

September 2022

Why digital trust truly matters

Consumer faith in cybersecurity, data privacy, and responsible AI hinges on what companies do today—and establishing this digital trust just might lead to business growth.



The results of our survey of more than 1,300 business leaders and 3,000 consumers globally suggest that establishing trust in products and experiences that leverage AI, digital technologies, and data not only meets consumer expectations but also could promote growth. The research indicates that organizations that are best positioned to build digital trust are also more likely than others to see annual growth rates of at least 10 percent on their top and bottom lines. However, only a small contingent of companies surveyed are set to deliver. The research suggests what these companies are doing differently.

46%

of consumer respondents make online purchases at least weekly

The incongruous state of digital trust

A majority of consumers believe that the companies they do business with provide the foundational elements of *digital trust*, which we define as confidence in an organization to *protect consumer data, enact effective cybersecurity, offer trustworthy AI-powered products and services, and provide transparency* around AI and data usage. However, most companies aren't putting themselves in a position to live up to consumers' expectations.

70%

of consumer respondents believe that the companies they do business with protect their data

57%

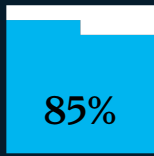
of executives report that their organizations suffered at least one material data breach in the past three years

Consumers value digital trust

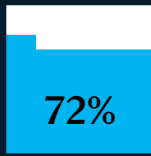


Consumers report that digital trust truly matters. They want companies to provide clear information about their AI and data practices, they expect rigorous data protections to be in place, and they will make purchase decisions based on these premises.

Consumers want transparency about digital policies . . .

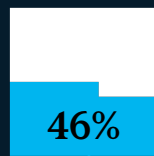


85% of respondents say that knowing a company's **data privacy policies** before making a purchase is important



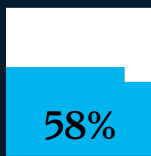
72% of respondents say that knowing a company's **AI policies** before making a purchase is important

. . . and clarity about how their data will be used.

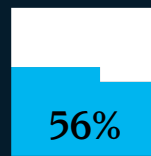


46% often or always consider another brand if the one that they are considering purchasing from is unclear about **how it will use their data**

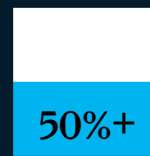
Among several segments, this figure increases to



58% of Asia-Pacific respondents



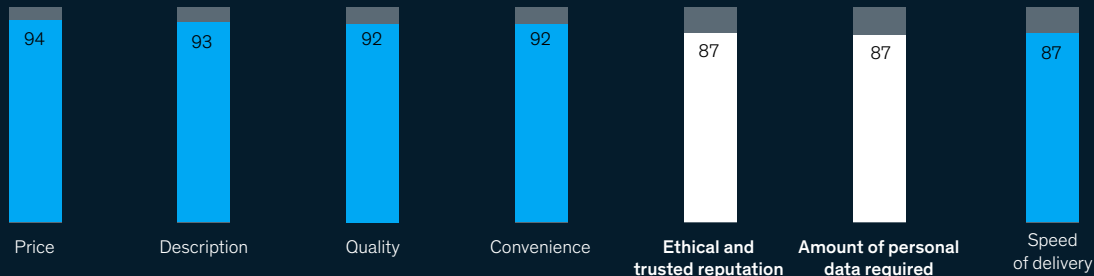
56% of those buying on behalf of their organizations



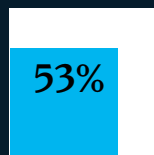
50%+ of millennial and Gen Z respondents

They consider trustworthiness and data protection to be nearly as important as price and delivery time.

Factors important to buying decision, % of respondents

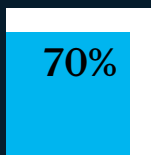


Many will only buy from companies that are known for protecting consumer data . . .

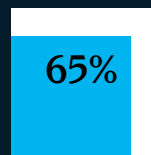


53% make online purchases or use digital services only after making sure that the company has a reputation for protecting **its customers' data**

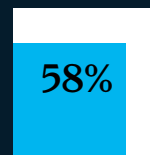
Among several segments, this figure increases to



70% of Latin and South American respondents



65% of those buying on behalf of their organizations



58% of millennial and Gen Z respondents

. . . and they'll stop buying from a company if it violates digital trust.

Stopped doing business with a company that was not protective of customer data, % of respondents



Often or always

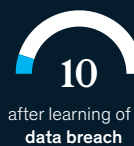


In the past year, at least 1 in 10 of all respondents stopped doing business with a company either because they disagreed with its ethical principles or because they learned of a data breach, even when they didn't know if their own data had been stolen.



14% due to disagreeing with ethical principles

In the past 12 months



10% after learning of a data breach

Source: McKinsey Global Survey on Digital Trust, 3,073 consumers, May 2022

Consumers believe that companies establish a moderate degree of digital trust

When it comes to how organizations are performing on digital trust, consumers express a surprisingly high degree of confidence in AI-powered products and services compared with products that rely mostly on humans. They exhibit a more moderate level of confidence that the companies they do business with are protecting their data. For organizations, this suggests that digital trust is largely theirs to lose.

