are for managing cyber risk.

One case in point is the rising importance of 5G, which appeared as a new entrant on this survey's list of top 5 digital transformation priorities. While 5G can enable new use cases—such as telemedicine, asset tracking in manufacturing, and augmented reality for advanced training—it also presents a large attack surface. Designing and embedding security from the start will be crucial for 5G adoption, but it also will bring a tremendous amount of complexity.

Meanwhile, AI, which remains among the top 5 priorities in the survey, can help organizations address complexity on a number of fronts, including cyber. As organizations struggle with security breaches, cyber AI can be a force multiplier, enabling security teams not only to respond faster than cyberattackers can move but also to anticipate these moves and act in advance. With AI and automation, organizations could also eliminate the tedious functions of some analysts—and then train those analysts for more strategic roles that may be challenging to fill.

And it is never too early to begin thinking about technologies that are much farther down the road, including quantum computing, which only 4% of survey respondents said would be a digital priority in the next few years. While quantum computing unleashes tremendous potential computing power for the enterprise, it also can provide a tool for cyberattackers to wield—and calls for a new enterprise footing of "quantum readiness."

Security by design

"We're actually investing in what we call 'secure by design' to make sure that security is one of the many elements of our value proposition. We are investing in policies, tooling, and controls across the software and product lifecycles to ensure we are creating great—and secure—technology. Our customers expect it."

—Allan Cockriel, Group CIO/CISO, Shell

Onward

The future of cyber and the future of business are tightly intertwined. How you embed cyber thinking, planning, and action into all of your business initiatives will directly influence the success of those initiatives.

Put another way: cyber is foundational. It is the bedrock for enabling and sustaining the digital trust on which the future of your business will stand. As business continues to shift ever more sharply into the digital realm, creating effective digital ecosystems will depend on creating effective cyber strategies that drive business outcomes.

Brand reputation. Customer trust and loyalty. Operational stability. Revenue growth. It is all connected to how well you plan and execute when it comes to cyber—on how strong you make your cyber foundation. Thinking "cyber first" is imperative—when embarking on new cloud initiatives, when developing new products and services, when adding third parties to your ecosystem, and when providing your workforce with new tools. And the importance of cyber is woven throughout all other digital imperatives, such as the need for insights, platforms, connectivity, effective experiences, and integrity.

Get started

How you approach cyber says a lot about how you will approach the future of your business, and how well you will achieve your business aims. No matter where you are today—and no matter where you want to go—it helps to start with a clear understanding of what is possible and what may lie on the road ahead.

Acknowledgements

Ian Blatchford, Scott Buzik, Luca Covolo, Deborah Elder, Jaya Gopalan, Jeremy Guterl, Matthew Holt, Dan Konigsburg, Daphne Lucas, Diana Kearns-Manolatos, Emily Mossburg, Mike Nash, Kelly Nelson, Jud Payne, Sean Peasley, Ashley Reichheld, Heather Saxon, Daniel Soo, Scott Tillett, Niels van de Vorle, Marius von Spreti, Emily Werner

Contacts

Emily Mossburg
Global Cyber Leader
emossburg@deloitte.com
+1 571 766 7048

Ian Blatchford
Asia Pacific Cyber Leader
iblatchford@deloitte.com
+61 474 288 278

Amir Belkhelladi
Canada Cyber Leader
abelkhelladi@deloitte.ca
+1 514 393 7035

Peter Wirnsperger
Central Europe
Cyber Leader
pwirnsperger@deloitte.de
+49 40 320804675

Niels van de Vorle
North and South
Europe Cyber Leader
nvandevorle@deloitte.nl
+31882882186

César Martín Lara
Spain Cyber Leader
cmartinlara@deloitte.es
+34 914381416

Deborah Golden
United States
Cyber Leader
debgolden@deloitte.com
+1 571 882 5106

Endnotes

1. Deloitte 2021 Future of Cyber Survey.
2. Closing the cloud strategy, technology, and innovation gap. Deloitte US Future of Cloud Survey Report, 2022.
3. Future of Digital Trust: Driving forces, trends and their implications on our digital tomorrow. Deloitte. 2021.
4. The Four Factors of Trust: How Organization Can Earn Lifelong Loyalty.
5. Fueling the AI transformation: Four key actions powering widespread value from AI, right now. Deloitte's State of AI in the Enterprise, 5th Edition report, October 2022.
6. Take 5: 5G cybersecurity, Part of Deloitte's 'Take 5 on 5G' article series.
7. Cyber AI: Real Defense, Deloitte Tech Trends 2022.
8. Quantum Cyber Readiness Deloitte's perspective on transitioning to a quantum secure economy

Deloitte.

To find out more, please visit **www.deloitte.com/futureofcyber**.