

The image features a dark, moody office environment. Two women are the central focus. One woman is seated in the foreground, wearing a brown jacket, looking towards the right. Another woman stands behind her, leaning over a desk, wearing a black and white polka-dot top. Two large, glowing green circles are superimposed over the scene, one centered on the seated woman and another slightly behind her. The background is filled with soft, out-of-focus lights, suggesting a modern, tech-oriented workspace.

Deloitte.

Digital Trust Maturity Survey

Earning and building greater
digital trust through cyber

How leading organizations are taking proactive measures to increase integrity and boost confidence across their digital and business landscapes.

Trust has always been essential in business, but in today's environment, it is the crucial currency that companies must use to engage with customers in exchange for their attention, business, and loyalty. Many organizations, however, struggle to achieve the highest levels of trust from their wide range of stakeholders, which includes customers, employees, suppliers, and investors among others.

An interconnected web of factors has created new challenges in this age of digital trust, a time in which information (and misinformation) is omnipresent, and cybersecurity and data privacy are under constant threat. It is in this time that cyber risk management will play a massive role in powering trust.

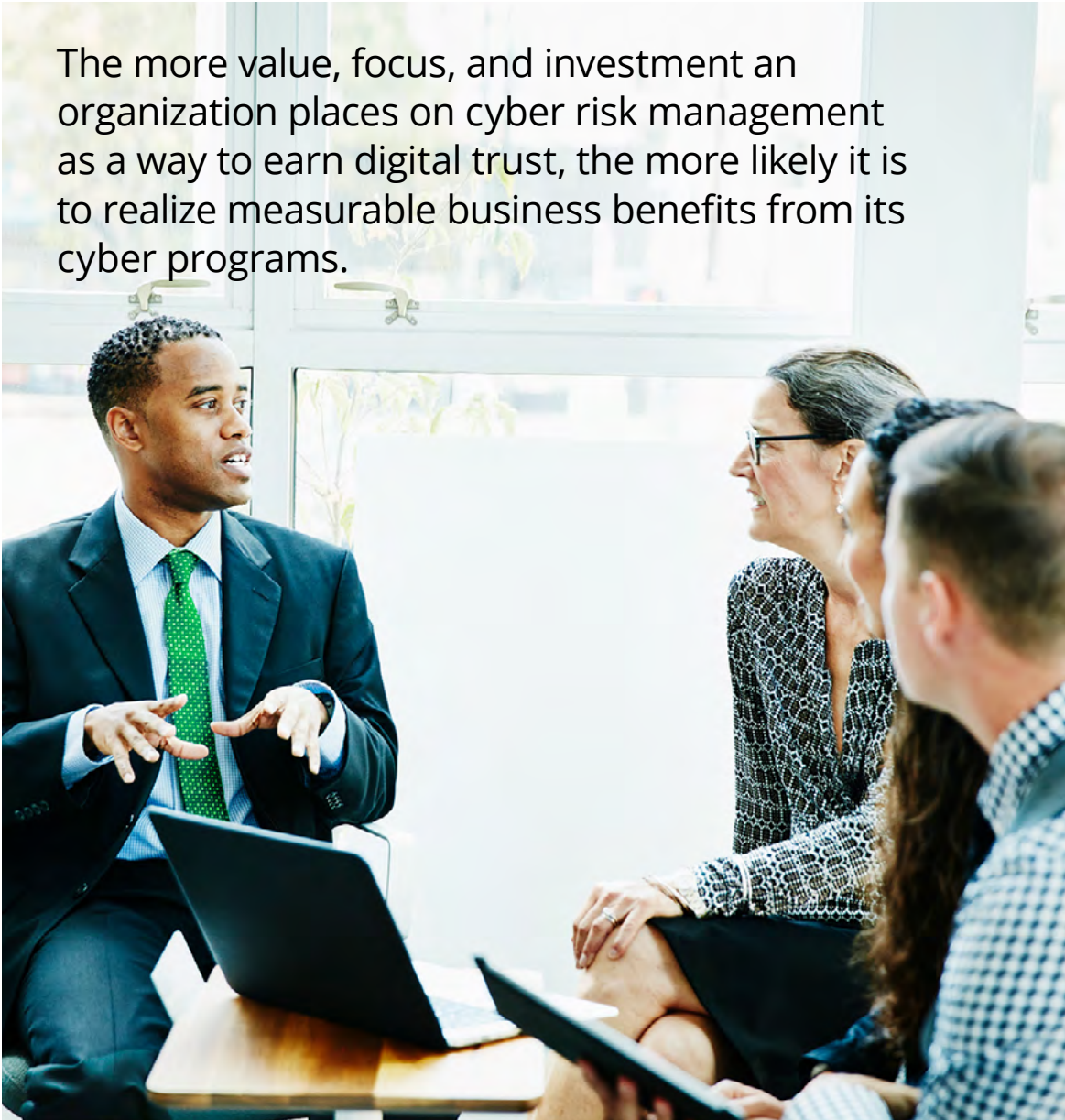
In fact, this data-driven analysis shows that organizations that place a high importance on digital trust increase confidence in and integrity of their business. Here's how they are making that connection.

Executive summary

Using data from the *Deloitte 2023 Global Future of Cyber Survey* which included 1,110 respondents worldwide, Deloitte has developed a Digital Trust Maturity scale for cyber that places organizations into three groups (high, medium, and low) based on the importance they place on digital trust.

Analysis of the data shows that organizations that fall into the high digital trust maturity group realize greater benefits from cybersecurity initiatives, compared to organizations in the medium and low digital trust maturity groups. Those benefits extend across operational, financial, and brand impact categories—including positive impact on reputation.

While the *2023 Global Future of Cyber Survey* establishes a clear connection between cyber and business value, this latest analysis shows a new connection: the more value, focus, and investment an organization places on cyber risk management as a way to earn digital trust, the more likely it is to realize measurable business benefits from its cyber programs. The research also shows a correlation between digital trust maturity and overall cyber maturity. A majority of the low digital trust maturity companies, for example, also had low overall cyber maturity.



The more value, focus, and investment an organization places on cyber risk management as a way to earn digital trust, the more likely it is to realize measurable business benefits from its cyber programs.

