Deloitte.

THE GLOBAL FUTURE OF CYBER SURVEY, 4TH EDITION

THE PROMISE OF CYBER

Enhancing transformational value through cybersecurity resilience

THE GROWING VALUE OF CYBER

The demands of cybersecurity are continually evolving. New threats, technologies, and changing business needs keep redefining priorities and possibilities for organizations operating in every industry.

Getting a clearer view into the future of cyber is a constant undertaking, allowing us to not only stay ahead of emerging risks but to identify new possibilities for business value.

In this, the 4th Edition of Deloitte's Global Future of Cyber Survey, we get that clearer view. We see that the link between cybersecurity and business value is growing stronger—with cyber becoming increasingly integral to enabling tech-driven programs and driving business outcomes. We see also how the role of C-suite leaders, including the chief information security officer (CISO), is evolving as cyber considerations intensify across the enterprise.

We are excited to share key findings from the survey and invite you to explore them here. In the following pages, you'll find a blend of data-driven insights plus observations based on Deloitte's deep global cyber experience, as well as reflections provided directly by interview respondents. Take a look and, if you are interested in a deeper dive, we would love to hear from you.

Happy reading,

Emily Mossburg
Deloitte Global Cyber Leader

WHAT'S INSIDE

A NEW ERA OF TRANSFORMATIONAL CYBER STRATEGIES

Focusing on outcomes and resilience

The future of cyber is constantly evolving as organizations across the globe deal with ongoing business complexity and change, as well as a myriad of new threats and risks. Yet one thing remains constant: Cyber and business value are deeply intertwined, and cybersecurity stays central to how organizations in every industry consistently deliver the outcomes they desire.

That powerful connection between cybersecurity and business impact comes into sharp focus in Deloitte's 4th Edition of The Global Future of Cyber Survey—which asked nearly 1,200 leaders in various industries worldwide 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, risk, and the business.

The focus on outcomes is growing stronger

In our previous report, the 3rd edition of the survey, Deloitte recognized the extent to which cyber was 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.

In this 4th edition of the survey, we see that, in addition to cyber strategy being essential to unlocking greater business value, cybersecurity in practice has become increasingly integrated into technology transformation activities. We also see that the voice of cyber leadership—in particular, the CISO—has grown in importance, along with the emergence of a new cyber-savvy C-suite.

Despite the growing focus on cybersecurity, only about half (52%) of all respondents are very confident in the C-suite and board's ability to adequately navigate cybersecurity. And specifically among C-suite respondents who are focused mainly on cybersecurity, only 34% are very confident—suggesting that they have less confidence in their abilities than others do.

But when we look just at organizations that Deloitte has classified as having high cyber maturity, we see two important findings: Cybersecurity is recognized at senior levels, and there is a strong correlation between organizations' cyber maturity and having greater confidence in adequately navigating cybersecurity. In fact, among high-cyber-maturity organizations, that confidence in the C-suite and board grows to 82%—compared to 52% and 39% for medium- and low-cyber-maturity organizations, respectively.

The survey's findings indicate that, on average, 86% of respondents are implementing actions to a moderate or large extent to increase cyber strategies and actions, embracing cyber as an essential component of the enterprise. And, on average, 85% of respondents expect to achieve their desired business outcomes to a moderate or large extent. While this underscores the critical role cyber plays in driving successful strategy implementation, not all organizations will realize those benefits equally.

And the more cyber-mature the organization, the bigger the potential impact. The survey found that respondents in high-cyber-maturity organizations anticipate almost two times the positive business outcomes compared with their peers. How these high-cyber-maturity organizations view cybersecurity—and how they are taking action—provides insights and a potential path for others to follow as they seek to increase their own cyber maturity.

52%

of respondents are very confident in the C-suite and board's ability to adequately navigate cybersecurity.

Respondents in high-cyber-maturity organizations anticipate almost **two times** the positive business outcomes compared with their peers.

Being more cyber mature does not make these organizations immune to threats. It makes them **more resilient** when they occur, to enable critical business continuity.

Cyber-mature organizations are more prepared and resilient

In this edition of the survey, Deloitte identified high-cyber-maturity organizations based on several factors. As in the previous edition of the survey, we assessed their level of strategic cybersecurity planning and specific cybersecurity activities, and engagement in cybersecurity at the board level. Based on these factors, among the most cyber-mature organizations, there is a clear sign that cybersecurity's influence in supporting and shaping technology-driven projects has grown by three percentage points.

However, given the rapid advancement in artificial intelligence (AI) technology, global organizations have experienced more sophisticated attacks. At the same time, opportunities have emerged to invest in AI-powered tools and cybersecurity solutions. Accordingly, we have updated the Deloitte cyber maturity index to include the extent to which respondents use AI capabilities within cybersecurity programs (see Cyber Maturity, page 25).

Among these high-cyber-maturity organizations, the CISO and other cybersecurity leaders are being called in as experts to help guide investments in cloud-driven business initiatives, AI-enabled activities, enterprise resource planning (ERP) modernization, and other digital transformation priorities. Put another way, cybersecurity is playing a large role in helping to secure funding for technology capabilities. The heightened focus on cybersecurity also means that the CISO is more involved in strategic conversations related to digital transformation.

While these high-cyber-maturity organizations are implementing foundational cyber actions—such as having a strategic and operational plan, cyber risk monitoring, and more—what is most notable is their ability to bounce back rapidly from cyberattacks. Being more cyber-mature does not make these organizations immune to threats. It makes them more resilient when they occur, to enable critical business continuity.

As compared to overall survey respondents, high-cyber-maturity organizations expect to achieve business outcomes by 27 percentage points more, on average, than global respondents overall. And they maintain those expectations despite reporting 11 or more cyber breaches in the past year (eight percentage points more than overall) and despite suffering negative consequences (on average seven percentage points more than overall). It may be that high-cyber-maturity organizations are identifying more cyber breaches—and therefore reporting more—not necessarily experiencing more.

The leaders of high-cyber-maturity organizations understand that being prepared to respond to and recover from the inevitable attack—to get their businesses back up and running quickly, and to serve their customers—is what matters most.

What are organizations hoping to prepare for (or avoid) as they become more resilient—and how has the picture changed? Compared with the previous edition of the survey, a loss of confidence in tech integrity (i.e., reliability, accuracy, and availability of systems and data) has risen to the top of the list as the number one negative consequence of cybersecurity incidents or breaches—becoming increasingly important as organizations accelerate their digital transformation journeys.

Operational disruption, including supply chain or partner ecosystem disruption, remains high on the list, in the number two spot, underscoring the importance of business continuity across partners and infrastructure. However, there is also a notable shift, as this was the top concern in the previous edition of the survey. Reputational loss climbed up one place as the number three concern (Figure 1).

The steps organizations take today should focus on how cyber investments can optimize, preserve, protect, and create value for the organization. That includes laying a strong foundation for future growth through cyber practices that enable data security and integrity across digital products and infrastructure. That foundation also should incorporate the fundamentals of a responsive infrastructure and digital ecosystem—for enabling future growth and business resilience. This edition of the survey shows a marked trend toward cyber programs and CISOs gaining greater strategic influence across all these value streams through more integrated technology transformation strategies—especially among the most cyber-mature organizations.

An effective approach to cybersecurity should extend beyond the traditional focus on incident response. It should delve into the core of how businesses need to integrate cyber—risk, security, and trust—into their overall strategy. Adopting a holistic, business-oriented perspective allows you to bridge broader business objectives and operational needs. This approach ensures that cyber is not just a reactive measure but a proactive, integral part of the organization's strategic business, technology, and operational framework. Moreover, Deloitte's research illustrates that the most cyber-mature organizations in the market are gaining significant value through a similar business-oriented approach.

WHERE ORGANIZATIONS ARE FEELING THE PAIN (FIGURE 1)

Cybersecurity incidents and breaches are resulting in these top negative consequences for survey respondents.

Negative consequences resulting from cyber incidents and breaches	3rd Edition (Rank)	3rd Edition (Percent)	4th Edition (Rank)	4th Edition (Percent)
Loss of confidence in tech integrity	6	55%	1	66%
Operational disruption *(including supply chain/or partner ecosystem)*	1	58%	2	66%
Reputational loss	4	55%	3	65%
Negative talent recruitment/retention impact	7	54%	4	64%
Loss of revenue	2	56%	5	64%
Loss of customer trust/negative brand impact	3	56%	6	63%
Intellectual property theft	8	54%	7	63%
Regulatory fines	10	52%	8	63%
Drop in share price	9	52%	9	63%
Defunding of a strategic initiative	5	55%	10	63%

"Our threat surface is quickly increasing. As we connect our factories with new technologies, new risks emerge. As soon as we tie in a supplier's robot who wants to call back to the manufacturer for maintenance or push a software package to an assembly line component, things gets much more complicated."

—Kevin Tierney, Chief Cyber Security Officer, General Motors

HOW WE DEVELOPED THE INSIGHTS

Behind the research

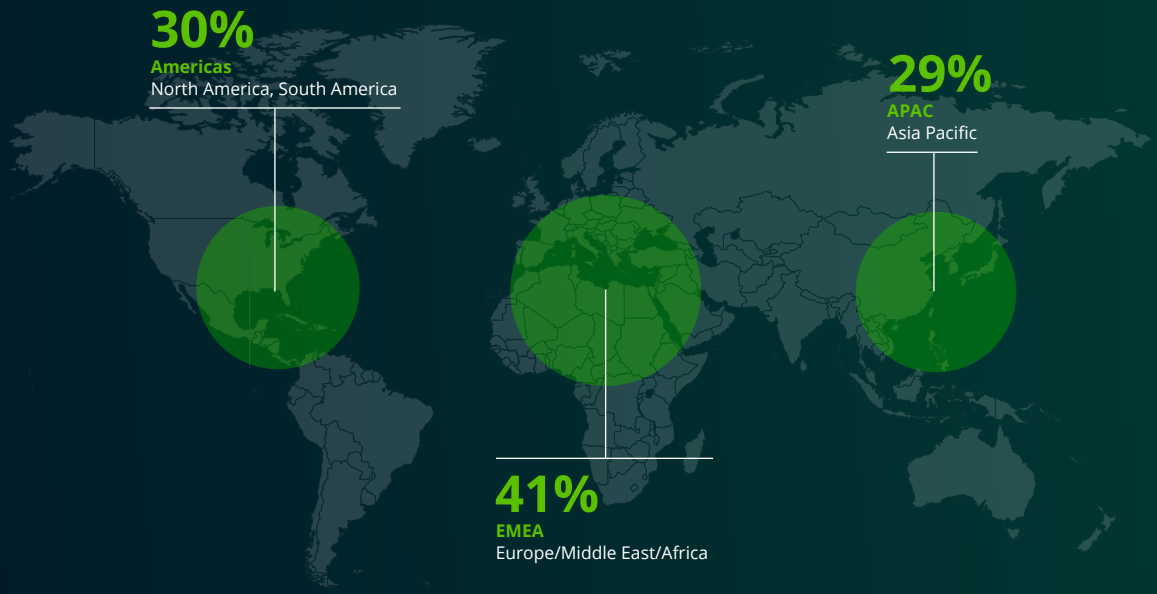
Deloitte designed the 4th Edition of The Global Future of Cyber Survey based on the complexity of today's business and technology landscape, focusing on the needs of enterprise leaders who may recognize the importance of cybersecurity yet struggle to harness its value.

Deloitte based its research on a survey of nearly 1,200 cyber decision-makers at the director level or higher, including C-suite executives and their direct reports, covering a mix of business and IT functions. The survey reflects data gathered across 43 countries and six industries, and is limited to organizations with at least 1,000 employees and US$500 million in annual revenue.

Deloitte also conducted in-depth interviews with 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 and culture to technology implementation.

At the core of this research, we focused our efforts on exploring how cybersecurity has changed since the last edition of our report while applying a forward-looking lens, to help bring the future of cyber into sharper focus. We also wanted to get a clearer view into the cyber savviness of the C-suite today. Throughout the survey, we have looked to unlock insights for better understanding the cyber-related business value and impact organizations are experiencing, as well as the distinct actions that leading organizations are taking to increase value.

Headquarters locations of the organizations we surveyed



CYBER INFLUENCES STRATEGIC VALUE

Working toward a bigger business impact

The path to cyber maturity is becoming even clearer as we look toward the future of cyber. Organizations that travel along that path will integrate cybersecurity risk strategies, security practices, and trust-building approaches into their business and technology transformation—enabled by a cyber-savvy C-suite and highly influential CISO. Those organizations can expect to see a bigger impact when it comes to measures of success, positioning their organizations to undertake transformation more effectively in a rapidly evolving digital landscape.

As organizations take continuous steps toward becoming cyber mature, they can set themselves apart from their peers by prioritizing and building cybersecurity connections across their business and technology operations, and their leadership. Doing so will enable them to more successfully achieve the strategic outcomes that we saw being prioritized in the previous edition of the survey.

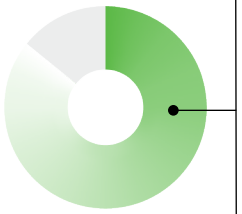
In this report, we will explore high-level insights grounded in data from the survey, the cyber maturity index, and insights from global leaders, to show how and where high-performing organizations are standing out and to guide global cybersecurity professionals on how to become more mature in their cyber practices.

We will examine how...

1. Cybersecurity remains an essential element for strategic business value—and the focus is intensifying.
2. The CISO's influence is growing across an increasingly cyber-savvy C-suite.
3. Cybersecurity has become deeply integrated with tech-driven programs and digital business transformation.
4. Organizations with greater cyber maturity are more confident and realizing greater benefits from their cyber actions and investments.