More than two-thirds of consumers say that they trust products or services that rely mostly on AI the same as, or more than, products that rely mostly on people (Exhibit 1). The most frequent online shoppers, consumers in Asia–Pacific, and Gen Z respondents globally express the most faith in AI-powered products and services, frequently reporting that they trust products relying on AI *more than* those relying largely on people—41 percent, 49 percent, and 44 percent, respectively.

However, these survey results could be influenced, at least in part, by the fact that consumers may not always understand when they are interacting with AI. Although home voice-assisted devices (for example, Amazon’s Alexa, Apple’s Siri, or Google Home) frequently use AI systems, only 62 percent of respondents say that it is likely that they are interacting with AI when they ask one of these devices to play a song.

While 59 percent of consumers think that, in general, companies care more about profiting from their data than protecting it, most respondents have confidence in the companies *they choose* to do business with. Seventy percent of consumers express at least a moderate degree of confidence that the companies they buy products and services from are protecting their data.

And the data suggest that a majority of consumers believe that the businesses they interact with are being transparent—at least about their AI and data privacy policies. Sixty-seven percent of consumers have confidence in their ability to find information about company data privacy policies, and a smaller majority, 54 percent, are confident that they can surface company AI policies.

Exhibit 1

Most consumers trust products and services that rely on AI as much as, or more than, those that rely on people.

Trust in products or services that rely on AI compared with those relying on people,¹ % of respondents



¹We asked respondents to complete this sentence: "I trust products and/or services that mostly rely on artificial intelligence technology _____ those that mostly rely on people."
Source: McKinsey Global Survey on Digital Trust, 3,073 consumers, May 2022

Where consumer digital hygiene could use a cleanup

Much like businesses, a majority of consumers believe that they are taking the appropriate steps to protect themselves from digital threats, yet their behavior suggests otherwise. This presents organizations with the opportunity to

engage with their customers to help them better help themselves.

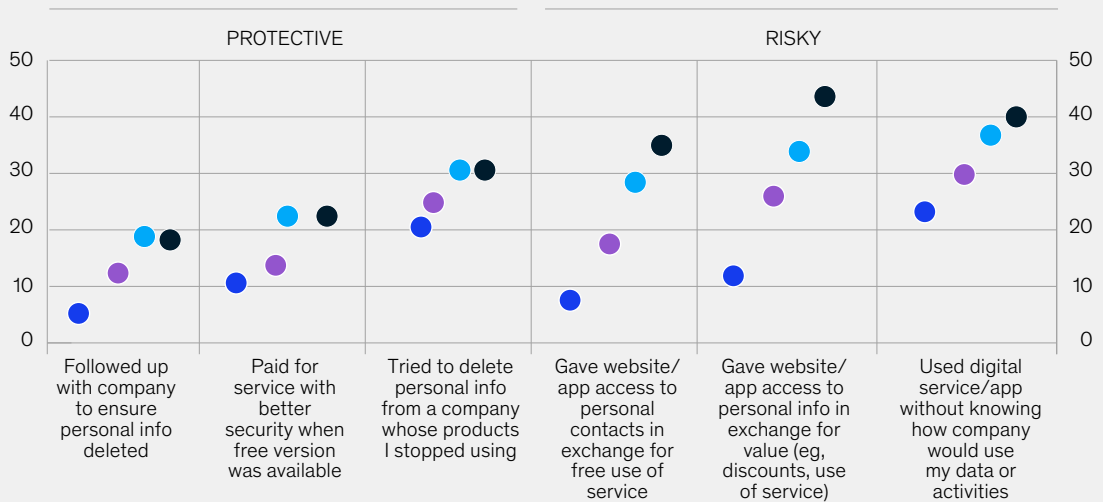
Seventy-seven percent of consumers say that they have at least a moderate degree of confidence that they are adequately protecting their personal information from being stolen or misused online.

Younger consumers are particularly likely to report high confidence in their ability to secure their data—while being more likely to engage in risky behaviors than protective ones. They are also more likely than other generations to store sensitive information online (exhibit).