Key insights

Organizations that place a high priority on digital trust see tremendous benefits related to improved tech integrity, customer trust, and brand reputation that can greatly outweigh their challenges, though talent is a pervasive issue.

The greatest benefit from cyber for high digital trust maturity companies is

71%

improved confidence in tech integrity, 50 percentage points more than their low digital trust maturity counterparts.

Other top cyber-related benefits cited by this high maturity group include:

68%

improved customer trust or brand impact

65%

improved brand reputation



Those organizations in the high digital trust maturity group were more likely to engage multiple stakeholder groups in their cyber activities. Compared to the other two groups, they are more likely to focus on activities such as keeping employees aware (77%), evaluating third-party risks (74%), and providing regular board updates (54%).



Cyber challenges varied across the three segments, with high digital trust maturity organizations citing talent and funding as top challenges, and with low digital trust maturity organizations more often citing challenges related to management and governance.

While cyber investments are expected to increase annually across all groups, organizations with high digital trust maturity differentiate themselves with cyber planning strategies and activities.

Across all three segments, the majority of respondents intend to increase annual cyber investments—with

65%

of the high digital trust maturity group looking to boost cyber spend.

High digital trust maturity organizations are focusing heavily on cyber planning strategies and activities.



They are roughly 1.5 times more likely than medium and nearly 3 times as likely as low digital trust maturity organizations to embrace cyber planning strategies such as employing risk quantification tools to ensure return on cyber investments and benchmarking cyber activities against industry leaders.



An overwhelming majority of companies in the high digital trust maturity group engaged in eight key activities supporting cyber—including annual employee cyber awareness training and purchasing cybersecurity insurance. (See Figure 5.)

There is a noteworthy correlation between digital trust maturity and overall cyber maturity, as established in Deloitte's 2023 Global Future of Cyber Survey.

43%

of the high digital trust maturity respondents also fall into the high cyber maturity category.



Organizations that want to close the gap on digital trust and cyber—and realize greater business benefits—have abundant options, including expanding digital trust education at the C-suite level, focusing cyber activities more on relationship-building, and embedding digital trust in programs beyond cyber, such as marketing activities.

Digital (and cyber) at the center

Proactively building trust equity—i.e., the amount of trust an organization has accumulated with its stakeholders—has become increasingly important as a business imperative.

Digital trust: What it means

Deloitte defines digital trust as the earned confidence and reliance on a digital platform, asset, product, or service by consumers—achieved through an organization's:

- Transparent and integrity-driven data practices
- Ability to protect and proactively prevent against harm to consumers
- Measurable privacy, safety, and secure protocols and measures
- Fair and compliant business practices

New digital products and features, new systems and applications, new data sets, new experiences to create emotional connections, and new cloud models add to the urgency and complexity of the challenge. They all present points at which trust can be bolstered or damaged, and require that digital trust be woven into the broader fabric of your digital strategy—and solidly supported with cyber risk strategies and capabilities.

Today, cyber risk management is essential to building digital trust, helping to elevate confidence in your data, products and services, processes, relationships, and ultimately your business and its brand. Case in point: When B2B purchasers strongly disagree that a brand “employs measures to prevent data loss and privacy breaches,” they are 26% less likely to go out of their way to purchase from the brand.¹

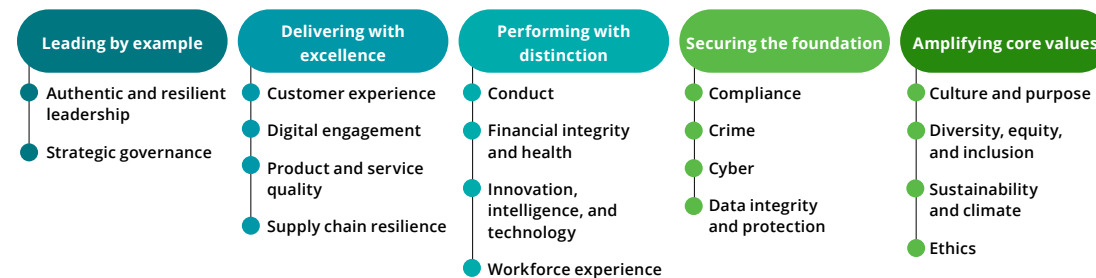
Simply put, with a stronger cyber posture comes the potential for greater digital trust and, in turn, greater overall trust for your business.

As organizations embed integrity, safety, security, transparency, and privacy into their digital strategies, including platforms, products, and services, they can win the confidence of end customers and business users.

Cyber strong

A trusted organization = competence + intent

Deloitte's Enterprise Trust Framework identifies five areas in which organizations can earn and build trust. Cyber is an essential pillar for securing the foundation of the enterprise.



Keys to earning trust

Organizations earn trust by demonstrating high competence and positive intent. This vital relationship between an enterprise and its stakeholders can be established by demonstrating capability, reliability, humanity, and transparency across 18 enterprise domains. Of these areas, cybersecurity, data privacy and integrity, and digital engagement are essential to the digital dimensions of trust.

Making an impact with trust

Chief Information Security Officers (CISOs) already understand the critical role that cyber plays in supporting digital trust, and the positive impact it has on overall trust for the enterprise.

But recognizing the impact of trust and what drives it may not always be obvious across the business and ecosystem. Build greater trust in your products, services, processes, and capabilities, and you can drive performance across a wide range of business dimensions. Trustworthy companies, for example, can outperform nontrustworthy companies by 2.5 times,² and 88% of customers who highly trust a brand will buy again from that brand.³