CYBERSECURITY REMAINS AN ESSENTIAL ELEMENT FOR STRATEGIC BUSINESS VALUE—AND THE FOCUS IS INTENSIFYING.

The foundational importance of cybersecurity is undeniable in today's deeply interconnected digital environment. And organizations have no shortage of activities/actions and strategic levers they can pull to bolster their cyber readiness to enhance business value.



86%

of respondents reported implementing specific activities/actions to a moderate or large extent to increase cybersecurity.

Taking action is a first step, but not the only step

Most respondents are taking the need for cybersecurity action seriously, with 86% of them implementing specific activities/actions to a moderate or large extent to increase cybersecurity. This level of action suggests that organizations overwhelmingly understand the need for these activities and a robust cybersecurity program to implement them. It also suggests that they are keeping pace as the list of activities they need to stay on top of continues to grow.

These respondents are focusing on a variety of activities for managing cybersecurity, including but not limited to: mitigating risks, enhancing cybersecurity controls, improving incident response, increasing employee awareness, and adopting a strategic cybersecurity plan.

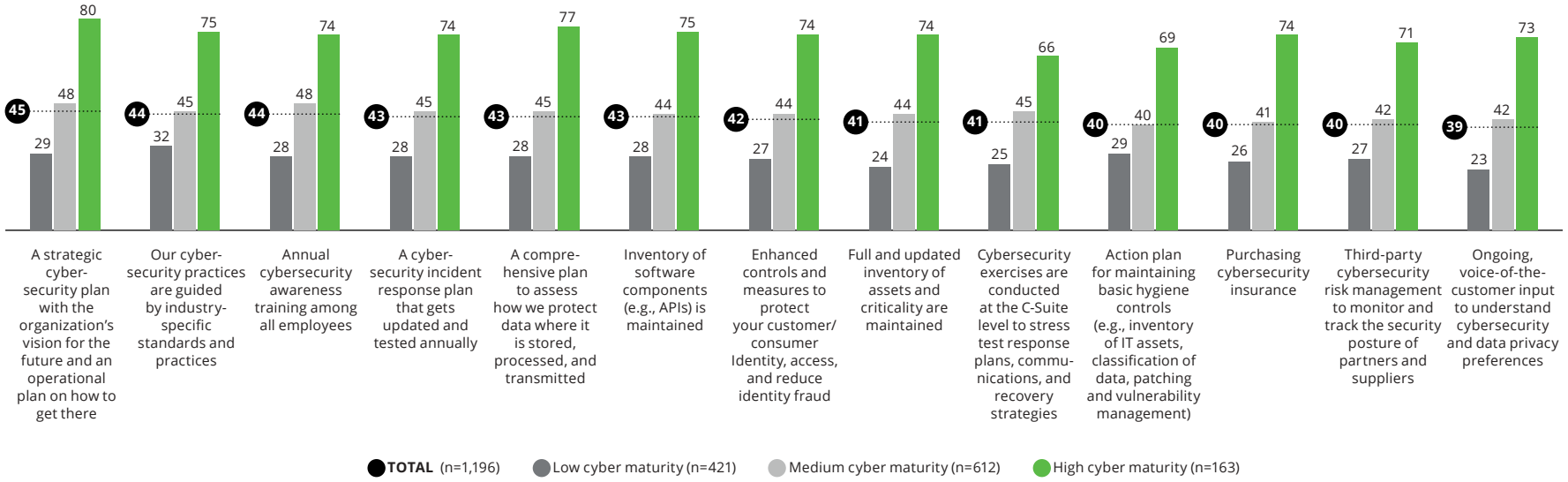
When we project those activities through the lens of cyber maturity, we see that organizations with high cyber maturity undertake these actions to a greater extent compared to less cyber-mature organizations (Figure 2, see also Cyber Maturity, page 25).

> **"It's really about getting the basics right and maturing them and being excellent at them, every day, consistently. Things like foundational controls, asset management, vulnerability management. You really need to excel there, almost mindlessly. They just have to happen"**
>
> **—CISO, Life Sciences and Healthcare Organization**

CYBERSECURITY ACTIVITIES AND THE CONNECTION TO MATURITY (FIGURE 2)

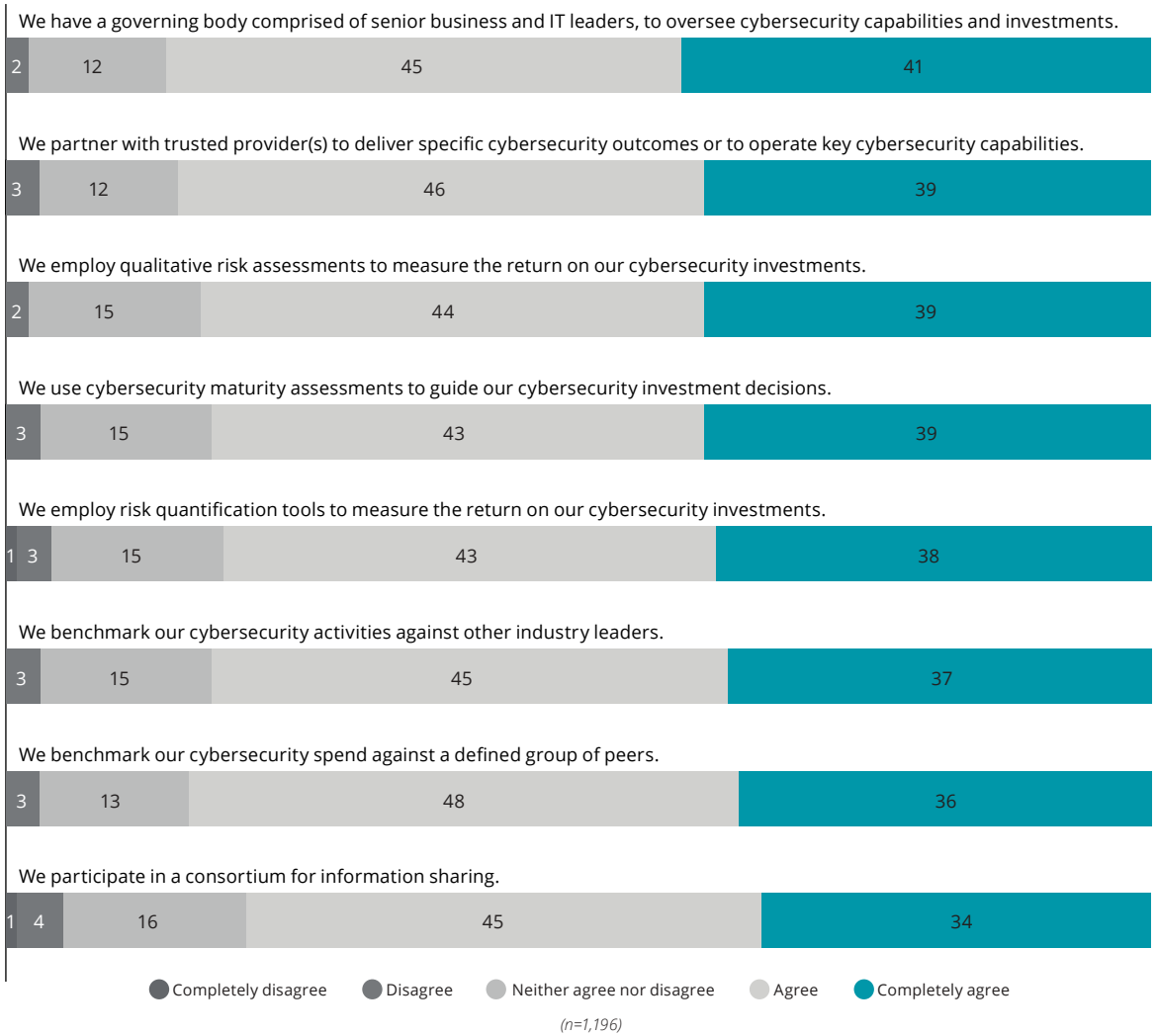
Organizations with high cyber maturity are engaging in these key cybersecurity activities to a greater extent compared to less cyber-mature organizations.

(Percentage)



GETTING STRATEGIC ABOUT CYBERSECURITY (FIGURE 3)

The specific strategies respondents say they are undertaking to enhance and improve cybersecurity.



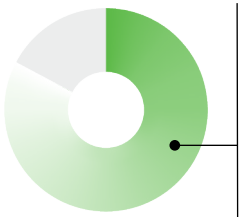
(n=1,196)

Note: Percentages may not add up to 100% due to rounding.

Guided by strategy, cybersecurity execution gets more integrated across the business

The overwhelming majority of organizations are also embracing a number of strategic cyber actions including: benchmarking and measurement, collaborating with trusted providers, participating in consortia for information sharing, and establishing governing bodies that comprise senior business and IT leaders to oversee cybersecurity capabilities and investments.

Overall, 83% of respondents surveyed agree or completely agree that such measures are an integral part of their overall cybersecurity strategy. This level of agreement suggests continued integration of cybersecurity strategy into the business.



83%

of respondents overall agree that these measures are an integral part of their overall cybersecurity strategy.

Eyeing bigger cybersecurity investments amid increasing threats

More than half of the global respondents surveyed (57%) anticipate increasing their budget for cybersecurity over the next 12 to 24 months. Fifty-eight percent of respondents also indicated that they expect to begin integrating their cybersecurity spend with budgets for other programs, such as digital transformation initiatives, IT programs, and cloud investments. This level of investment and budget integration underscores the increasingly interwoven nature of cybersecurity activities across the business. It also emphasizes the reality that cyber funding is a zero-sum game, as cybersecurity is often overlooked during transformation projects, to save costs in a zero-sum environment.

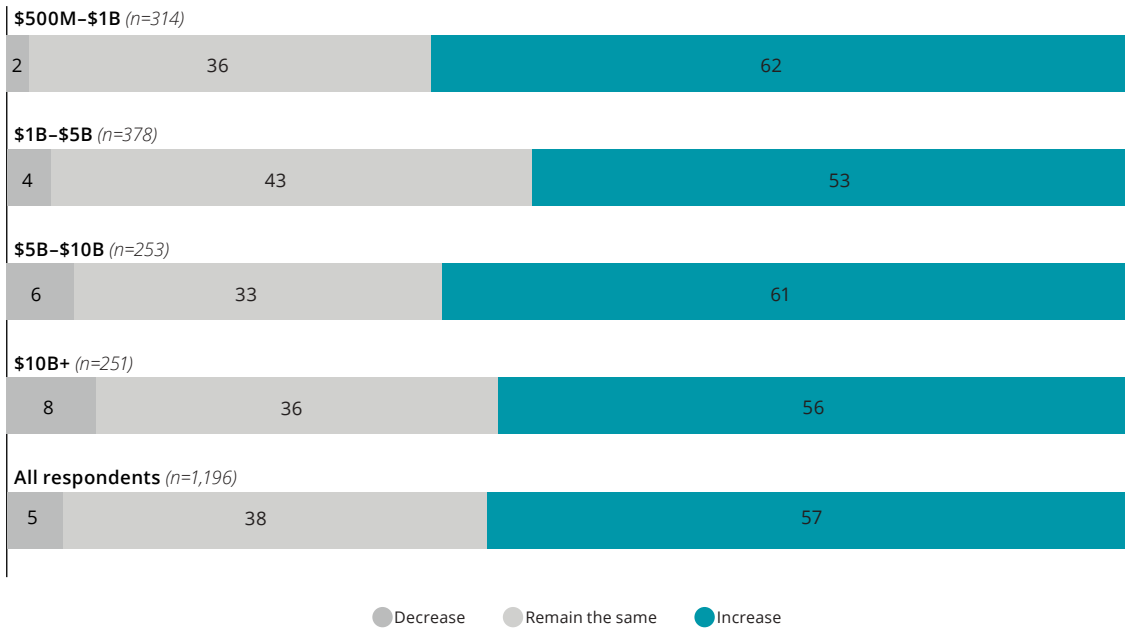
Continuously prioritizing and building cybersecurity connections across business and technology operations, as well as leadership, is crucial for organizations to differentiate themselves and achieve strategic outcomes successfully. A cyber-mature organization understands that cybersecurity is not just an IT issue but a business-critical imperative that requires integration across all functions and levels of the organization. By fostering such strong cybersecurity connections, organizations can enhance collaboration, information sharing, and decision-making related to cybersecurity.

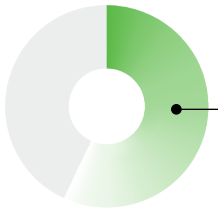
This approach enables leaders to make informed strategic decisions that align with business objectives and mitigate cyber risks effectively. Ultimately, organizations that prioritize cybersecurity and build strong cybersecurity connections—integrating cyber across enterprise functions and leadership roles—can better protect their assets, reputation, and overall resilience in an increasingly digital world.

SPENDING ON THE RISE (FIGURE 4)

57% of respondents anticipate increasing their cybersecurity budgets over the next 12 to 24 months.

(In US dollars and percent)





57%

of respondents anticipate increasing their budget for cybersecurity over the next 12 to 24 months.

"As companies differ across factors such as size, type of data they possess, online presence, and supply chain practices, their threat profiles will be unique. It's imperative every company have a strong threat intelligence strategy that includes understanding who cares about them and why, and how they operate. Understanding the motivations and tactics of potential attackers is crucial for effective security measures."

