CISCO
SECURE

CISCO
The bridge to possible

# Privacy's Growing Importance and Impact

CISCO 2023 DATA PRIVACY BENCHMARK STUDY

# Table of Contents

## Introduction

Privacy continues to increase in importance for organizations around the world and those they serve. Data privacy remains mission critical and an attractive investment for organizations as reflected in its integration into business priorities and processes, economic value, and visibility to senior management and the Board of Directors. Yet, organizations' priorities regarding the use of personal data are not fully aligned to those of consumers, especially when it comes to using Artificial Intelligence (AI) and automation to make decisions that affect the individual. This report, our sixth annual review of key privacy challenges for organizations, examines privacy's impact on organizations around the world.

## Methodology

The data in this study is derived from the Cisco Security Outcomes survey in which respondents were anonymous to the researchers and not informed who was conducting the study. Using the same methodology as prior years, more than 4700 security professionals from 26 geographies[1] completed the survey in Summer 2022. Survey respondents represent major industries and a mix of company sizes. (See Appendix) We directed privacy specific questions to the more than 3100 respondents who indicated they are familiar with the data privacy program at their organizations. In this report, we also included relevant results from the Cisco 2022 Consumer Privacy Survey[2], which was completed in Summer 2022 by 2600 adults in 12 geographies.

[1] Australia, Brazil, Canada, Chile, China, Columbia, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Philippines, Saudi Arabia, Singapore, South Korea, Spain, Taiwan, Thailand, The Netherlands, UK, US, and Vietnam.

[2] Cisco 2022 Consumer Privacy Survey: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

## Key findings:

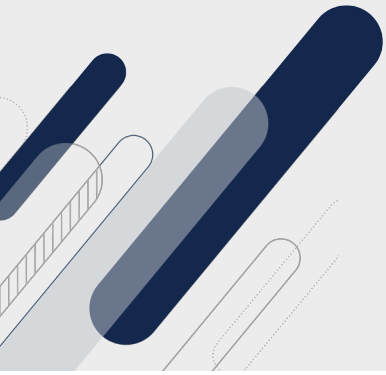
1. Privacy continues to be an attractive investment for organizations globally, even in a difficult economic climate, delivering higher average benefits across the board, and a strong 1.8 times return on investment.
2. Nearly all organizations have integrated privacy into their priorities and processes with 98% of respondents reporting privacy-related metrics to their Board of Directors and 95% saying "all of their employees" need to know how to protect data privacy.
3. Organizations are not fully in sync with consumers when it comes to building trust — especially in the use of their personal data for AI and automated decision-making.
4. Organizations are recognizing that global providers, operating at scale, can better protect their data compared to local providers.

### 1: The economics and importance of privacy remain strong

Privacy continued to be a critical business driver for organizations around the world in 2022, with the vast majority of survey respondents confirming the value and importance of privacy. Ninety-five percent (95%) of respondents said privacy is a business imperative, up from 90% last year. Ninety-four percent (94%) said their customers would not buy from them if their data was not properly protected, up from 90% a year ago. And 95% said privacy is an integral part of their organizations' culture, up from 92%. See Figure 1.