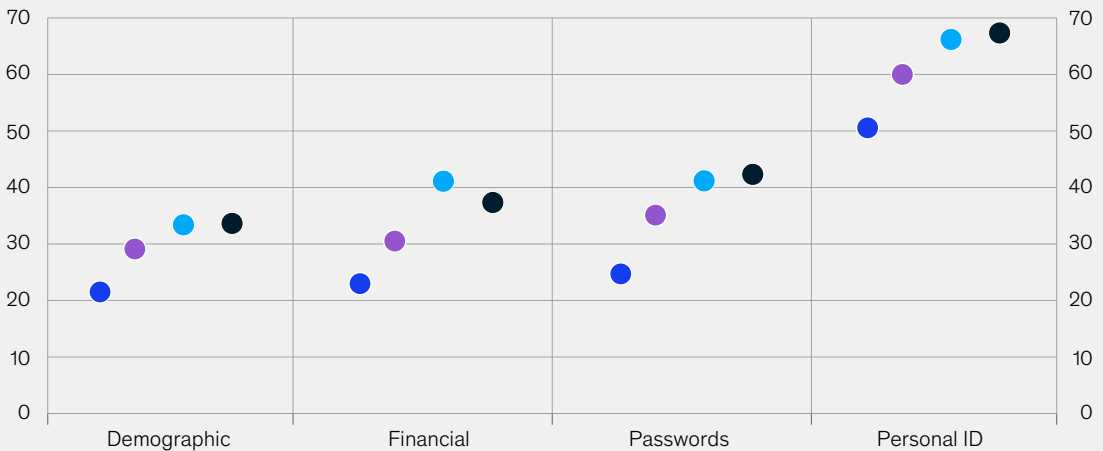
Exhibit

People are more likely to engage in risky online behaviors than protective ones.

Protective and risky consumer online behavior by generation, % of respondents



Type of data consumers saved on a company website by generation, % of respondents



Source: McKinsey Global Survey on Digital Trust, 3,073 consumers, May 2022

Most businesses are failing to protect against digital risks

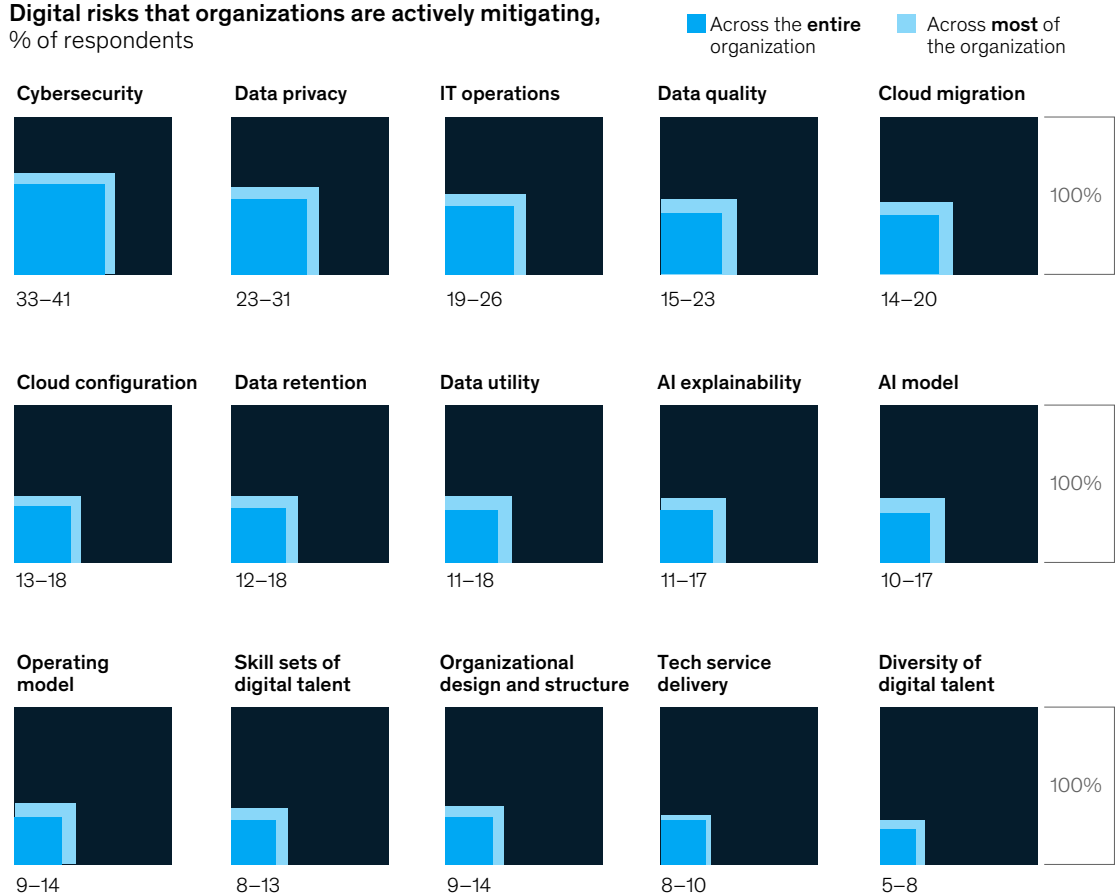
Our research shows that companies have an abundance of confidence in their ability to establish digital trust. Nearly 90 percent believe that they are at least somewhat effective at mitigating digital risks, and a similar proportion report that they are taking a proactive approach to risk mitigation (for example, employing controls to prevent exploitation of a digital vulnerability rather than reacting only after the vulnerability has been exploited). Of the nearly three-quarters of companies reporting that they have codified policies on data ethics conduct (meaning those that detail, for example, how to handle sensitive data and provide transparency on data collection practices beyond legally required disclosures) and the 60 percent with codified AI ethics policies, almost every respondent had at least a moderate degree of confidence that those policies are being followed by employees.