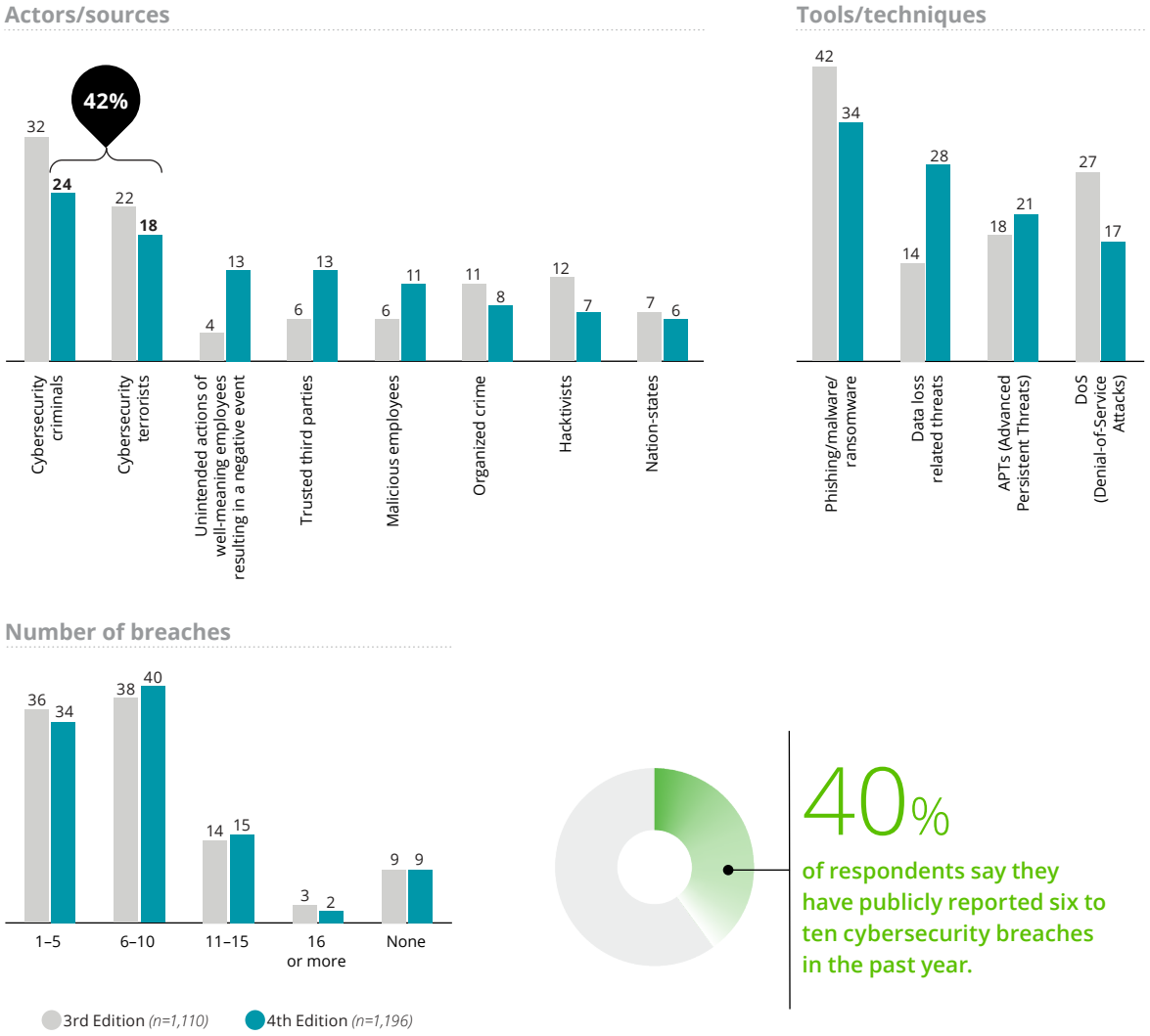
—Gary Harbison, Chief Information Security Officer, Johnson & Johnson

We found that on average, overall respondents are spending between US$147 million and US$266 million annually on IT. Of that, 19% (US$39 million) is allocated for cybersecurity related activities, and respondents expect to increase that by 3% in the next 12–24 months.

THE THREATS THAT ARE BREAKING THROUGH (FIGURE 5)

Where cybersecurity breaches are coming from—and how many organizations are experiencing them.

(Percentage, 3rd edition vs. 4th edition)



40%

of respondents say they have publicly reported six to ten cybersecurity breaches in the past year.

Attack realities are growing, including new threats and cyber risks related to Generative AI (GenAI)

The expected increase in investments comes as organizations experience a growing and diverse mix of cyber threats. Similar to the previous edition of the survey, cyber criminals and terrorists make up the top threat actors. They were reported by 42% of respondents as the leading concern across a diverse set of threat actors, which included hacktivists (threat actors aiming to make a statement related to political or social causes), cyber criminals (perpetrating malicious activities for financial profit), and insiders (with personal grievances and gains at stake).

As for the tools and techniques employed by cyberattackers, phishing, malware, and ransomware combined emerged as the top threat vector, reported by 34% of respondents. That level is down eight percentage points from the previous survey, coinciding with a significant jump in reported threats related to data loss—up from 14% in the previous survey to 28% in this survey.

Meanwhile, 40% of respondents said they have publicly reported six to ten cybersecurity breaches in the past year—an increase of two percentage points compared to the previous survey. And it is no surprise that attacks continue to trend upwards. The attack surface available to threat actors is large and continues to grow.

The survey also tracks how respondents are responding to new cyber risks arising from the emergence of GenAI. The analysis shows awareness of these risks is more pronounced among high-cyber-maturity organizations versus less-mature counterparts. Among the most cyber-mature organizations, these are the top four GenAI-related risks that respondents believe will impact their cybersecurity strategy:

- Explainability in GenAI outputs (82%)
- GenAI algorithms introducing information integrity risks (81%)
- Effectively developing controls related to GenAI and humans working together (81%)
- Data poisoning (e.g., corrupting the training data set to influence GenAI outputs) (80%)

As more organizations automate their processes and share their data with suppliers and other third parties, new vulnerabilities can emerge. These increasingly complex digital infrastructures and ecosystems introduce new opportunities for attack.

> **"Everything—and everyone is so interconnected, that the risk is magnifying. Think about our entire supply base. Think about all the levels of security capabilities across the whole spectrum of companies out there. We feel pretty good about what is happening on our campus and with our employees. But how do we ensure everyone coming in contact with our network has the same level of capability and capacity to deal with security and controls?"**
>
> **—Patrick Milligan, Chief Information Security Officer, Ford Motor Company**

Technology integrity is the top concern among respondents as expectations for the benefits to be gained from cyber programs grow

Amid the persistent web of threats, organizations are experiencing a range of negative effects, including impacts across three domains—financial, operational, and brand (Figure 6). Overall, across all three of these domains combined, the top two concerns are loss of confidence in tech integrity and operational disruption (Figure 1, page 7). This continued focus underscores the importance of having strong cybersecurity programs that can maintain critical technologies and operations, and boost business resilience.

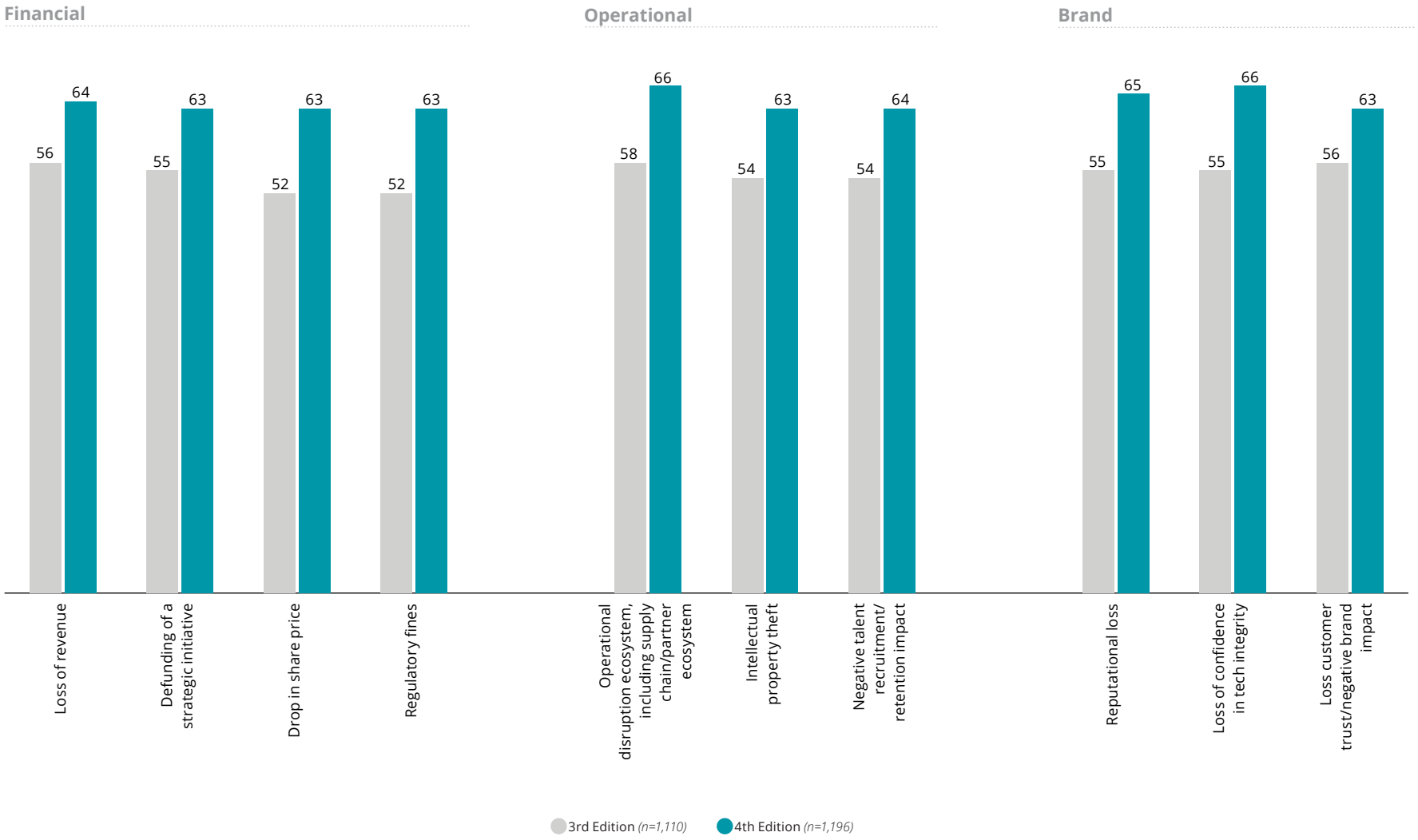
Respondents are experiencing all negative consequences to a higher extent than in the previous edition of the report. On average, 56% experienced all these consequences to a moderate and large extent in the 3rd edition of the report, compared to 64% in the 4th edition.

This increase points to two potential realities. First, organizations might be more comprehensively reporting the impact from cyberattacks, signaling increased awareness. Second, the attack surface and frequency has increased due to GenAI and other advanced technologies, which highlights the growing importance of cybersecurity in the future and provides a clear call to action for putting in place robust cybersecurity plans.

TAKING A CLOSER LOOK AT THE NEGATIVE CONSEQUENCES, THROUGH THREE LENSES (FIGURE 6)

Where respondents see cybersecurity incidents having the biggest impact across financial, operational, and brand areas.

(Percentage)



These negative consequences from incidents or breaches sharply contrast with the benefits—positive business outcomes—that organizations expect to achieve with their cybersecurity initiatives. According to the survey, the top three expected outcomes of cybersecurity initiatives were (1) protecting intellectual property, (2) improving threat detection and response, and (3) increasing efficiency and agility (Figure 7).