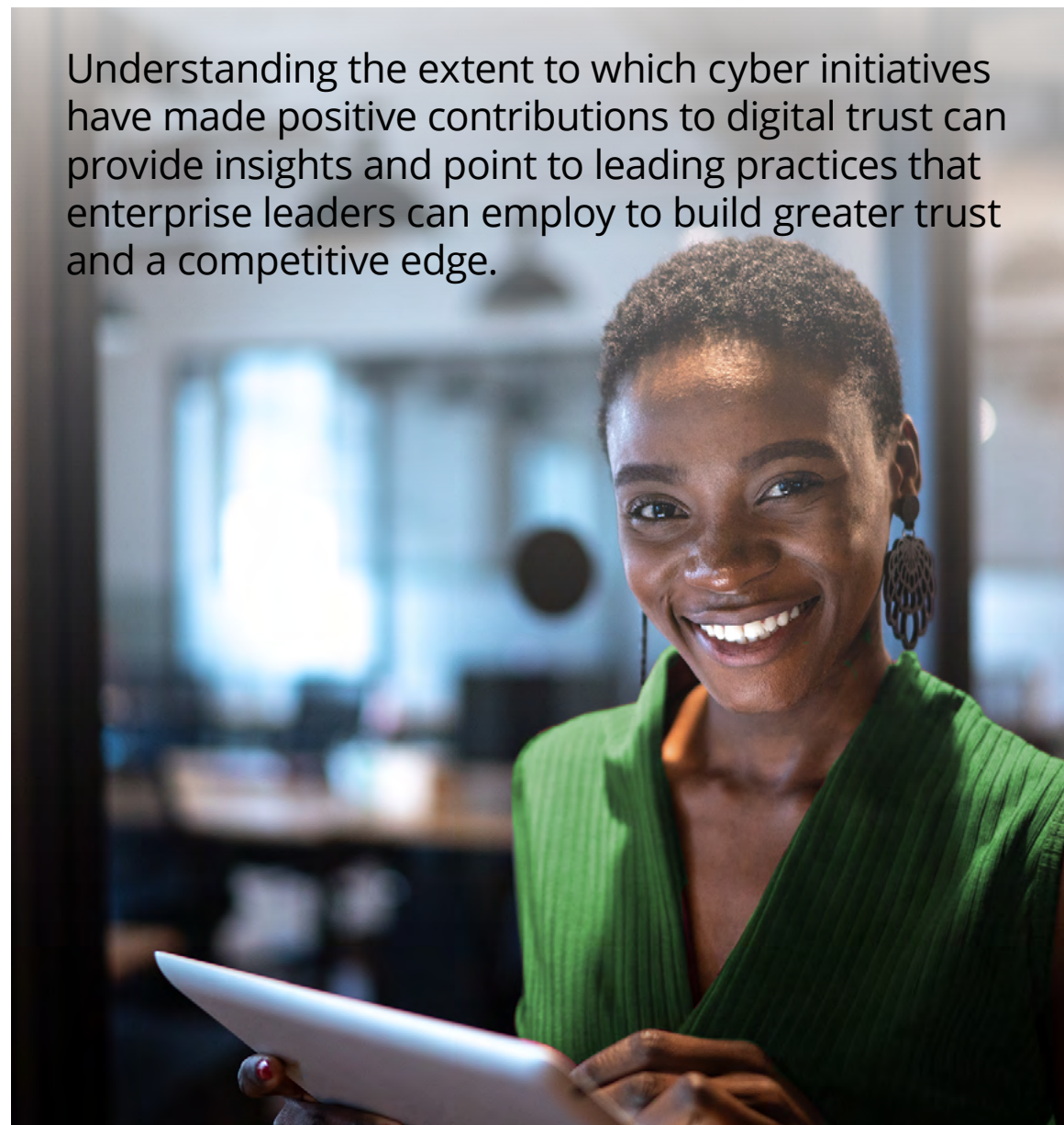
Future in focus for digital trust leaders

Deloitte's *2023 Global Future of Cyber Survey* took a close look at how organizations across industries and regions were embedding cyber across the enterprise and leveraging it to deliver business outcomes.⁴ As part of our research, we collected data on how 1,110 respondents were thinking about, and acting on, digital trust.

Deloitte has continued to examine this data to gain a better understanding of the importance of digital trust to businesses, as well as the role that cyber plays. Understanding the extent to which cyber initiatives have made positive contributions to digital trust can provide insights and point to leading practices that enterprise leaders can employ to build greater trust and a competitive edge.

In this report, we take a deep dive into some of the digital trust findings that emerged from our earlier survey. We zeroed in on organizations that place a high importance on digital trust—what sets them apart from other organizations and the lessons other businesses can learn from them as they seek to make cyber a bigger enabler of business value.

Understanding the extent to which cyber initiatives have made positive contributions to digital trust can provide insights and point to leading practices that enterprise leaders can employ to build greater trust and a competitive edge.



Defining the journey of digital trust

Our approach

As we examined the data related to digital trust, we segmented respondents into three distinct groups: organizations that place a high importance on digital trust, those who place medium importance on digital trust, and those for which digital trust was of low importance.

These three segments help us understand how the trust journey can vary across organizations and allow us to create a Digital Trust Maturity scale based on how respondents are distributed across the following groups: 22% high importance for digital trust, 50% medium importance, and 28% low importance.

Methodology

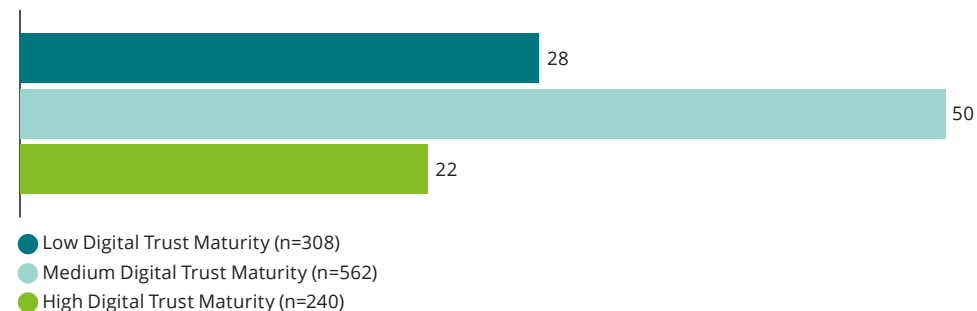
Three factors determined where each organization fell based on scoring their responses to questions related to:

- The importance given to building digital trust for the success of your organization
- The extent to which your cybersecurity success impacts the success of building digital trust
- The extent to which cyber initiatives made a positive contribution and improved digital trust

Organizations that said these factors were “very important” or mattered “to a large extent”—were classified as having a “high” digital trust maturity, while those that did not choose any were considered to have “low” digital trust maturity. All others fell into the “medium” category.