## Figure 1: Importance of privacy to organizations


Source: Cisco 2023 Data Privacy Benchmark Study

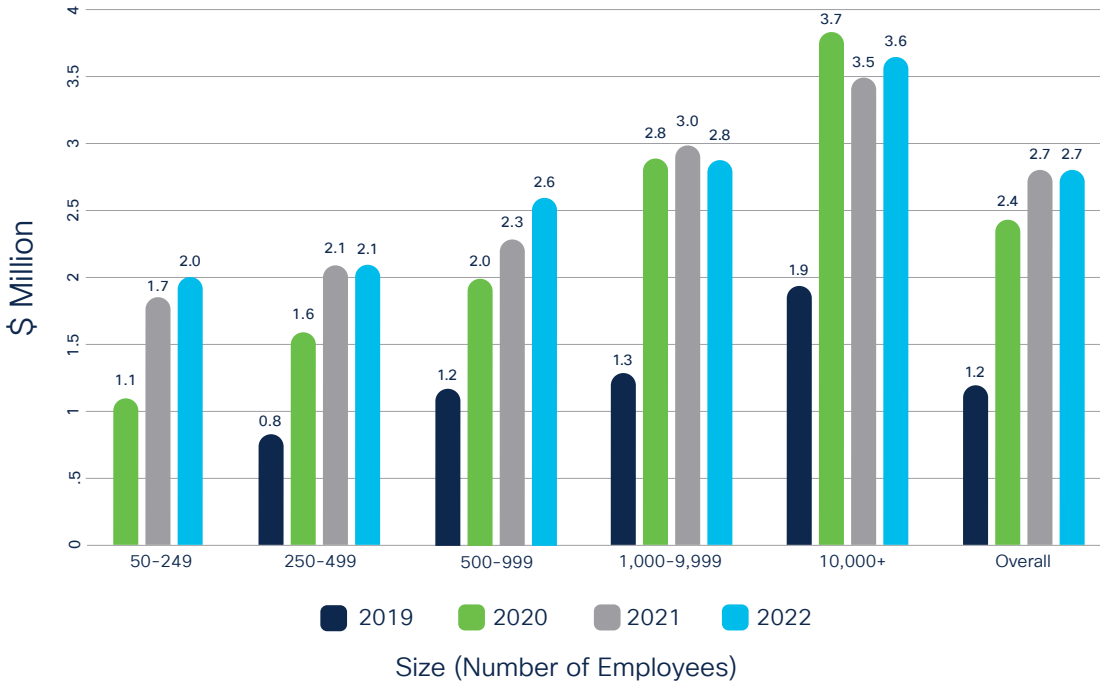


"An organization's approach to privacy impacts more than compliance. Investment in privacy drives business value across sales, security, operations, and most importantly, trust."

Dev Stahlkopf, Executive Vice President and Chief Legal Officer, Cisco

Despite a difficult economic environment in 2022, privacy spending did not decrease, and in some cases, grew in 2022. The average spending was $2.7 Million, up significantly from $1.2 Million just 3 years ago. The most significant growth from 2021 to 2022 occurred at smaller organizations: spending at organizations with 50-249 employees increased more than 17% to $2.0 Million from $1.7 Million. At organizations with 500-999 employees, spending rose more than 13% to $2.6 Million from $2.3 Million. Spending at larger organizations remained relatively unchanged after steep increases from 2019 to 2020. See Figure 2.