The expected benefits speak to the enhanced operational resilience many respondents are seeing from their cybersecurity investments, with some variance by industry:

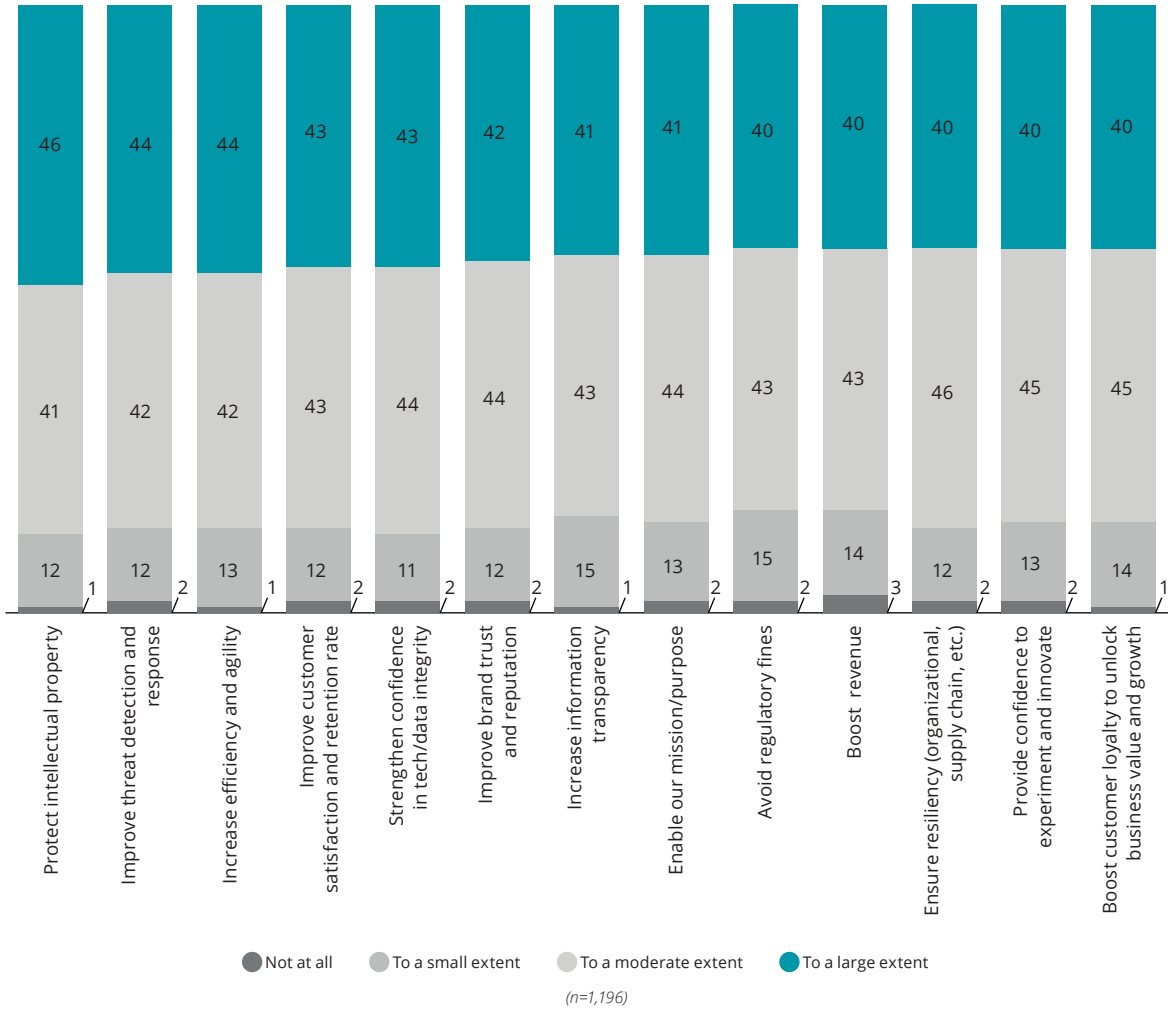
Consumer	Energy, Resources & Industrials (ER&I)	Financial Services Industry (FSI)	Government & Public Services (GPS)	Life Sciences & Health Care (LSHC)	Technology, Media & Telecom (TMT)
Strengthening confidence in tech/data integrity	Increasing efficiency and agility	Improving threat detection and response, tied with protecting intellectual property	Protecting intellectual property	Improving customer satisfaction and retention rate	Increasing efficiency and agility

The hopes for cybersecurity are clearly high. As the primary owner of the cyber function, those expectations are directed at the CISO, who faces a massive job in managing and achieving business expectations. For any organization, a breach or incident will be inevitable, but the promise of cybersecurity is to minimize the risks and negative impacts and maximize as many benefits as possible—ultimately enabling a more secure and resilient organization operating with trusted data for use in driving growth.

EXPECTING OUTCOMES FROM CYBERSECURITY (FIGURE 7)

The benefits that respondents anticipate from cybersecurity initiatives—and the degree to which they are expecting them.

(Percentage)



(n=1,196)

THE CISO'S INFLUENCE IS GROWING ACROSS AN INCREASINGLY CYBER-SAVVY C-SUITE.

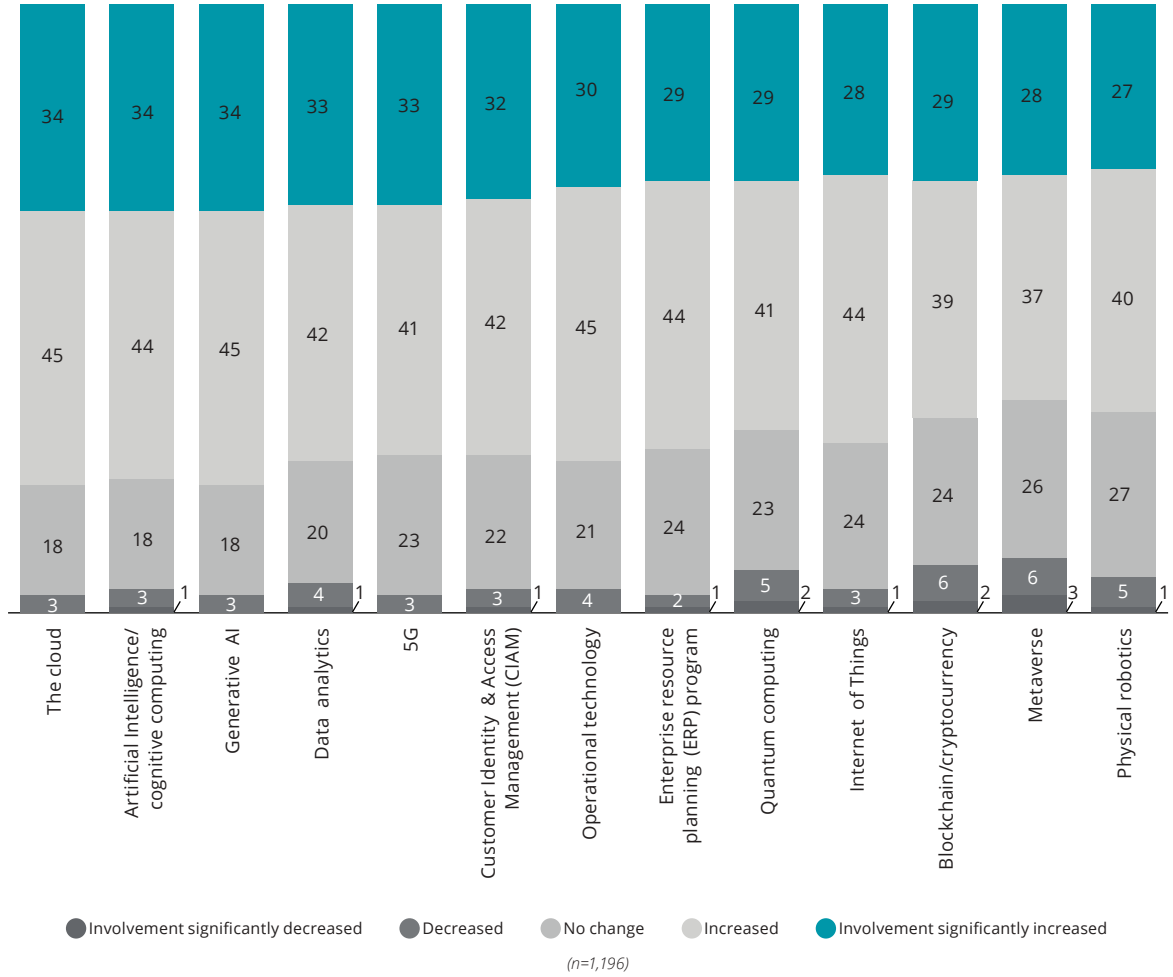
Survey respondents indicated that in their organization the CISO tends to hold the primary responsibility for the majority of cybersecurity activities asked about in our survey, with chief information officers (CIOs) also playing a key role. Often, those CISOs report to CIOs or to chief technology officers (CTOs). Approximately one-fifth of CISOs, however, report directly to the chief executive officer (CEO), according to the survey. This is an important signal of business alignment, with influence across the C-suite and executive leadership.

The influence of the CISO appears to be growing in other ways, too. The CISO, or equivalent leader, is increasingly involved in strategic business conversations about technology capabilities, reflecting their growing importance in driving business value.

CISO involvement is no longer optional

Roughly one-third of respondents said CISO involvement had significantly increased in the past year when it came to strategic conversations about the following technology capabilities: cloud, AI/cognitive computing, GenAI, data analytics, 5G, and customer identity and access management (Figure 8).

BRINGING THE CISO INTO STRATEGIC CONVERSATIONS (FIGURE 8)
Areas in which CISOs are involved in discussions on business-critical technology capabilities—and the degree to which they are involved.
(Percentage)



(n=1,196)

As the CISO's voice of influence grows across leadership, and as organizations seek to become more cyber-savvy, we foresee them becoming an essential partner to advise and educate the board of directors and the C-suite on security vulnerabilities, risk scenerios, and actions needed for greater resilience. In the future, the CISO will be expected to not only lead the organization's overall cyber security strategy, but will also provide strategic guidance, collaborating closely with other C-suite executives to align security initiatives with business goals.

Among C-suite executives focused on cybersecurity, only 34% are very confident their C-suite and board can adequately navigate cybersecurity. They are 18 percentage points less confident than respondents overall (Figure 9).

The analysis indicates that cyber-mature organizations understand that the role of the CISO has become crucial to engaging the C-suite and the board, and key to addressing cybersecurity risks effectively. They recognize that, in taking on a more influential role, the CISO can provide valuable insights and guidance, and ensure that cybersecurity receives the attention and resources it deserves—as a strategic business issue requiring continuous attention and investment. While Deloitte sees this trend with the CISO role growing, we recommend organizations accelerate their actions to elevate the CISO's role, given the evolving nature of cyber threats, technology capabilities, and cybersecurity's integration with the business.

While most say the CISOs role is evolving, and they have a seat at the table, there is still a lack of confidence that the C-suite can confidently navigate today's complex cyber environment. These lower confidence levels could indicate a sobering of the C-suite to the complexity of today's cyber landscape as CISOs effectively educate them to risks/threats and the organization's ability to address them as well as an over-confidence in the organizations' cyber maturity and resilience among respondents overall.

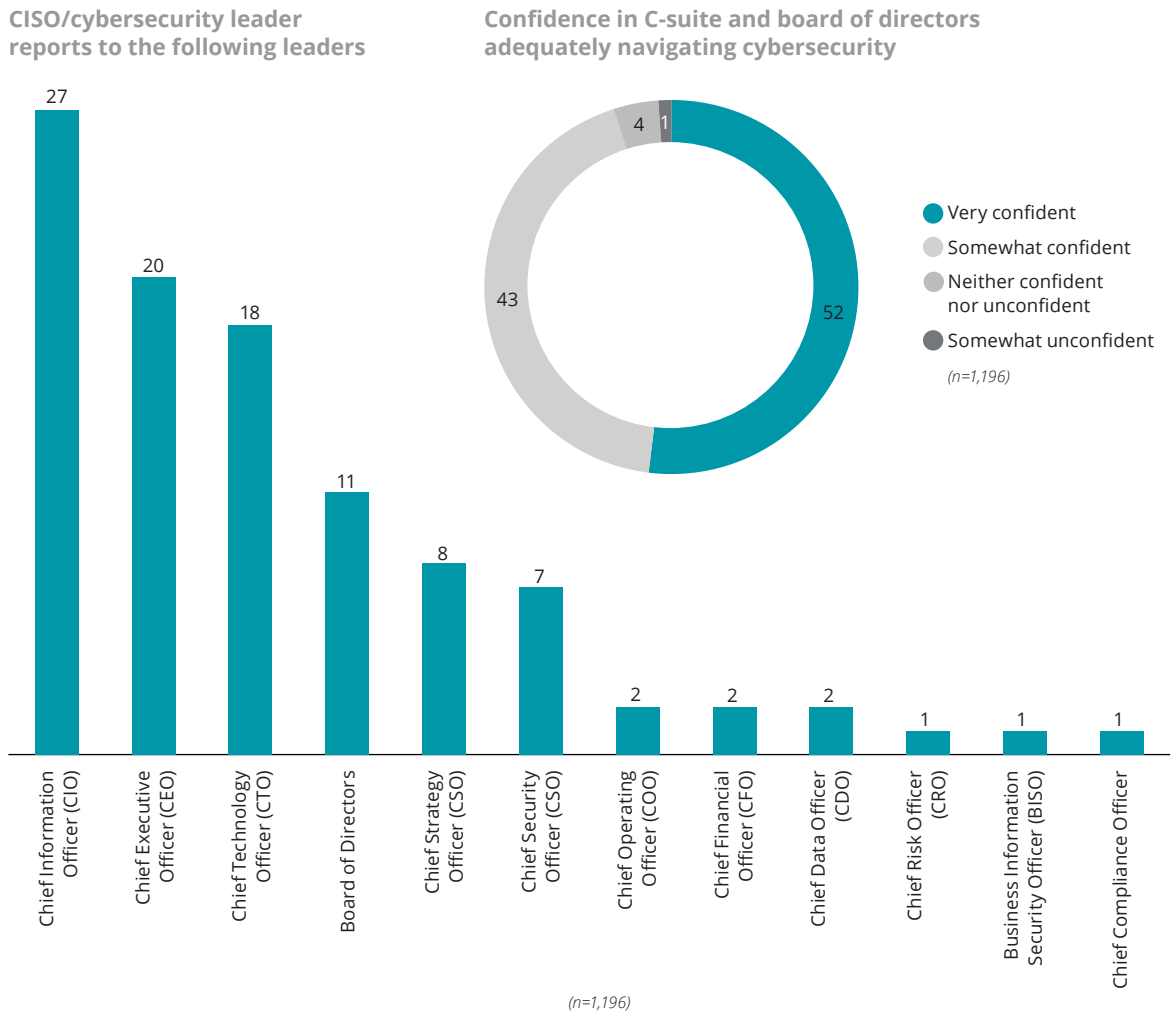
> **"The big shift for us is by bringing in the security discussion before, not after, building the solution. We really want to move into 'security by design' as opposed to what often happens—'security during assessment'—which requires security to be more of a strategic part of the overall business."**
>
> **—Director General, Cyber and IT Security, Government and Public Services Agency**

CYBERSECURITY SAVVINESS IN THE C-SUITE AND A LOOK AT THE CISO'S REPORTING ALIGNMENT

(FIGURE 9)

A look at the level of confidence leaders have in the C-suite, as well as an overall view on who CISOs report to.