Figure 1: Deloitte’s Digital Trust Maturity scale

Based on 1,110 global respondents, falling into the following three groups.
(Percentage)



Source: Analysis of Deloitte’s 2023 *Global Future of Cyber Survey*

What can we learn from these groups?

Let’s start with some key questions we asked in the 2023 *Global Future of Cyber Survey*. Then let’s examine those questions and responses through the lens of each of the three segments—to determine how high digital trust maturity organizations stand apart from their counterparts when it comes to cyber, trust, and business priorities.

Trusting in benefits

Impact for companies

Where cyber maturity and digital trust maturity intersect

In the 2023 *Global Future of Cyber Survey*, we placed all respondents into one of three categories for their overall cyber maturity (high, medium, and low).

Our latest analysis on digital trust maturity reveals some noteworthy correlations with a large number of high digital trust maturity companies (43%) overlapping with high cyber maturity companies.

Similarly, most low digital trust maturity companies (53%) also have low cyber maturity overall.

This reinforces the notion that cyber and digital are mutually reinforcing actions and outcomes.

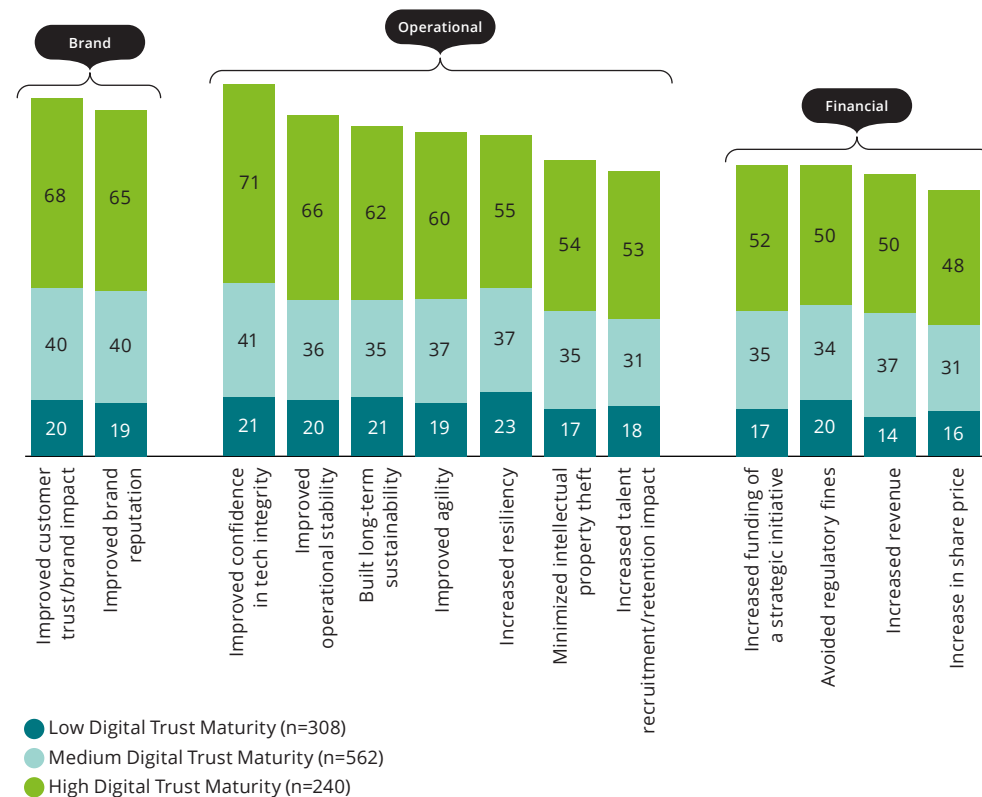
Cyber and business value have become inextricably linked. So how does digital trust integrate with that picture? One important question we asked was to what extent cybersecurity initiatives made a positive contribution in over a dozen areas.

Our analysis found that high digital trust maturity organizations realize greater benefits from cybersecurity initiatives across operational, financial, and brand impact categories. These leading organizations see a return on trust that goes beyond traditional financial measures, to include positive impact on reputation and how the organization runs. The greatest benefit they cite is improved confidence in tech integrity (71%), 50 percentage points more than their low digital trust maturity counterparts. Additionally, they report significant benefits across all types of impact, leading the other groups in benefits reported across every measure asked about in our survey.

68% of high digital trust maturity organizations report improved customer trust or brand impact as a benefit of their cyber initiatives—compared to 40% of the medium digital trust maturity group and 20% of the low digital trust maturity group.

65% of high digital trust maturity organizations report improved brand reputation as a benefit of their cyber initiatives—compared to 40% of the medium digital trust maturity group and 19% of the low digital trust maturity group.

Fig. 2: Positive contributions by cybersecurity initiatives
For organizations with high digital trust maturity, significantly more of them are reporting benefits from cyber across their business.
(Percentage)



Source: Analysis of Deloitte's 2023 *Global Future of Cyber Survey*

Solving for digital trust

Cyber challenges, strategies, and activities in the mix

Across the Digital Trust Maturity scale, each segment faces many of the same cyber challenges, but in varying degrees of priority. The groups also vary noticeably when it comes to the cyber activities and strategies they are undertaking to address their challenges.

Deloitte's 2023 *Global Future of Cyber Survey* asked respondents to rate the level of challenge for several issues when managing cyber needs across their organizations, and from there to select their top two issues.

Organizations with high digital trust maturity cited lack of skilled cybersecurity professionals and lack of adequate funding as their top challenges in managing cybersecurity. Meanwhile organizations in the low digital trust maturity group cited lack of management alignment on priorities, inadequate governance across the organization, and lack of executive support/ sponsorship as their top challenges.

For these two groups on the Digital Trust Maturity scale, the line between the top challenges is fairly well-defined—with external challenges such as finding skilled cybersecurity professionals and obtaining adequate funding more pronounced for the high digital trust maturity companies, and with internal challenges such as lack of leadership consensus on the importance of cyber more prominent at the low digital trust maturity companies. These differences suggest that leadership buy-in on cyber can be a major contributing factor to success for cyber ambitions and ultimately for digital trust. Or from another perspective, a lack of leadership alignment on cyber among the low digital trust maturity group may be one of the reasons their organizations rate digital trust lower on the list of priorities.