However, the data show that this assuredness is largely unfounded. Less than a quarter of executives report that their organizations are actively mitigating a variety of digital risks across most of their organizations, such as those posed by AI models, data retention and quality, and lack of talent diversity. Cybersecurity risk was mitigated most often, though only by 41 percent of respondents' organizations (Exhibit 2).

Exhibit 2

Few respondents report that their organizations are mitigating digital risks.

Digital risks that organizations are actively mitigating,
% of respondents



Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

Given this disconnection between assumption of coverage and lack thereof, it's likely no surprise that 57 percent of executives report that their organizations suffered at least one material data breach in the past three years (Exhibit 3). Further, many of these breaches resulted in financial loss (42 percent of the time), customer attrition (38 percent), or other consequences.

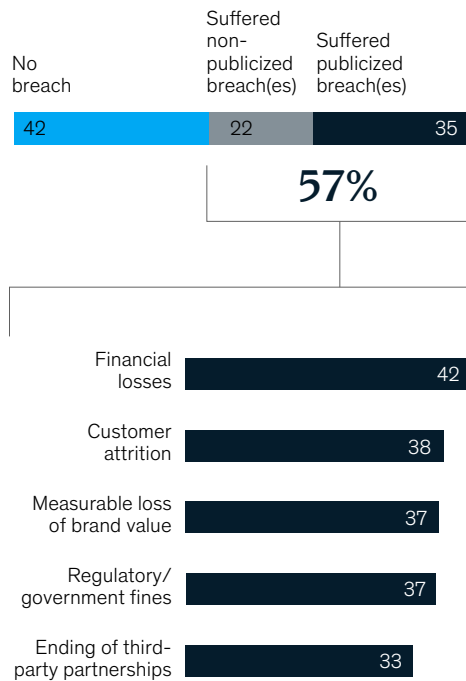
A similar 55 percent of executives experienced an incident in which active AI (for example, in use in an application) produced outputs that were biased, incorrect, or did not reflect the organization's values. Only a little over half of these AI errors were publicized. These AI mishaps, too, frequently resulted in consequences, most often employees' loss of confidence in using AI (38 percent of the time) and financial losses (37 percent).

Advanced industries—including aerospace, advanced electronics, automotive and assembly, and semiconductors—reported both AI incidents and data breaches most often, with 71 percent and 65 percent reporting them, respectively. Business, legal, and professional services reported material AI malfunctions least often (49 percent), and telecom, media, and tech companies reported data breaches least often (55 percent). By region, AI and data incidents were reported most by respondents at organizations in Asia-Pacific (64 percent) and least by those in North America (41 percent reported data breaches, and 35 percent reported AI incidents).

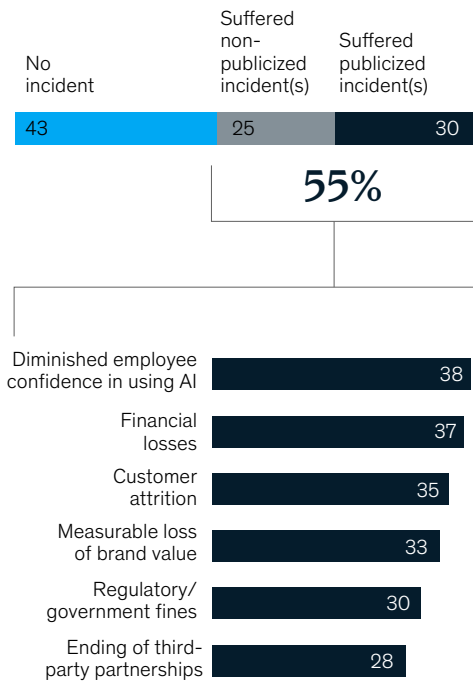
Exhibit 3

More than half of executives reported a recent data breach or AI incident.

At least 1 data breach and effects in the past 3 years,¹% of respondents



At least 1 AI incident and effects in the past 3 years,¹% of respondents



¹Figures do not sum to 100, due to exclusion of those who answered "Don't know."
Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

McKinsey commentary

Liz Grennan

Associate partner, Stamford, CT

Consumers are only just beginning to learn how their data are used, the value this information provides to companies, what digital identity is, and what is or isn't AI. Given that other surveys, such as the Edelman Trust Barometer,¹ show that people in general trust businesses above all other institutions right now, it makes sense that many consumers today simply trust companies to do the right thing on these fronts.

We have seen, however, that with awareness comes heightened concern about these issues. The survey results corroborate this: those who are more digitally savvy or are part of generations that were raised on digital are more likely to consider these issues on par with typical buying factors such as price when making (or discontinuing) purchases. Sales, marketing, and operations teams are likely spending time every day discussing the impact that factors such as pricing and delivery times have on customer behavior; the survey results suggest that it is time to ensure that digital trust is incorporated into these conversations as well.

Additionally, the companies that are doing more to build trust and are communicating this effectively to consumers will likely shift the landscape of consumer expectation even further. As an analogy, consider the increased awareness around the use of trans fat—built up largely through scientific research and company action—and how many food companies now print “no trans fat” on their labels. Consumers are now attuned to looking for trans fats and avoiding them. Those who fail to address trust risk getting “canceled” in consumers' minds. While we see many consumers still using products from companies that have arguably violated trust, we're seeing this slowly start to shift, which the survey results confirm.