(Percentage)



While cybersecurity is a staple on the board's agenda for most organizations, with 88% of respondents saying that their boards are addressing cyber-related issues quarterly, if not more often, there's clearly room for greater education and for the CISO to advise on strategic risks and corresponding actions. On this point, Deloitte's *Tech-Forward Boardroom* report recommends that to elevate boardroom conversations, tech leaders can translate technical jargon to business needs, partner more closely with the CFO to articulate business impacts, consistently structure reporting and benchmarking, co-present to the board, workshop through deep-dive technology sessions, create feedback loops, and cascade these activities across small board sessions and meetings.

"We have standard, quarterly updates with the board, and that did not exist a few years ago. I would say the depth of the discussion, not just frequency, is greater now as well. We have many more deep dives on key topics that the board now has questions about. We end up scheduling more time to go deeper."

—Chief Information Security Officer, Financial Services Corporation

88%

of respondents say that their boards are addressing cyber-related issues quarterly, if not more often.

While most say the CISO's role is evolving and they have a seat at the table, there is still a **lack of confidence** that the C-suite can confidently navigate today's complex cyber environment.

CYBERSECURITY HAS BECOME DEEPLY INTEGRATED WITH TECH-DRIVEN PROGRAMS AND DIGITAL BUSINESS TRANSFORMATION.

The boundaries of cybersecurity are blurring, just as the lines of digital transformation are blurring. As organizations share data and systems access with partners and other third parties, concerns about security and privacy are paramount. Ultimately, the growth of business, customer, data, and digital trust depends on cyber. Accordingly, many organizations are integrating cybersecurity across business and technology functions (Figure 10).

"I always look at cyber as an enabler. If you want to drive fast on the highway, you need to make sure you've got bumpers and brakes and you know a number of things are working in your car, or you are not going to be able to stay on the road. Cyber acts as those bumpers or brakes to support the car (so you can drive at Internet speeds)."

—Vivek Khindria, SVP Cyber Security, Network, and Technology Risk, Loblaw

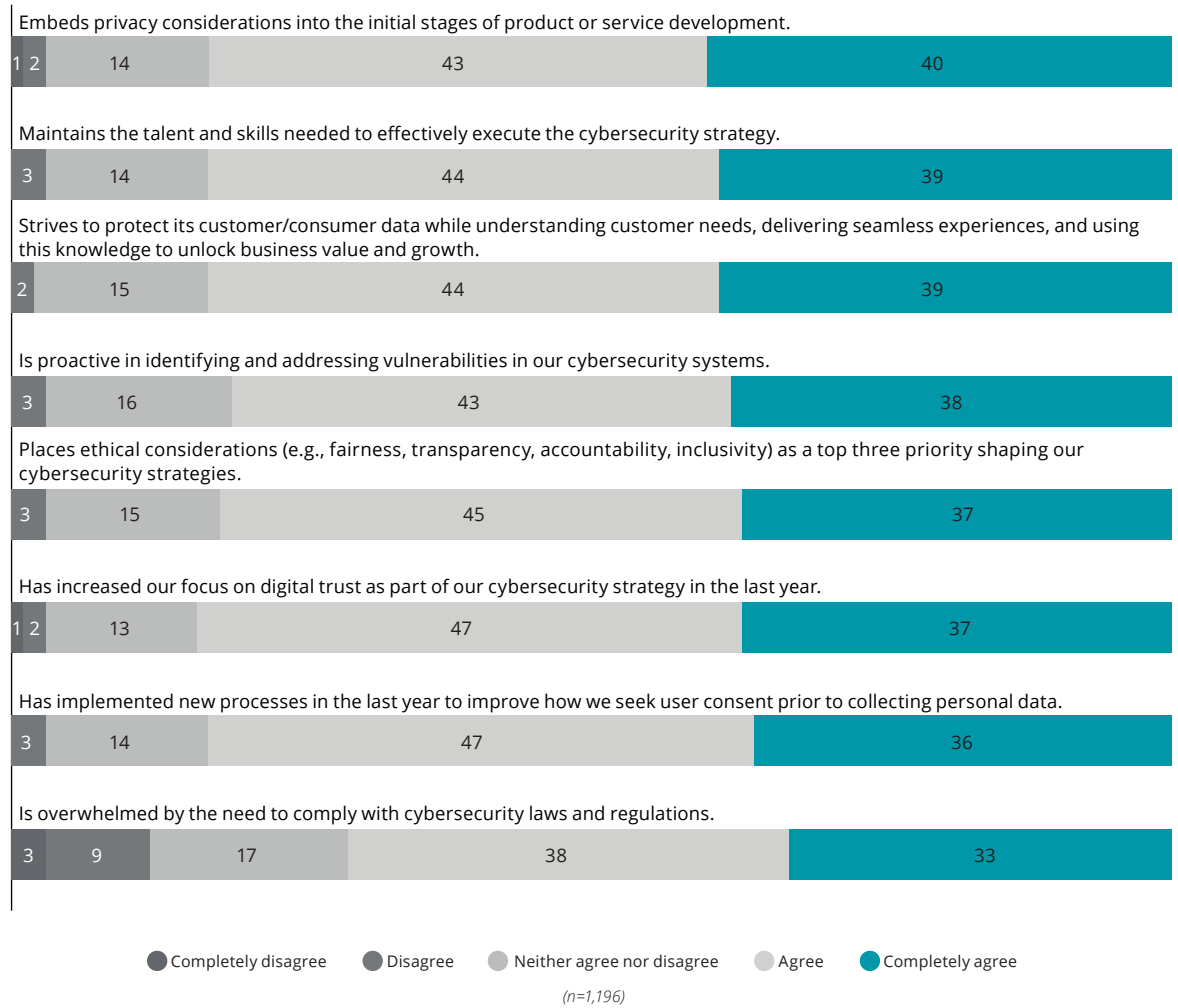
Integrating cyber across the business

Not only are organizations enhancing and securing their technological capabilities; they are changing the way they create new offerings. More than 80% of respondents say they are integrating privacy considerations into the early stages of product development, for example, which can help safeguard customer data and foster greater digital trust. Such considerations indicate that DevSecOps processes are reaching a new level of maturity, with cybersecurity leaders successfully embedded into product design and development teams (Figure 10).

PRIORITIZING PRIVACY, TRUST, AND ETHICS (FIGURE 10)

Most respondents are taking steps to integrate cybersecurity with needs such as product development, protecting customer data, and other key areas.

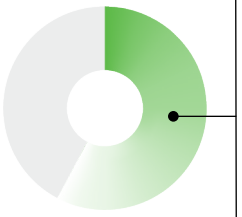
(Percentage)



(n=1,196)

The integration of cybersecurity into more aspects of the business extends to spending, as well. As previously noted, a majority of respondents (58%) expect cybersecurity spend will begin to become integrated with other budgets for initiatives such as digital transformation, IT programs, and cloud investments. At the same time, a majority (55%) also see spend remaining siloed (Figure 11).

Those two majority views are not at odds; 25% of respondents selected both options—integrated spending as well as siloed spending—when asked about the future of cybersecurity spend. That duality reflects what Deloitte sees across organizations, with cybersecurity spend often coming from a mix of dedicated cybersecurity budgets, as well as budgets for IT, digital transformation, business areas, and products. In other words, the scale of cybersecurity spend slices across many priorities, requiring leaders to explore different, often concurrent models, to finance it.



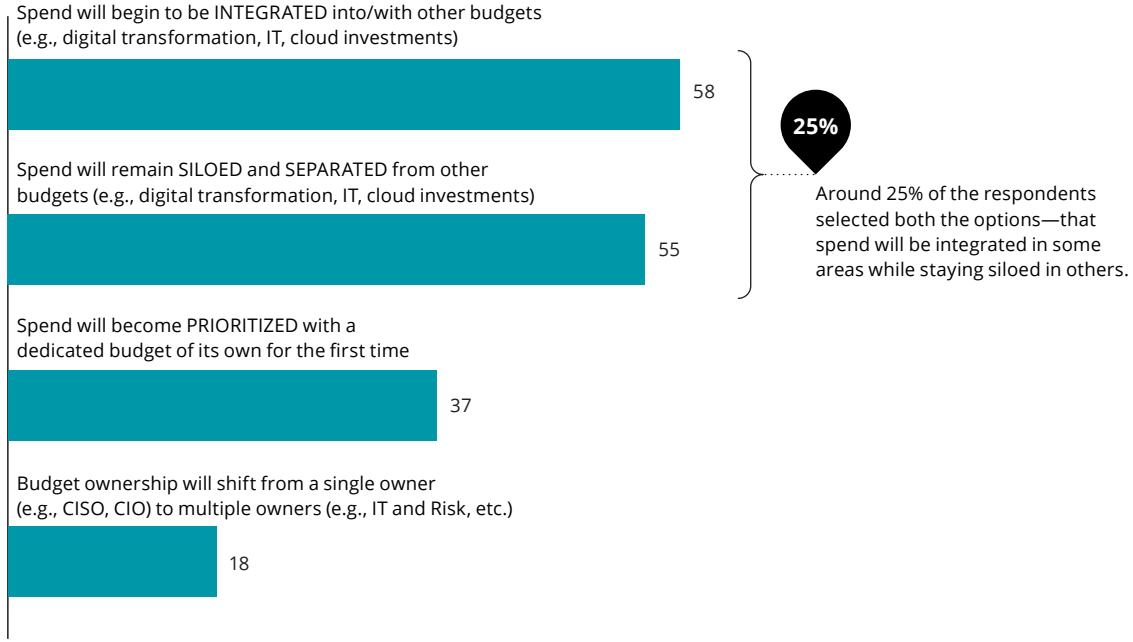
58%

of respondents expect cybersecurity spend will begin to become integrated with other budgets.

WHERE CYBERSECURITY SPEND AND DIGITAL TRANSFORMATION INTERSECT (FIGURE 11)

How do you see the evolving digital landscape impacting your organization's cybersecurity spend? Select all that apply.

(Percentage)

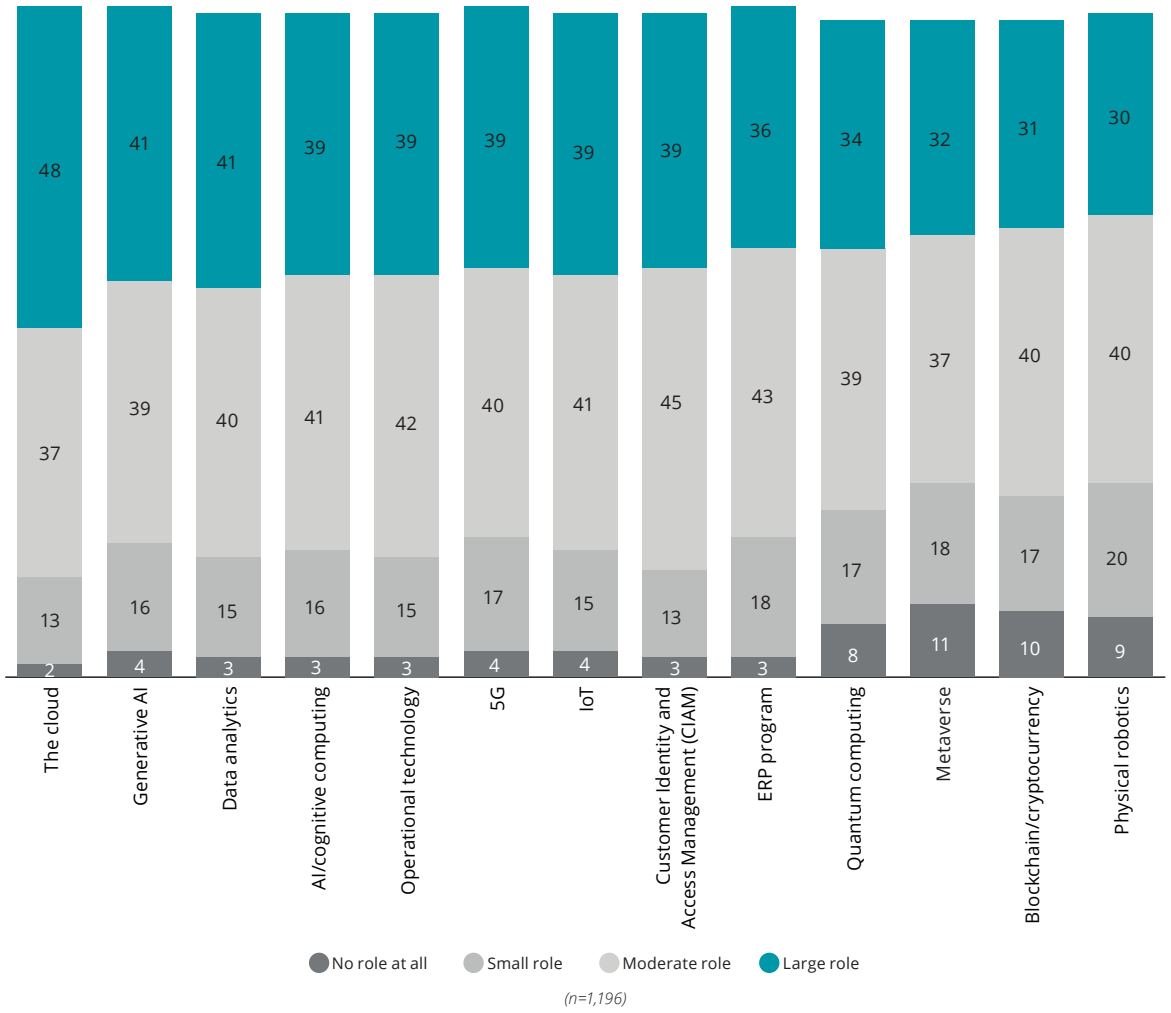


(n=1,196)

Note: Percentages may not add up to 100% due to rounding.