## Figure 2: Privacy spending, 2019-2022

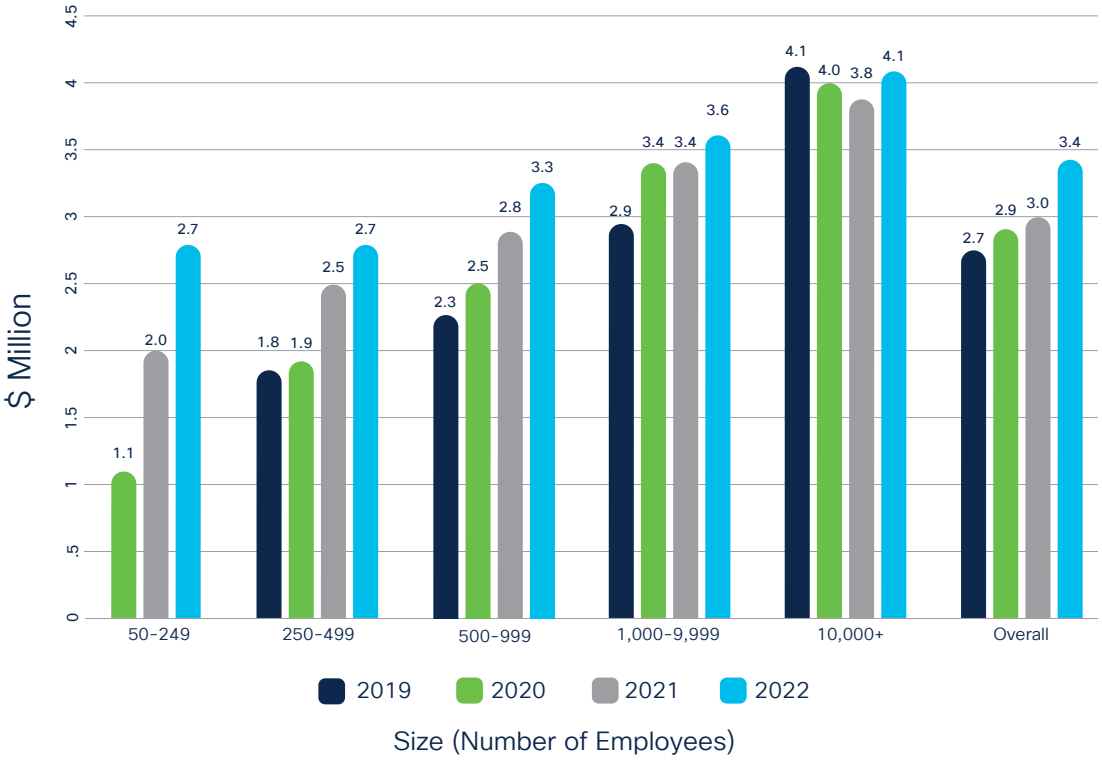



Note: 50-249 category initiated in 2020

Source: Cisco 2023 Data Privacy Benchmark Study

At the same time, the estimated dollar value of benefits from privacy were up significantly this year. The average estimate rose more than 13% to $3.4 Million from $3.0 Million last year with significant gains across the various organization sizes. Benefits at organizations with 50-249 employees rose 35% to $2.7 Million from $2.0 Million, and those with 500-999 employees rose 18% to $3.3 Million from $2.8 Million. Estimated benefits at larger organizations of 1000-9999 employees and 10,000+ employees also rose 6% and 8% respectively as shown in Figure 3.

## Figure 3: Estimated privacy benefits, 2019-2022

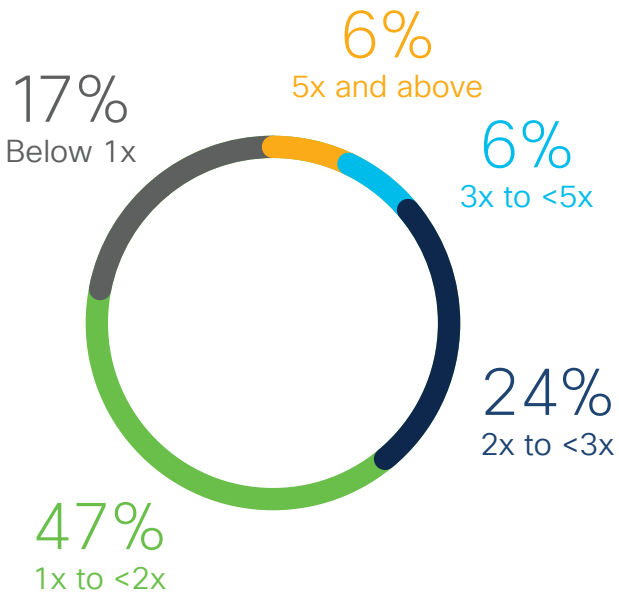



Note: 50-249 category initiated in 2020

Source: Cisco 2023 Data Privacy Benchmark Study

Putting spending and the estimated dollar value of the benefits together, privacy remains a very attractive financial investment for most organizations. The average organization is getting benefits estimated to be 1.8 times spending, as it was in last year's survey. Thirty-six percent (36%) of organizations, up from 32% last year, are getting returns at least twice their spending with many realizing returns upwards of 3 to 5 times their investment. See Figure 4.