¹ 2022 Edelman Trust Barometer, Daniel J. Edelman Holdings, March 10, 2022.

Digital trust connects to growth

The survey results suggest that delivering on digital trust could provide significant benefits beyond satisfying consumer expectations. Leaders in digital trust are more likely to see revenue and EBIT growth of at least 10 percent annually.

Digital-trust leaders are

1.6×

more likely than the global average to see revenue and EBIT growth rates of at least 10 percent

Digital-trust leaders lose less and grow more

Digital-trust leaders are defined as those companies with employees who follow codified data, AI, and general ethics policies and that engage in at least half of the best practices for AI, data, and cybersecurity that we asked about. These companies are outperforming their peers both in loss prevention and business growth.

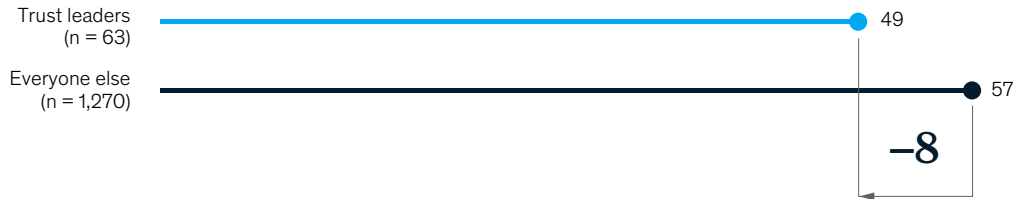
Loss prevention. The companies doing the most to establish digital trust are less likely to have experienced a negative AI incident in the past three years. Forty percent of digital-trust leaders experienced an adverse event in the past three years versus 53 percent of all other institutions. Leaders in digital trust are also less likely to have suffered a data breach, though the difference is less stark: 49 percent versus 57 percent of all others (Exhibit 4).

Growth. Digital-trust leaders are 1.6 times more likely than the global average to see revenue and EBIT growth rates of at least 10 percent. In fact, with every step of progress a company makes toward establishing robust digital trust, we see a correlative increase in the likelihood that a company reports these higher revenue and EBIT growth rates (Exhibit 5). For example, simply codifying ethical conduct, rather than not doing so, is commensurate with higher growth. Making a further commitment to digital trust by incorporating these policies into mission statements correlates with still higher propensities for better growth. And adding in specific best practices in cybersecurity, data protection, and the provision of trustworthy AI increases the likelihood of higher growth further still, with more practices leading to more likelihood for such growth.

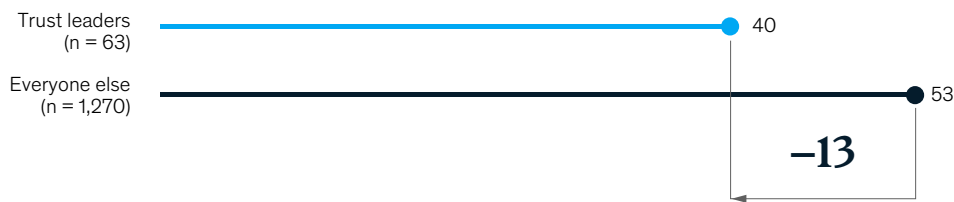
Exhibit 4

Companies most committed to digital trust are less likely to have suffered a recent data breach or AI incident.