That march toward cybersecurity budget integration tracks closely with another emerging reality: Cybersecurity is a driver of business ambitions. Our survey results show that cybersecurity plays a large role in securing an organization's investment in technology capabilities—especially when it comes to the priority areas such as cloud (48%), GenAI (41%), and data analytics (41%) (FIgure 12).

THE ROLE CYBERSECURITY PLAYS IN SECURING TECHNOLOGY INVESTMENTS (FIGURE 12)
How cybersecurity is influencing decisions on budgets in technology capabilities.
(Percentage)



(n=1,196)

Note: Percentages may not add up to 100% due to rounding.

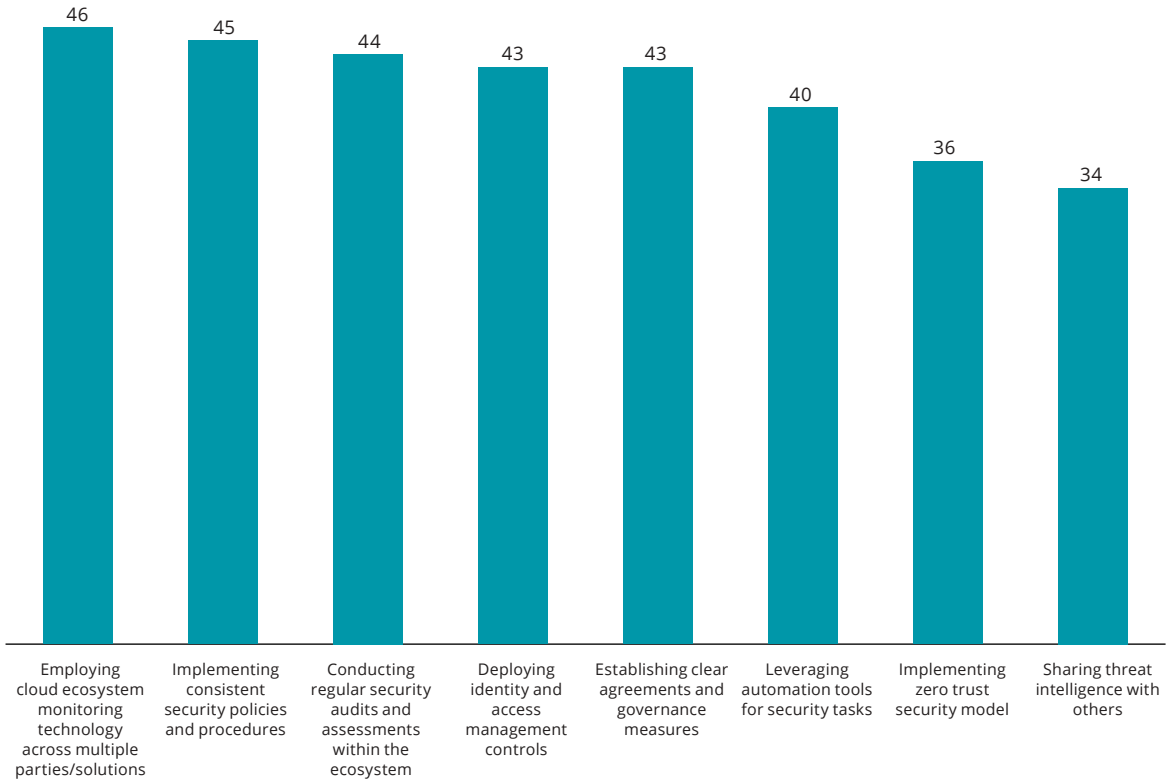
"For our group, which operates globally, strengthening security is a crucial activity that is essential for promoting digital transformation. We have established an internal structure called the JFE-Security Integration and Response Team, allocating resources such as budget and personnel, and implementing necessary measures in terms of human, technological, and physical aspects. We aim to enhance cybersecurity measures in various business activities, including the development, design, manufacturing, and provision of products, systems, and services. As a result, we contribute to strengthening cybersecurity throughout the supply chain and, ultimately, to the overall cybersecurity enhancement of society on a global scale."

—Akira Nitta, Chief Information Security Officer, JFE Steel

CYBERSECURITY ACTIONS TAKEN TO REDUCE CLOUD ECOSYSTEMS (FIGURE 13)

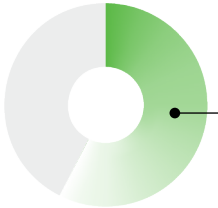
What cybersecurity actions is your organization taking to reduce complexity across your cloud ecosystems?

(Percentage)



(n=1,196)

When it comes to cloud technologies, cybersecurity has a major role to play as an enabler, helping bolster security while simplifying the cloud landscape overall for organizations. The top cybersecurity actions respondents are taking to reduce the complexity of cloud ecosystems include conducting regular security audits and assessments (44%), implementing consistent security policies and procedures (45%), and employing cloud ecosystem monitoring technology across multiple parties and solutions (46%) (Figure 13).



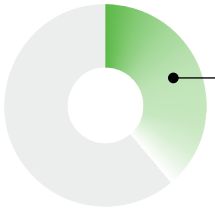
46%

of respondents reported employing cloud ecosystem monitoring technology across multiple parties and solutions.

Eye on AI-enabled cyber solutions

Given the importance of AI today, we included it in our index for cyber maturity in this edition of the survey. Some of the top ways organizations are focused on using AI to enhance cybersecurity capabilities include digital infrastructure monitoring, advanced simulations, and automated security.

Artificially generated content enables attackers to create customized content with a much lower time investment. A wave of artificially generated content is now targeting enterprises, exploiting vulnerabilities by impersonating trusted sources. The problem is accelerating rapidly. None of this means enterprises are powerless against the tidal wave of artificially generated content coming their way. Leading enterprises are taking proactive steps to make sure they don't become victims (Source: *Deloitte 2024 Tech Trends: Defending reality: Truth in an age of synthetic media*).



39%

of respondents, on average, reported using AI capabilities in their cybersecurity programs to a large extent.

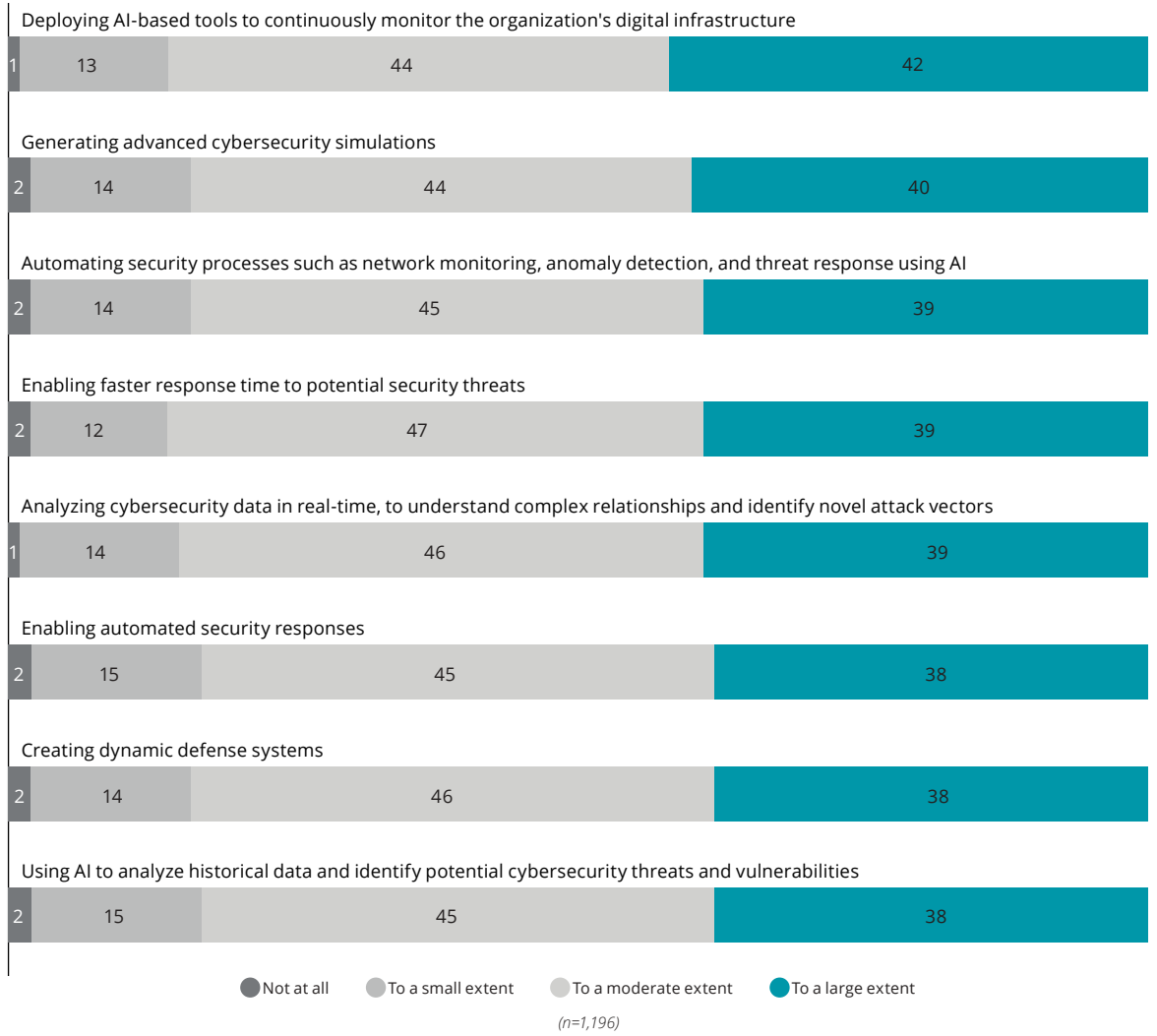
And while the future of AI is evolving, so too is the future of cyber. They are evolving together as organizations leverage novel AI solutions to ease the cybersecurity burden. Among survey respondents, 39%, on average, are using AI capabilities in their cybersecurity programs to a large extent. At the same time, respondents have also expressed concerns related to AI, expressing a need to update their cybersecurity strategies to keep up with continuous technology innovation (Figure 14).

> **"Of course, the focus is keeping the bad guys out. But we also have to look into the impact of these new technologies (like AI) and how that will impact our landscape. How do we make sure that we apply and use AI in a safe and secure manner, as well as how we use AI to better deliver security within our cyber framework?"**
>
> **—Director General, Cyber and IT Security, GPS Agency**

AI CAPABILITIES COMING INTO FOCUS (FIGURE 14)

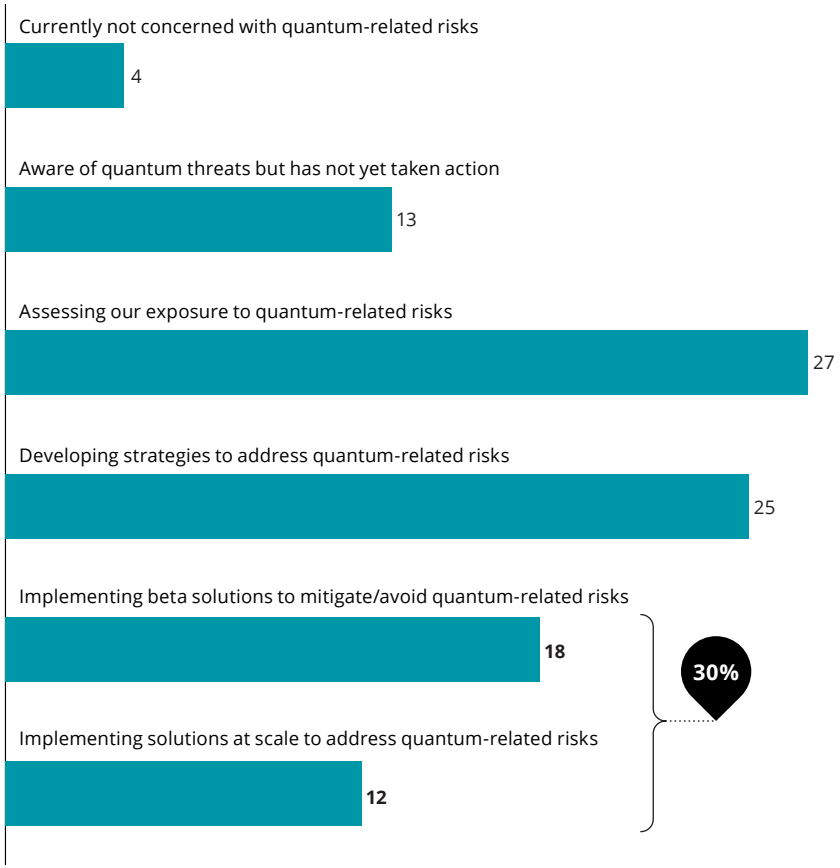
Where and how respondents are seeing AI emerge as a tool in their cybersecurity programs.