Fig. 3: Top challenges in managing cyber

Organizations with high digital trust maturity cite talent and funding as top challenges, while low digital trust maturity organizations more often cite challenges related to management and governance.

(Percentage)



Source: Analysis of Deloitte's 2023 *Global Future of Cyber Survey*

The three Digital Trust Maturity groups also undertake different planning strategies and activities to address these challenges.

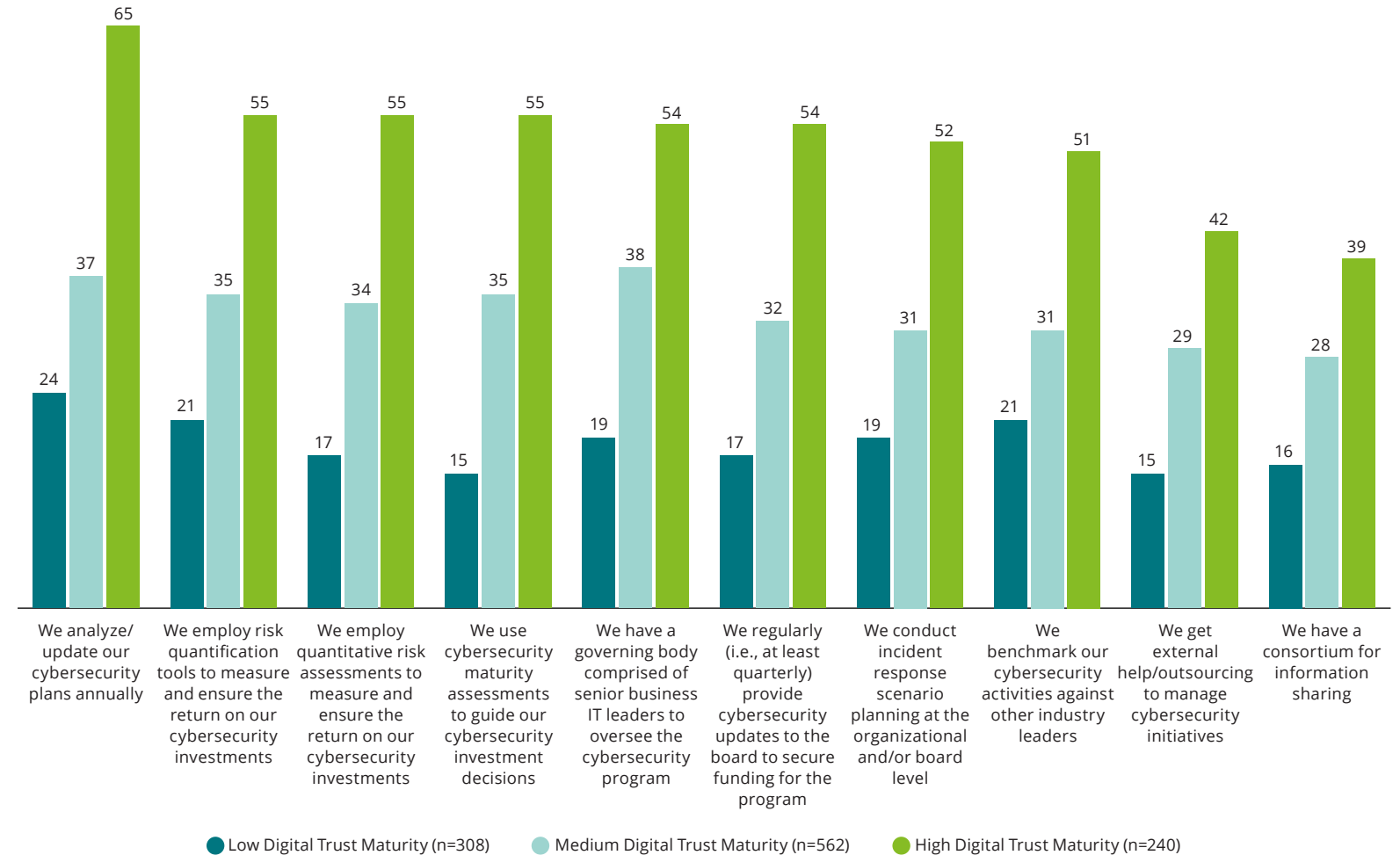
On average, high digital trust maturity organizations are roughly one and a half times more likely than medium, and nearly three times as likely as low digital trust maturity organizations, to embrace the following cyber planning strategies:

- Employing risk quantification tools to ensure the return on cybersecurity investments
- Benchmarking their cybersecurity activities against industry leaders
- Conducting incident response scenario planning at the organizational and/or board level

Fig. 4: Key cyber planning strategies and priorities

The high digital trust maturity group engaged in all activities at a higher rate.

(Percentage)