Data breaches and effects in the past 3 years, % of respondents



AI incidents and effects in the past 3 years, % of respondents

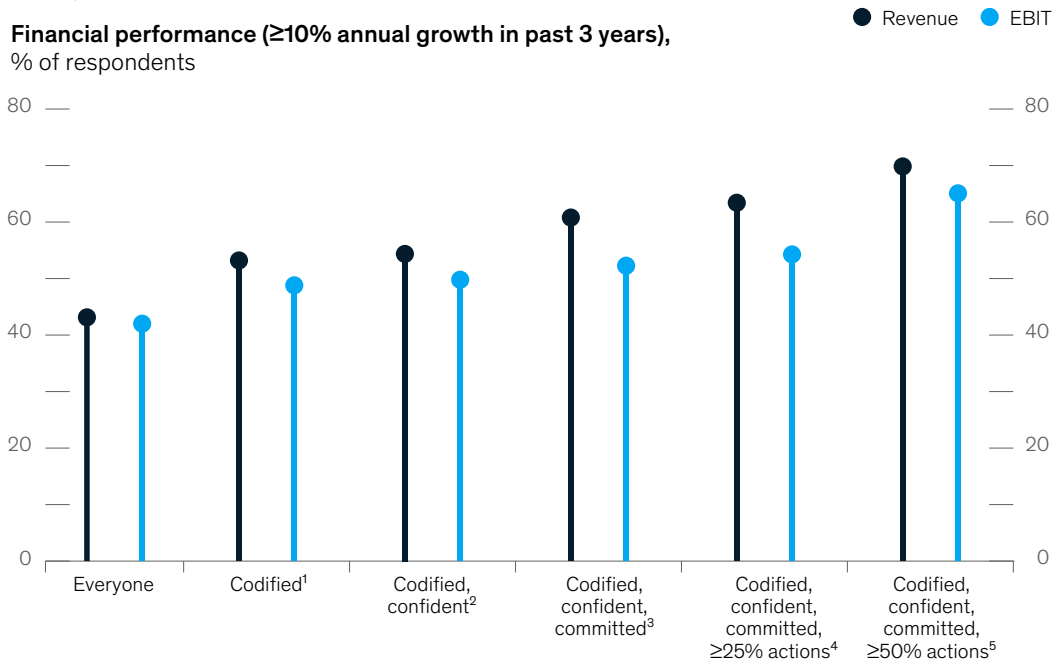


Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

Exhibit 5

The more committed a company is to establishing digital trust, the more likely it is to have a high growth rate.

Financial performance (≥10% annual growth in past 3 years), % of respondents



¹Has codified ethics policies for data, AI, and core values. ²Codified and confident that employees will follow those data, AI, and core ethics policies.

³Codified, confident, and has incorporated those policies in its mission statement. ⁴Codified, confident, committed, and following through with at least 25% of the best practices for data privacy, AI, and cybersecurity. ⁵Codified, confident, committed, and following through with at least 50% of the best practices for data privacy, AI, and cybersecurity.

Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

What digital-trust leaders do differently

A look at the practices of digital-trust leaders shows that their success starts with goal setting. First, they simply set more goals—leaders in digital trust set twice as many goals for trust building (six) than all other organizations. They are also more likely to focus on value-driving goals—particularly, strengthening existing customer relationships and acquiring new customers by building trust and developing competitive advantage through faster recovery from industry-wide disruptions (Exhibit 6).

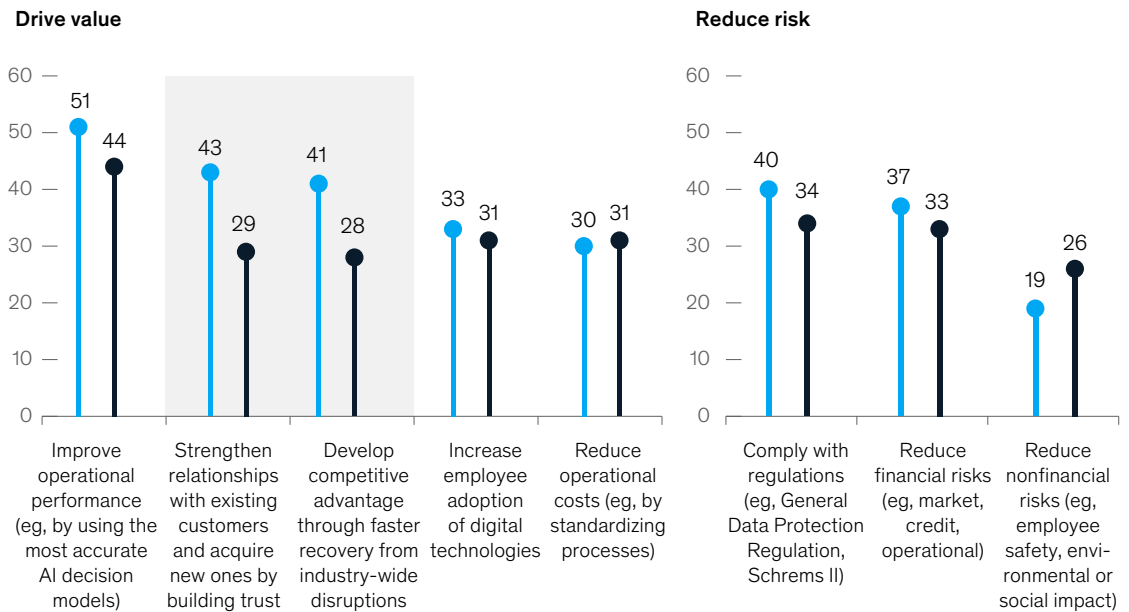
Exhibit 6

For digital-trust leaders, success starts with goal setting.

Goals for digital-risk management, average number per respondent



Goals for risk mitigation, % of respondents who ranked them as a top 3 goal



Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

As digital-trust leaders pursue these goals, they are more likely to mitigate every single digital risk we asked about, from the most obvious, such as cybersecurity, to the less so, such as those associated with cloud configuration and migration (Exhibit 7).