(Percentage)



(n=1,196)

THE QUANTUM CONNECTION (FIGURE 15)
How organizations are thinking about the approaching quantum era and the need for quantum cybersecurity readiness.
(Percentage)



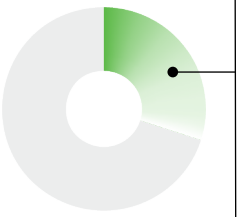
(n=1,196)

Readying for the next wave of emerging technologies

As organizations continue to address AI-related risks and opportunities, other disruptive technologies are also evolving and marching steadily toward widespread viability. Quantum cybersecurity readiness is becoming a bigger focus for many organizations, as quantum computing gets closer to reality—projected to become mainstream in the next several years and providing a powerful new tool for cyberattackers to use in breaking cryptography.

The data shows almost 83% of respondents are assessing quantum-related risks or taking some kind of action, whether developing strategies, implementing pilot solutions, or implementing solutions at scale. While the majority (52%) of respondents are still assessing their exposure and developing quantum-related risk strategies, others (30%) are taking decisive action to implement solutions as early adopters.

These figures point to clear momentum on the issue, and leaders can get ahead of the challenge by understanding risk potential, reviewing their data and system governance, prioritizing vulnerabilities relative to business operations, and developing a roadmap for cryptographic algorithm updates. Doing so can allow them to get a head-start on what is often a multiyear initiative and introduce new algorithms in an orderly way across broader enterprise transformations, as well as via updates to contracting mechanisms.



30%
of respondents reported taking decisive action to implement solutions as early adopters.

ORGANIZATIONS WITH GREATER CYBER MATURITY ARE MORE CONFIDENT AND REALIZING GREATER BENEFITS FROM THEIR CYBER ACTIONS AND INVESTMENTS.

CYBER MATURITY INDEX

Deloitte drew from our experience working with thousands of organizations worldwide to segment high-cyber-maturity organizations from their medium- and low-cyber-maturity counterparts.

To identify this distinct class of cyber leaders and more fully understand the extent to which cybersecurity supports business success and value, we used four sets of leading practices to rate, or index, organizations:

- **Robust cybersecurity planning**, indicated by the presence of strategic, operational, and tactical plans to defend against, and respond to, cyber threat (see Figure 3, page 11, for full list of planning strategies).
- **Key cybersecurity activities**, such as qualitative and quantitative risk assessment, industry benchmarking, and incident response scenario planning (see Figure 2, page 10, for full list of activities).
- **Effective board engagement**, exemplified by organizations whose boards address cyber-related issues on a regular basis.
- **Deployment of AI capabilities within the cybersecurity program**, focusing on organizations that are undertaking at least five of eight cyber-AI-related actions to a large extent (see Figure 14, page 23, for full list of actions).

This last criterion—for AI capabilities—is new in this edition of the survey, to reflect the evolution of technology and business, and what it means to be cyber-mature. When we use just the first three criteria (the same index we used in the previous edition), we see a three-percentage-point increase in cyber-mature organizations—from 21% of organizations to 24%—which is promising growth.

By including the AI factor in this edition's cyber maturity index, however, we can define a more elite group of organizations that are at the forefront of shaping the future of cyber.

In this edition of the survey, high-cyber-maturity organizations represent 14% of respondents surveyed. How they are approaching cybersecurity compared to the medium- and low-cyber-maturity groups provides important lessons that enterprise leaders can use to elevate their organization's cyber and business value.

Expectations run high for the cybersecurity function

Respondents in high-cyber-maturity organizations are highly attuned to the potential benefits that can come from their cybersecurity measures. On average, respondents in high-cyber-maturity organizations are 2.4 times more likely than respondents in low-cyber-maturity organizations (and 1.6 times more likely than respondents in medium-cyber-maturity organizations) to expect positive outcomes from their cybersecurity measures (Figure 16).

Some of those benefits include ensuring organizational resiliency (76%), improving threat detection and response (74%), and protecting intellectual property stature (74%)—three areas in which the expectations of respondents in high-cyber-maturity organizations stand far apart compared to low-cyber-maturity groups.

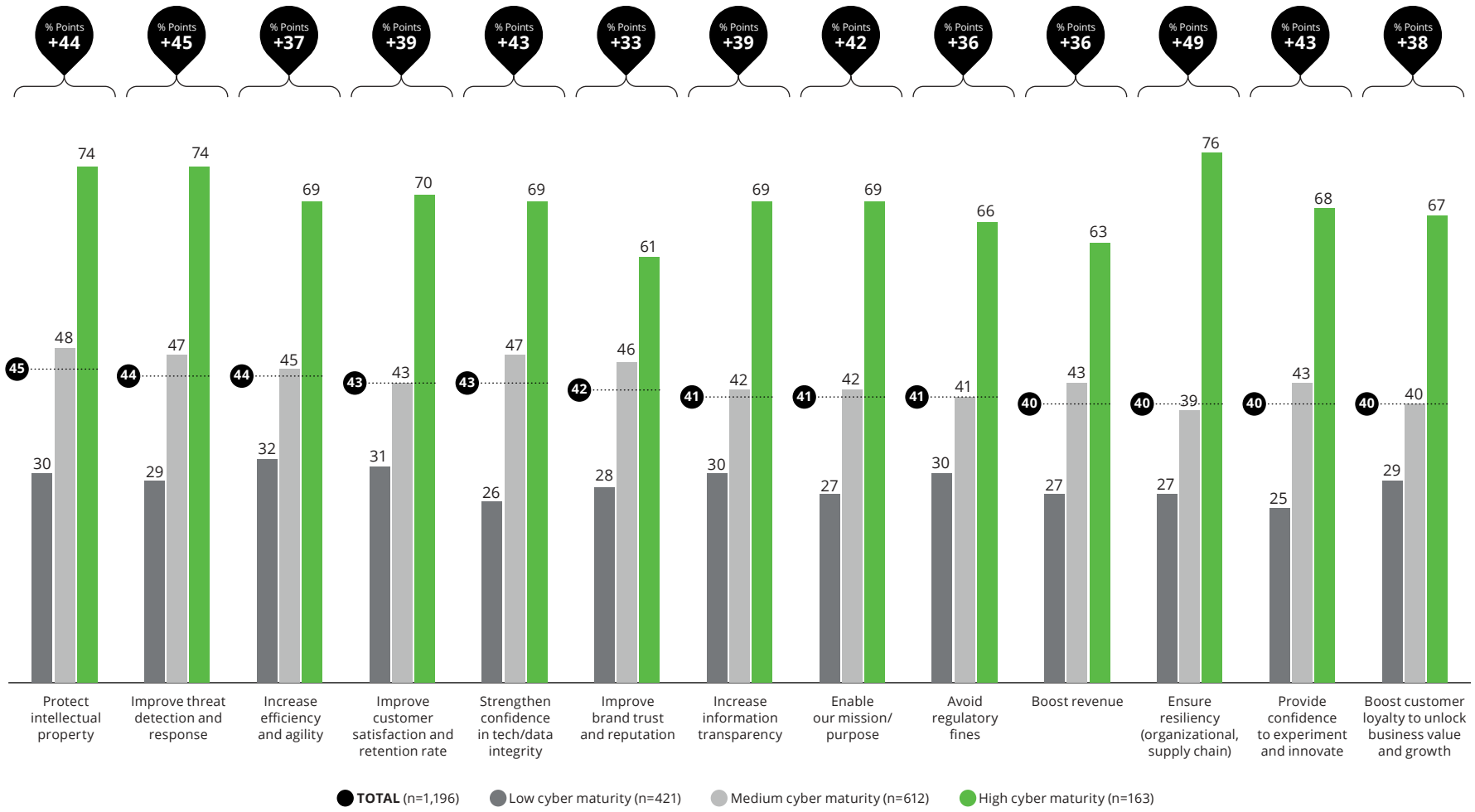
This picture reflects the challenge, as well as the promise, of cyber. The most cyber-mature organizations have considerably higher expectations across all measures. While they recognize the important role that cybersecurity should play, that realization puts more pressure on them to get things right.

CYBERSECURITY DRIVING OUTCOMES (FIGURE 16)

The benefits that organizations expect to see from their cybersecurity efforts.

(Percentage shown across all three cyber-maturity groups)

Differentials between high-maturity and low-maturity segments



Threat detection and response approaches continue to evolve

No organization is immune to the negative consequences of cyber breaches and incidents—even high-cyber-maturity organizations. On average, our analysis suggests that high-cyber-maturity organizations have a stronger ability to detect cyber threats and stronger diligence in complying with corresponding reporting requirements. For example, 25% of respondents in high-cyber-maturity organizations reported 11 or more cybersecurity incidents in the past year, eight percentage points higher than overall respondents. While this may seem like a negative, these organizations may have stronger threat detection capabilities that allow them to more effectively identify and respond to threats.

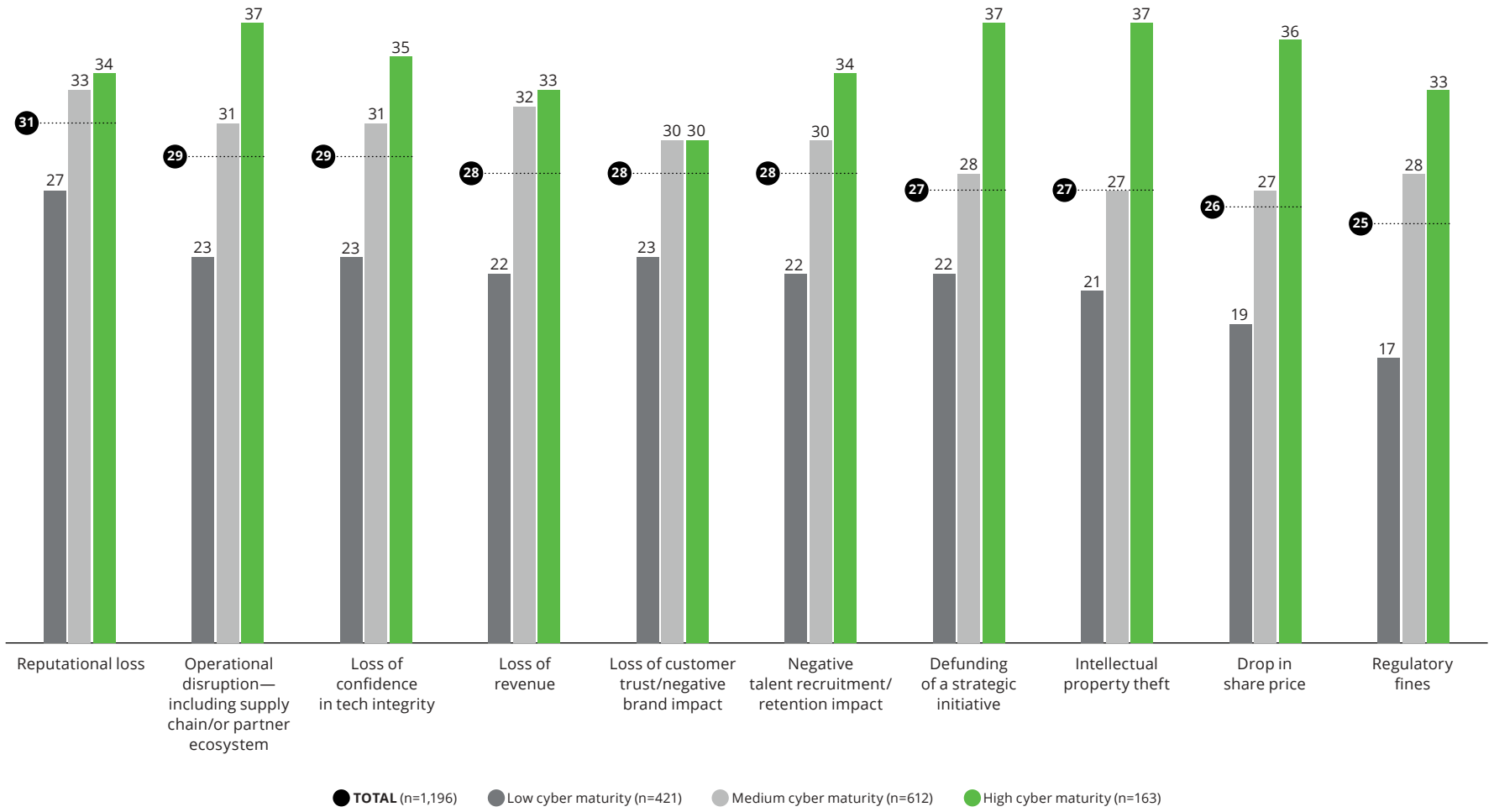
In addition to having greater awareness of breaches and incidents, these organizations also understand the true cost that goes along with them—and, on average, the high-cyber-maturity group is 13 percentage points more likely than their lower-cyber-maturity counterparts to acknowledge the extent of financial, operational, and brand impacts.

This greater understanding reflects a "virtuous cycle," providing a potential catalyst for the continued growth in cybersecurity integration across the business and its technology landscape. It also helps elevate the role of the CISO to preserve and protect value in the future, enable operational efficiency and resilience, and support innovation and revenue growth objectives.

EXPECTED NEGATIVE CONSEQUENCES, BY MATURITY GROUP (FIGURE 17)

Respondents with high cyber maturity are seeing more cybersecurity incidents—likely, in part, because of their greater threat detection capabilities.