Source: Analysis of Deloitte's 2023 Global Future of Cyber Survey

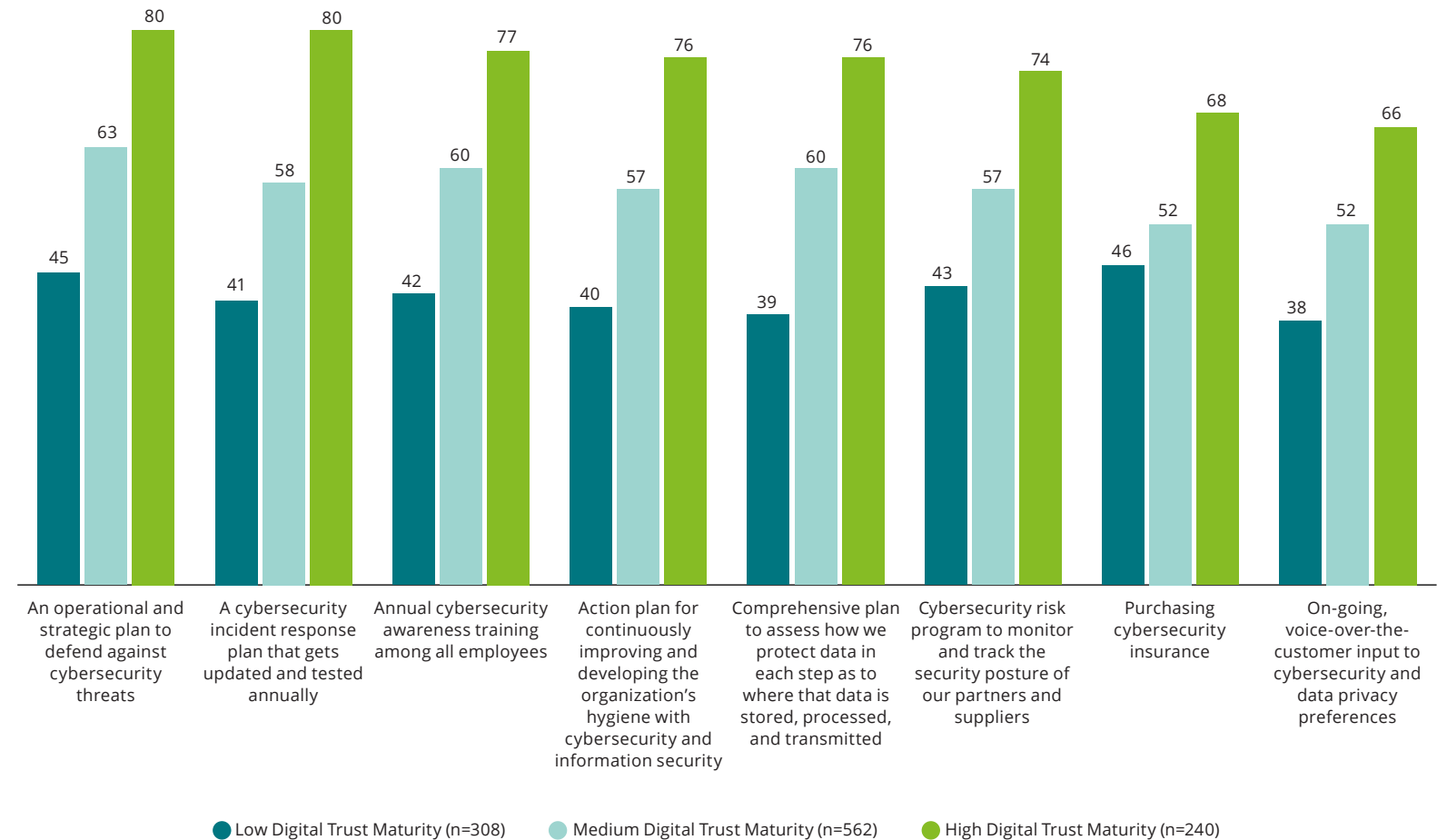
When it came to specific cyber activities, high digital trust maturity organizations were nearly twice as likely to have implemented the following activities compared to organizations with low levels of digital trust maturity, but only 1.3 times as likely as medium digital trust maturity organizations.

- An operational and strategic plan to defend against cybersecurity threats
- An action plan for continuously improving and developing the organization's cyber/information security hygiene
- A cybersecurity risk program to monitor and track the security posture of partners and suppliers

Fig. 5: Activities undertaken to boost cyber and information security

An overwhelming majority of companies in the high digital trust maturity group engaged in all of the following key activities supporting cyber.

(Percentage)



Source: Analysis of Deloitte's 2023 Global Future of Cyber Survey

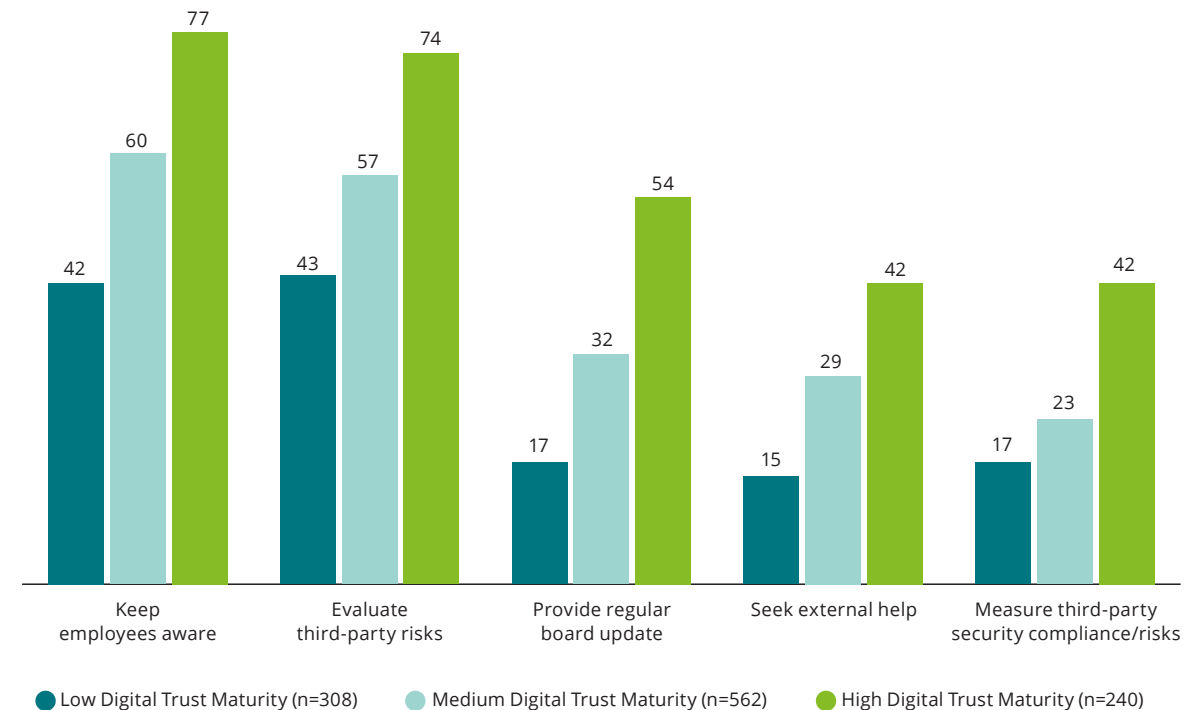
Trusting in others

Looking across our data for cyber planning strategies and activities, as well as data on risk quantification measures from the *2023 Global Future of Cyber Survey*, one additional pattern emerged—one that is highly reflective of the nature of trust: communicating with and including others. Those organizations in the high digital trust maturity group were more likely to engage multiple stakeholders in their cyber activities, focusing on certain activities at a greater level compared to the other two groups.