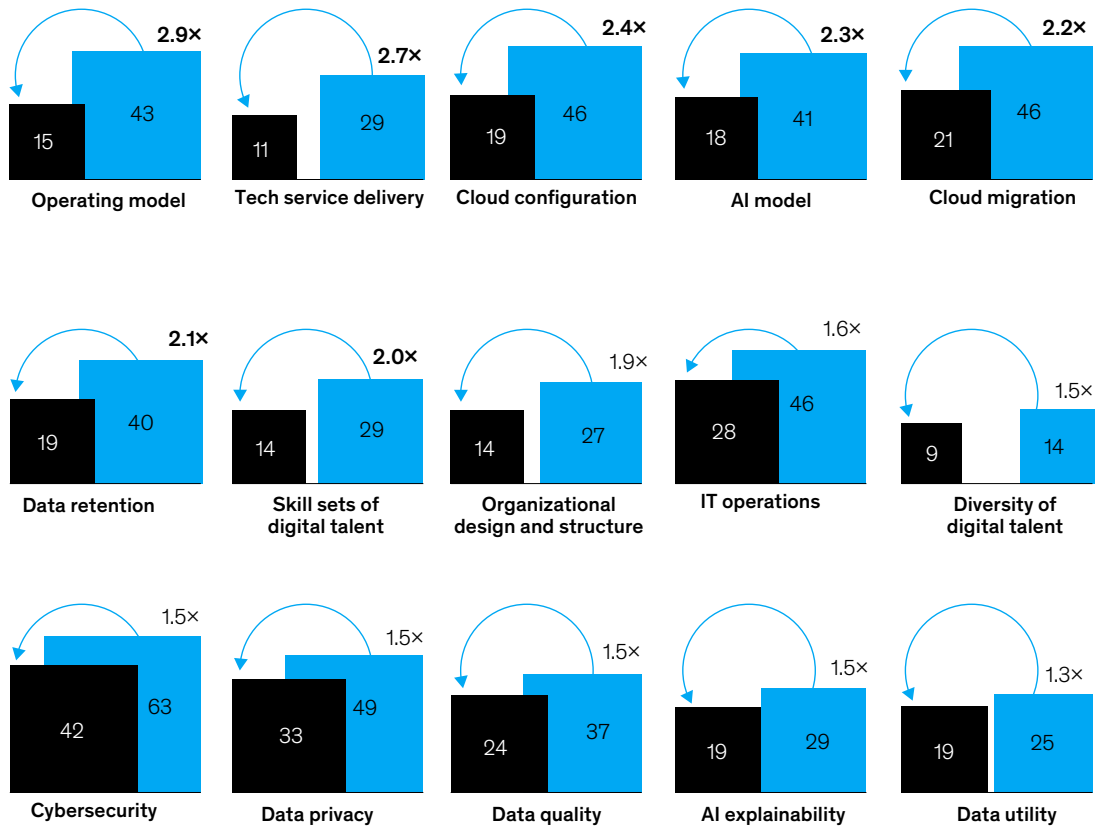
And while, by definition, digital-trust leaders engage in at least half of all the AI, data, and cybersecurity practices we asked about, they are also about twice as likely to engage in any—and every—single one (Exhibit 8).

Exhibit 7

Digital-trust leaders are often twice as likely to mitigate a variety of digital risks.

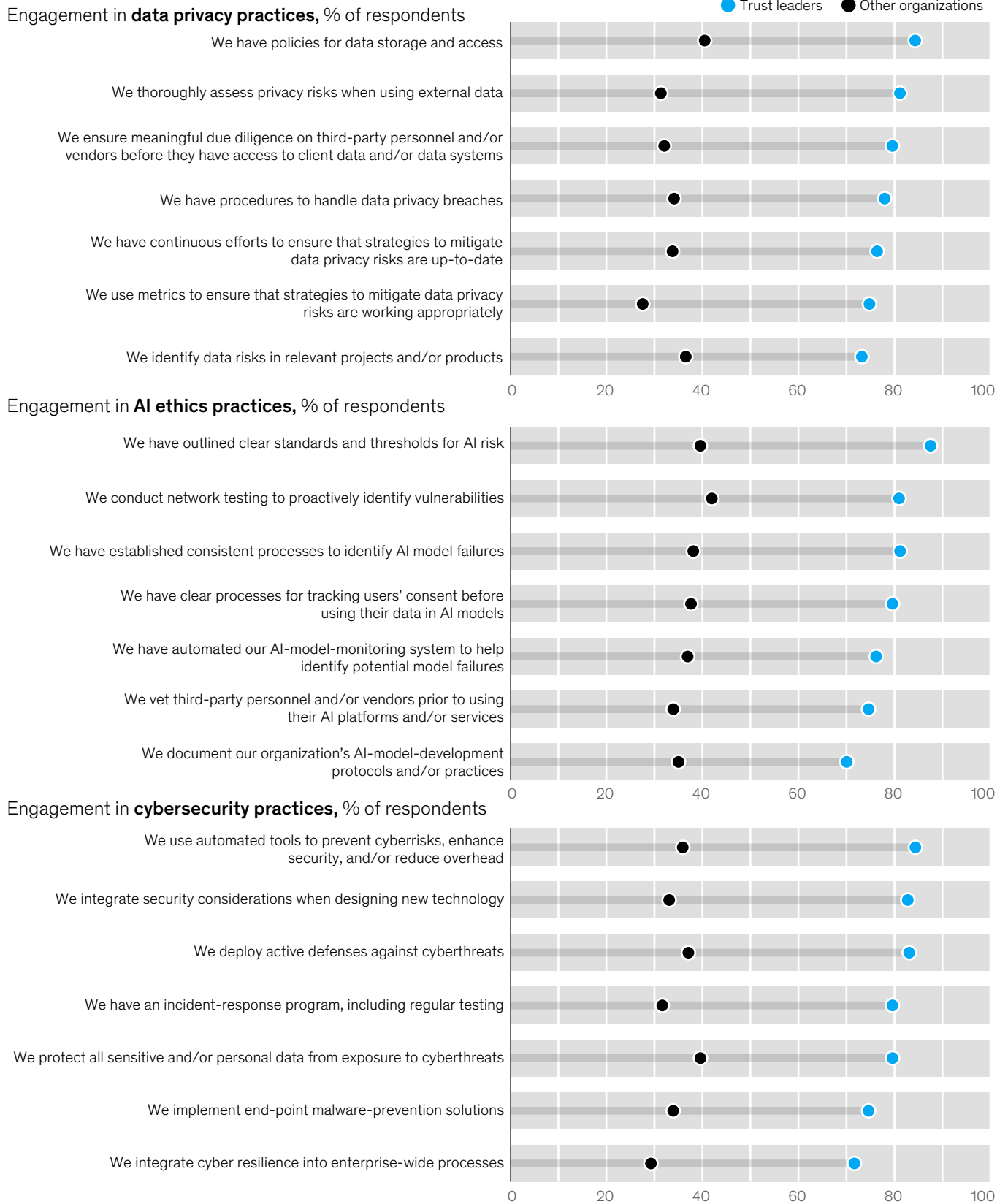
Digital risks that organizations are actively mitigating,
% of respondents