(Percentage)



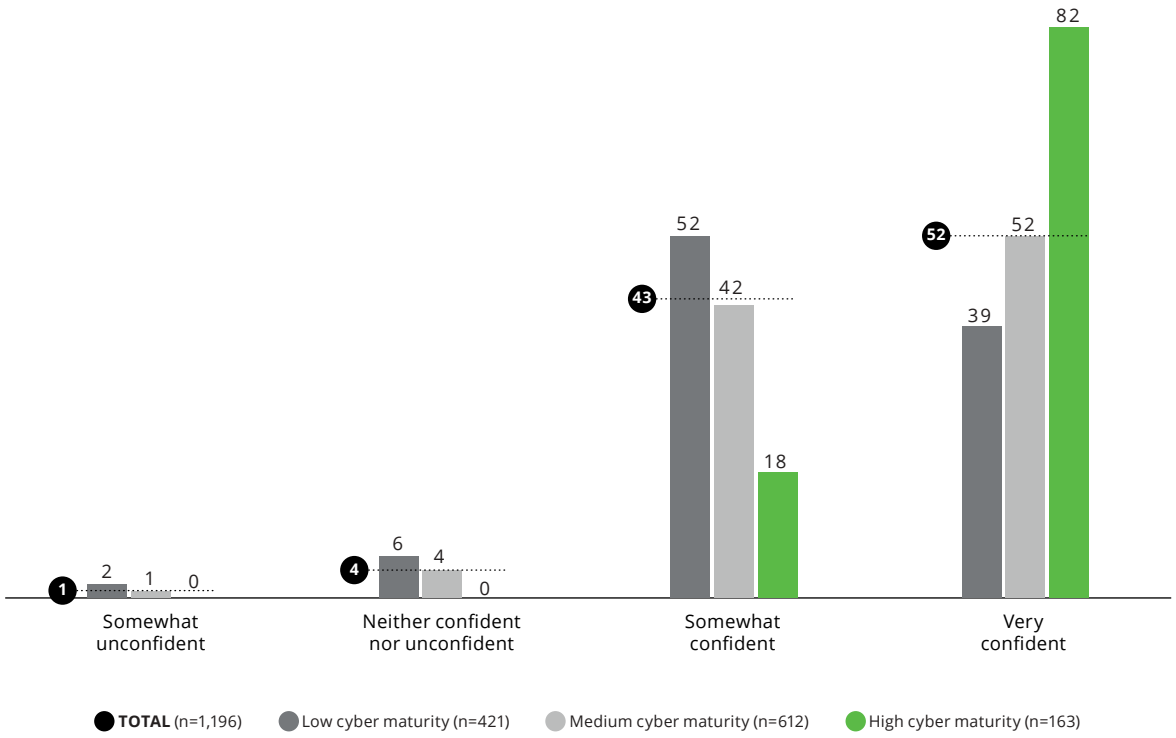
Creating confidence in the C-suite's cyber readiness

Confidence in their C-suite runs high among respondents in high-cyber-maturity organizations. They are twice as likely as respondents in low-cyber-maturity organizations to be very confident in the ability of the C-suite and board to effectively navigate cybersecurity needs (Figure 18).

CONFIDENCE AT THE HIGHEST LEVELS (FIGURE 18)

How confident respondents are when it comes to the C-suite's and board's ability to navigate cybersecurity.

(Percentages shown across all three cyber-maturity groups)



High-cyber-maturity organizations appear to be more adept at leveraging cybersecurity to secure investments for technology capabilities and in keeping the CISO involved in strategic conversations on digital transformation.

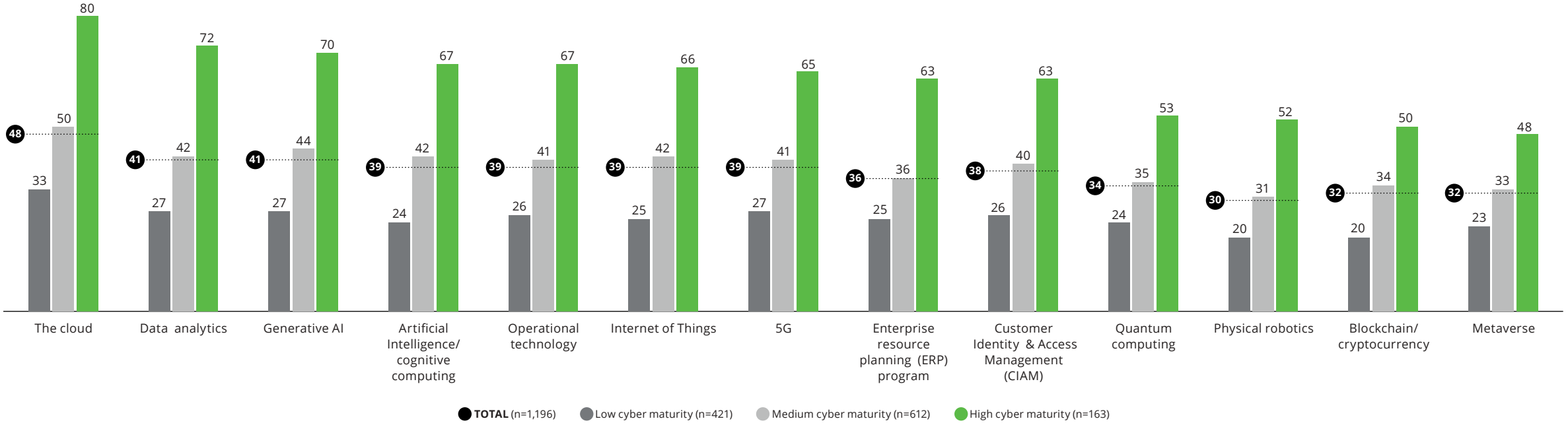
On average, respondents in high-cyber-maturity organizations are 2.5 times more likely than respondents in the low-cyber-maturity group to say that cybersecurity plays a large role in securing investments in their technology capabilities. The top areas in which they are securing those investments include cloud, data analytics, GenAI, operational technology (e.g., industrial control systems) and AI/cognitive computing (Figure 19).

GREATER MATURITY MEANS A GREATER ROLE FOR CYBERSECURITY IN TECH-DRIVEN CAPABILITIES

(FIGURE 19)

Compared to the other groups, the high-cyber-maturity group is seeing cybersecurity play a large role in securing investments in technology capabilities.

(Percentages shown across all three cyber-maturity groups)

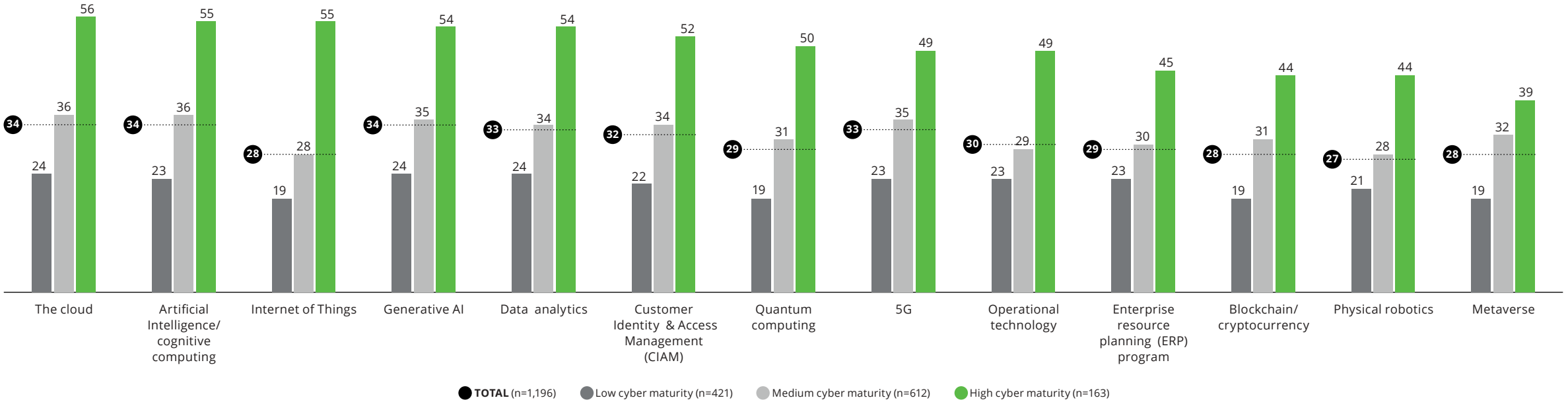


When it comes to strategy conversations around technology capabilities, compared to the low-cyber-maturity group, the high-cyber-maturity group is 2.3 times more likely to say that involvement by their CISO or cybersecurity leader has significantly increased. In high-cyber-maturity organizations, the areas in which CISO involvement is the greatest include cloud, AI/cognitive computing, the Internet of Things (IoT), GenAI, and data analytics (Figure 20).

"The role of the CISO is evolving. They need to bring in the right strategies to proactively guide the company in making data-driven decisions. As this entails increased engagement with executive leadership, CISOs should not only be technologically proficient but also operate with an executive-level mindset and business acumen to demonstrate how a cyber strategy will influence the business."

—Gary Harbison, Chief Information Security Officer, Johnson & Johnson

WITH CYBER MATURITY COMES MORE CISO INVOLVEMENT IN STRATEGIC CONVERSATIONS (FIGURE 20)
High-cyber-maturity groups are seeing their CISOs brought into conversations more frequently across all areas.
(Percentage)



INSIGHTS FOR NAVIGATING THE FUTURE OF CYBER

Elevating cybersecurity across the enterprise

Thriving in the future of cyber will require organizations to understand the emerging trends, navigate them, and, most importantly, take action on them to deliver measurable impact for the business. By focusing on the following factors and potential steps, organizations can make strides toward greater cyber maturity and set themselves apart from their peers.

Elevate the cyber essentials, foster connections and collaboration, build greater resilience

As the focus intensifies on cybersecurity as an element for strategic business value, leaders should recognize that cybersecurity is not just an IT issue; it is a business-critical issue that calls for integration across all functions and levels of the organization. That will require an ability to continuously build and prioritize the connection to cyber across business and technology operations.

As organizations establish stronger leadership and strengthen cyber connections, they can enhance collaboration, information-sharing, and decision-making wherever business needs intersect with cybersecurity. Doing so can enable leaders to make strategic decisions that are highly informed by the realities of their business—all aligned with business objectives and the effective mitigation of cyber risks. Ultimately, by making cybersecurity a priority and by building stronger connections to cybersecurity across the enterprise, organizations can better safeguard their critical assets and their reputations while enhancing their overall resilience in an increasingly digital world.

Once seen as a lead security guard for enterprise IT, **the role of the CISO is evolving** into one that helps safeguard the entire enterprise—from core business operations to brand reputation—while supporting innovation and the future of the business.

Increase engagement and savvy among leadership, from the CISO to the rest of the C-suite and the board

The future of cyber points to a clear imperative: ensuring that the CISO is actively involved in strategic conversations about technology capabilities and the business. Once seen as a lead security guard for enterprise IT, the role of the CISO is evolving into one that helps safeguard the entire enterprise—from core business operations to brand reputation—while supporting innovation and the future of the business.

And the CISO should be joined by other cyber-savvy peers across the top levels of leadership. Addressing cybersecurity risks effectively—and in the context of business objectives—demands that the entire C-suite and board are regularly engaged in cybersecurity conversations. Because cybersecurity is a top risk for organizations, top leadership must remain heavily involved in its management and oversight. With engaged CISOs providing valuable insights and guidance to the board and the organization on cyber matters, cybersecurity can receive the attention and resources it merits—as a strategic business issue that requires continuous investment.

Make intentional efforts to integrate budgets, anchored in strategy and governance

The trend of cybersecurity budgets becoming integrated with budgets for other digital transformation investments is an important one. It shows that cybersecurity is receiving the recognition it deserves and suggests more departments may include cybersecurity in their funding plans going forward.

This integrated approach can lead to a more comprehensive strategy and better outcomes for overall security. By establishing a clear governance framework that supports a broader agenda and defines aspirations for cybersecurity, organizations can take crucial steps toward their business objectives. Such an approach means that everyone in the organization understands the importance of cybersecurity, commits the appropriate level of investment, and works toward a common goal.

By having effective governance in place, organizations can ensure that cybersecurity initiatives are aligned with other important business priorities, but there is a possible drawback to such integrated transformational investments. If cybersecurity is not specifically stated as a line item in budgets, it may get diminished, because it is treated as a *portion* of the cost rather than a *value-enhancing investment*.

> **“When it comes to strategy, one of the things that we are maturing … is starting with the outcome. So always thinking about where do we want to be X years from now. And I believe in security creating a strategy more than two years out, you will change a whole lot because the threats will change, the technology will change, and so on … So we’re building based on outcome in mind, which is really critical.”**
>
> **—Chief Information Security Officer, Life Sciences and Health Care Company**

MAKING THE FUTURE MATTER

The future of cyber is being written right now—with every second. New risks, technologies, and business choices are taking shape. How your organization prepares for them and acts on them will define your cyber maturity as well as the future of your business.

As the recognition of cybersecurity's role grows within the enterprise, as top leadership becomes more engaged in strategic conversations about cybersecurity, and as cybersecurity becomes more integral to transformation ambitions, a new day is dawning. How will you make the most of what comes next? How will you make it matter for your business?

Get started

Contact us to explore insights from the 4th Edition of Deloitte's *Global Future of Cyber Survey*, and discover what else the most cyber-mature organizations are doing to drive business value and set themselves apart.

Connect with us

Sathish Gopalaiah
President
Technology & Transformation
Deloitte South Asia
sathishtg@deloitte.com

Gaurav Shukla
Partner and Leader – Cyber
Deloitte South Asia
shuklagaurav@deloitte.com

Deepa Seshadri
Partner
Deloitte India
deseshadri@deloitte.com

Deloitte.