Consider the following activities, indicating that high digital trust maturity organizations tend to expand responsibility for, and involvement in, cyber into other areas of the business:

Fig. 6: Involving others in cyber

Percentage of each maturity group engaging in these activities.



Source: Analysis of Deloitte's *2023 Global Future of Cyber Survey*

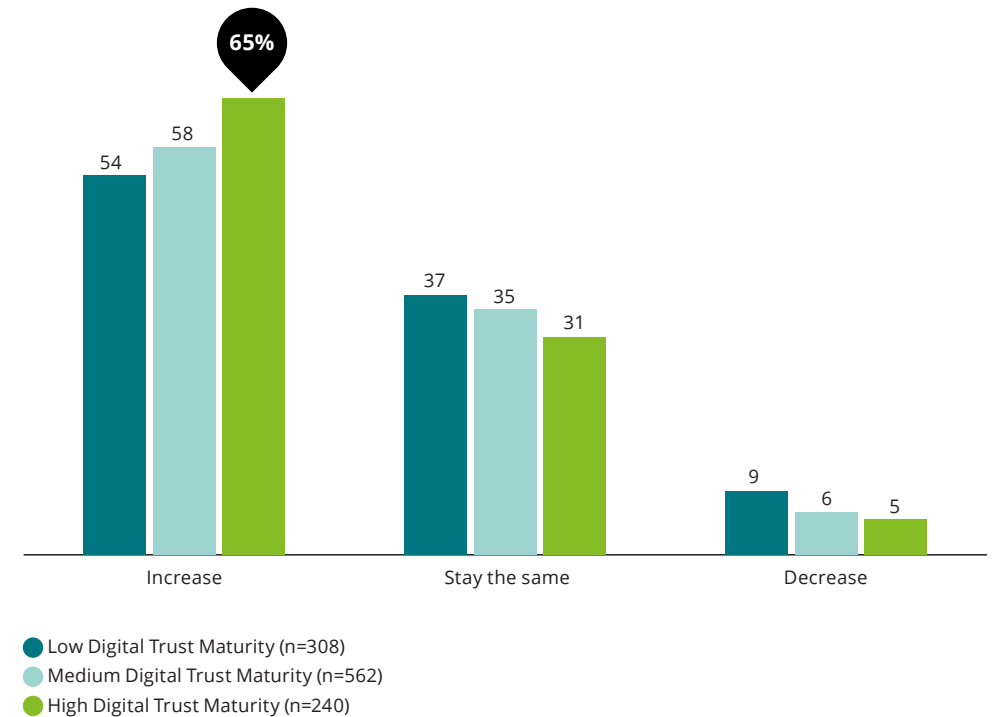
Eyeing investments

We also dug into our data to get a sense of how investments in cyber correlated with digital trust.

Cyber comes with a few caveats and the potential for many hypotheses. For one, Deloitte's *2023 Global Future of Cyber Survey* data was collected in late 2022. Since then, the economic environment has shifted. Second, our data may not reveal the extent to which companies are making investments that are proportional to the size of their businesses. Third, it is also difficult to assess the specific reason behind an increase or a decrease in spending—whether it is due to a major project kicking off or winding down, for example.

In light of those caveats, the research shows that, across all three segments, a majority intend to increase annual investments. Only a small number plan on reducing their investments, with 9% of the low digital trust maturity group intending to decrease spend, compared to 6% for the medium digital trust maturity segment and 5% for the high digital trust maturity segment.

Fig. 7: Investment in cyber
(Percentage)



Source: Analysis of Deloitte's *2023 Global Future of Cyber Survey*

Closing the gap

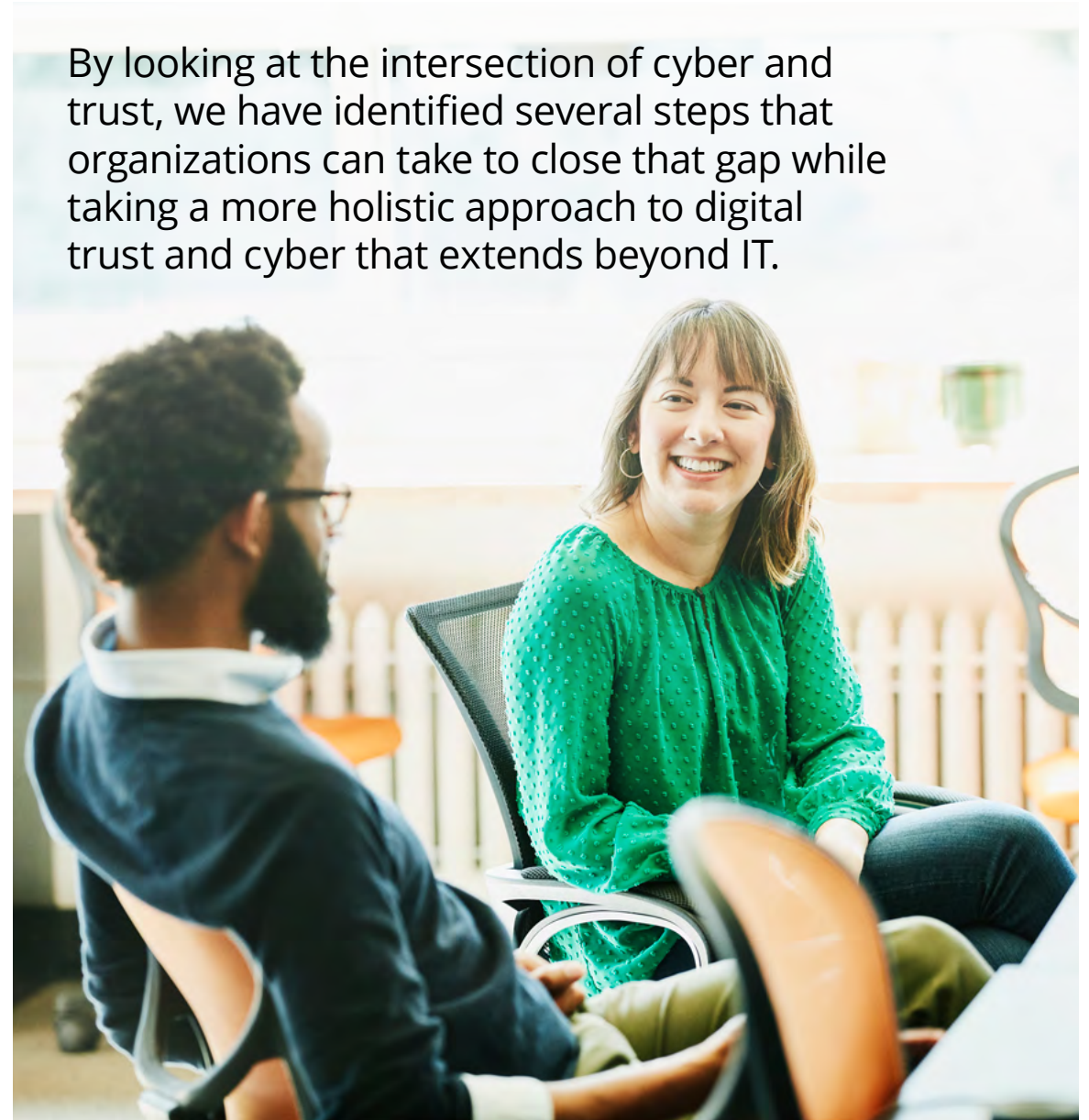
Deloitte's 2023 *Global Future of Cyber Survey* made clear the connection between cyber and business value. Our research now shows that the greater importance an organization places on digital trust, the more likely it is to invest in and focus on cybersecurity, and realize measurable business benefits from its cyber programs.