Trust leaders Other organizations



Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

Digital-trust leaders engage in a variety of best practices more often than others.



Note: For space considerations, practices shown are a subset of practices asked about and reflect those followed most often by digital-trust leaders; however, all practices were engaged in by at least 65% of trust leaders, who did so more often than all other organizations.
 Source: McKinsey Global Survey on Digital Trust, 1,333 C-suite and senior executives responsible for risk and technology, May 2022

McKinsey commentary

Jim Boehm

Partner, Washington, DC

Perhaps it is not surprising that the companies that are good at building digital trust are also more likely to experience the best financial performance. We wondered if the reason for this is because these companies simply execute better, and that sound execution results in trust. But the difference in the nature and number of their goals, as well as their commitment to most best practices, suggest a deliberate focus on a trust-building strategy and on performing with superior resilience during periods of great disruption. Our final conclusion is that in a digitally connected and data-driven world, achieving digital trust is a major strategic imperative and a huge business differentiator.

Managing trust can no longer focus solely on protecting against “what if” scenarios. Rather, executives need to think about trust in terms of what more can it enable us to do. Companies that build trust relationships with their customers can, for example, use data in broader, more creative ways to craft even more personalized services with higher conversion rates. In a separate analysis we are running, early results show that trusted brands have outperformed untrusted brands by a meaningful margin over the past five years. The picture is becoming clear that digital trust conveys an economic benefit.

One thing that did surprise and concern me is the lack of awareness among companies around what “good” looks like when it comes to building digital trust, particularly around cybersecurity. This is generally considered to be a more mature risk vector, but clearly we have more to do there, and we should widen the aperture to include adjacent areas in AI and data.

The takeaway from this research is clear: consumers are putting the safety of their digital identity in the hands of businesses they trust. Companies with digital products and services should prioritize measures that help maintain consumer trust. The practices we asked about for this survey, which we culled from best-of-breed institutions, suggest places to start. At the end of the day, building digital trust not only is the right thing to do but also offers the potential to unlock a future horizon of growth, making it a win–win for customers and organizations alike.



About the research


The data for this article were obtained through two global online surveys: one answered by business leaders, the other by consumers. Both were conducted from April to May 2022. The business leader survey included responses from 1,333 senior business executives (one-third of whom were CEOs) across 27 industries in 20 countries, including Australia, Brazil, Colombia, Germany, India, Indonesia, Pakistan, Singapore, Spain, the United Kingdom, and the United States. The consumer survey included responses from 3,073 adults from the same countries. The data were adjusted to better fit the survey sample to population estimates within each country using age and gender weights globally and, in the United States only, by weighting for region, income, and ethnicity.

The survey content and analysis were developed by **Jim Boehm**, a partner in McKinsey's Washington, DC, office; **Liz Grennan**, an associate partner in the Stamford, Connecticut, office; **Alex Singla**, a senior partner in the Chicago office; and **Kate Smaje**, a senior partner in the London office.

The authors wish to thank Elisabeth Ferland, Christopher Kahn, Andreas Kremer, and Dan Rubin for their contributions to this article.

Designed by McKinsey Global Publishing
Copyright © McKinsey & Company.

McKinsey.com/Digital

 [@McKinseyDigital](https://twitter.com/McKinseyDigital)

 McK.com/Digital

Find more content like this on the
McKinsey Insights App



Scan • Download • Personalize