For organizations in the low or medium digital trust maturity groups, there is a gap to close to ensure that their organizations can build digital trust through cyber and provide their businesses with the edge they will need in the age of digital trust.

By looking at the intersection of cyber and trust, we have identified several steps that organizations can take to close that gap while taking a more holistic approach to digital trust and cyber that extends beyond IT.

Without leadership alignment and support behind cyber as a priority, digital trust ambitions can fade. Ensure digital trust is a leadership priority and add it to the board's agenda.

By looking at the intersection of cyber and trust, we have identified several steps that organizations can take to close that gap while taking a more holistic approach to digital trust and cyber that extends beyond IT.



Steps to help close the gap

1

Define what digital trust means across different contexts in the enterprise.

Recognize that the definition may differ depending on your organization's context, sector, and stakeholders. As you work to understand the different meanings of digital trust, ask:

- Who are the key stakeholders for which digital trust matters?
- What is the baseline of trust today?
- What are the drivers of that trust, and how can you improve them?

2

Get all levels of management on the same page.

Low and medium digital trust maturity groups lag on management alignment with priorities. Digital trust should be a top priority in today's environment. But without leadership alignment and support behind cyber as a priority, digital trust ambitions can fade. Ensure digital trust is a leadership priority and add it to the board's agenda.

3

Help the C-suite understand threats to digital trust and how it evolves on an ongoing basis.⁵

Make it clear to them that, if you are trying to adopt new technologies such as GenAI or introduce new connected products and services that collect data, digital trust will be essential for driving user adoption—even more so if you do not already have high levels of brand and trust equity.

- Develop a collective business mindset when managing digital trust—recognize that digital trust is a business issue, not just a technology issue, and manage digital trust as you would any other key aspect of enterprise performance and risk.
- Subscribe to a culture of continuous learning in relation to emerging technologies, both in terms of how they are used and the risks and opportunities they present. This is essential at the individual and organizational levels.
- Illustrate your commitment to building a digital trust-preserving culture—by transparently discussing trust-relevant actions and challenges and opportunities across broad stakeholder audiences—and, most importantly, take action that genuinely demonstrates commitment in tangible ways.

4

Measure and evaluate digital trust dynamically on an ongoing basis.

Leverage context-sensitive metrics and ensure that they reflect how technologies can affect different stakeholders. Assess digital trust across employee groups, customer segments, third parties, and other groups. Where possible, look to understand trends based on established baselines, and compare results to the relative sector.

5

Think in terms of relationship-building, not transactions.

Just like trust overall, digital trust must be earned. Ask yourself what you can provide stakeholders to strengthen relationships and earn their digital trust. Greater privacy? More reliable data? Reduced business risk? Faster capabilities? Then ask how cyber can play a role in supporting that relationship-building activity.

Eye on the future

The landscape of digital trust and cyber will continue to evolve as new risks, technologies, and business forces emerge. How will you navigate the future of cyber and the future of digital trust? Organizations that want to close the gap and thrive should focus on continuously building insights and identifying opportunities that can help them generate new business value.

Get started

Acknowledgements

Michael Bondar, Criss Bradbury, Scott Buzik, Lisa Carlton, Alison Charles, Deborah Elder, Tanneasha Gordon, Kate Graeff, Diana Kearns-Manolatos, Daphne Lucas, Mike Nash, Kelly Nelson, Iram Parveen, Scott Tillett, Marius von Spreti

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
+31 88 2882186

César Martín Lara

Spain Cyber Leader
cmartinlara@deloitte.es
+34 91438 1416

Adnan Amjad

US Cyber & Strategic Risk
Offering Portfolio Leader
aamjad@deloitte.com
+1 713 982 4825

Tanneasha Gordon

Principal, Risk and
Financial Advisory
tagordon@deloitte.com
+1 415 783 4504

Marius von Spreti

Germany Cyber
Security Lead
mvonspreti@deloitte.de
+49 89290 365999

Endnotes

1. [How enterprise capabilities influence customer trust and behavior](#), Deloitte, June 2022.
2. Stephen M. R. Covey and Douglas R. Conant, "[The Connection Between Employee Trust and Financial Performance](#)," Harvard Business Review, July 18, 2016.
3. [Deloitte HX TrustID™ Survey](#), May 2020 (n=7,500).
4. Deloitte [2023 Global Future of Cyber Survey](#).
5. [Five actions C-suite leaders can take to protect digital trust in their organization](#), Deloitte.



Want more insights now?

Explore these other Deloitte publications on trust and cyber.

- Deloitte [*Cybersecurity Threat Trends Report 2023*](#)
- Deloitte [*2023 Global Future of Cyber Survey*](#)

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.