## Figure 4: ROI ranges for respondents

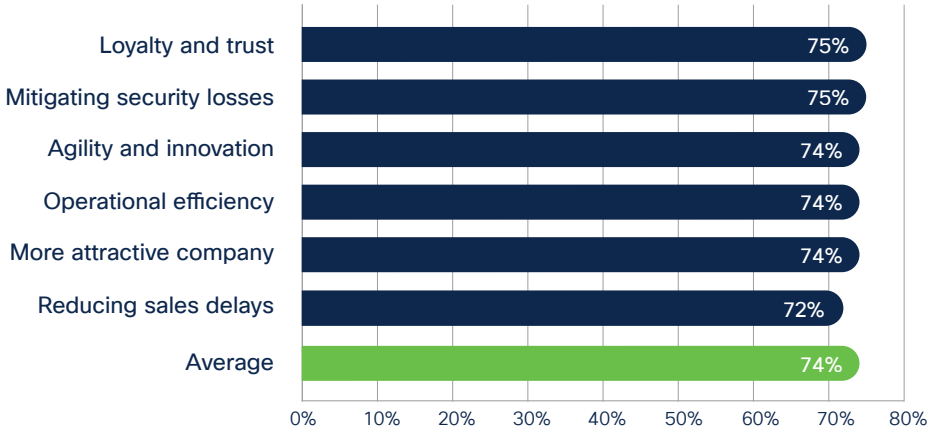



Source: Cisco 2023 Data Privacy Benchmark Study

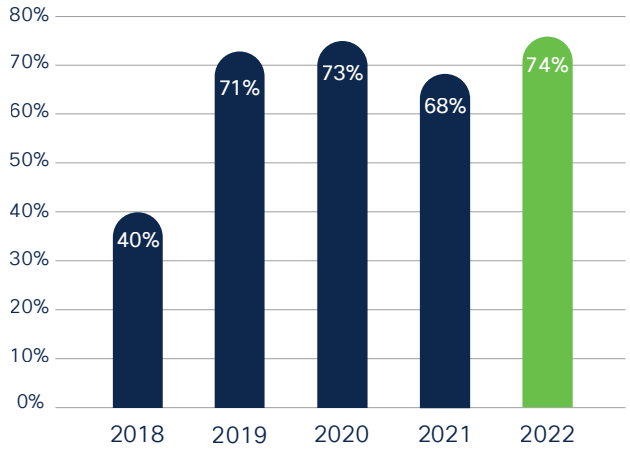
We continue to ask respondents about specific areas of potential benefits from privacy, including reducing sales delays, mitigating losses from data breaches, enabling innovation, achieving operational efficiency, building trust with customers, and making their company more attractive. Among this year's respondents, over 70% indicated they were getting "significant" or "very significant" benefits from each of these areas. The average across the six areas was 74%, representing a significant increase from the 40% average response in our first survey from 2018 and up 6% from last year. See Figure 5.

## Figure 5: Organizations recognizing business benefits of privacy investment

### Percentage getting significant benefits in each area, 2022




### Averages, 2018–2022



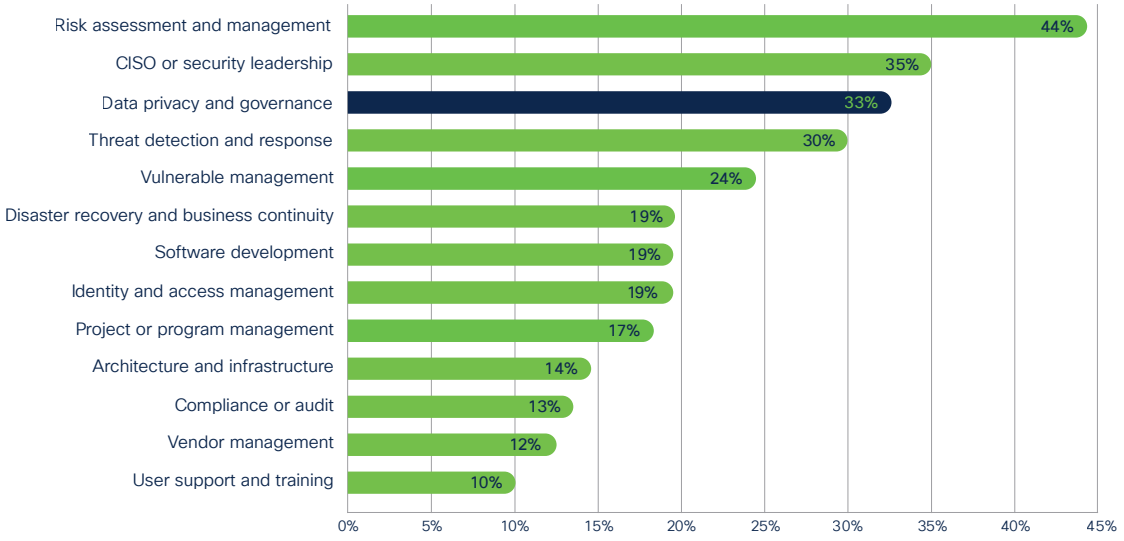

Source: Cisco 2023 Data Privacy Benchmark Study

## 2: Integration of privacy into organizational roles and responsibilities

With privacy as a critical business priority, more organizations are recognizing that everyone across their organization plays a vital role in protecting personal data. In this year's survey, 95% of respondents said that "all of their employees" need to know how to protect data privacy.

Additionally, privacy skills are particularly critical among those who are directly responsible for keeping data safe. The security professionals who completed our survey were asked to define their top 3 areas of responsibility: One-third (33%) of these respondents selected "Data Privacy and Governance," ranking only behind "Risk Assessment and Management" (44%) and "CISO or Security Leadership" (35%). See Figure 6.

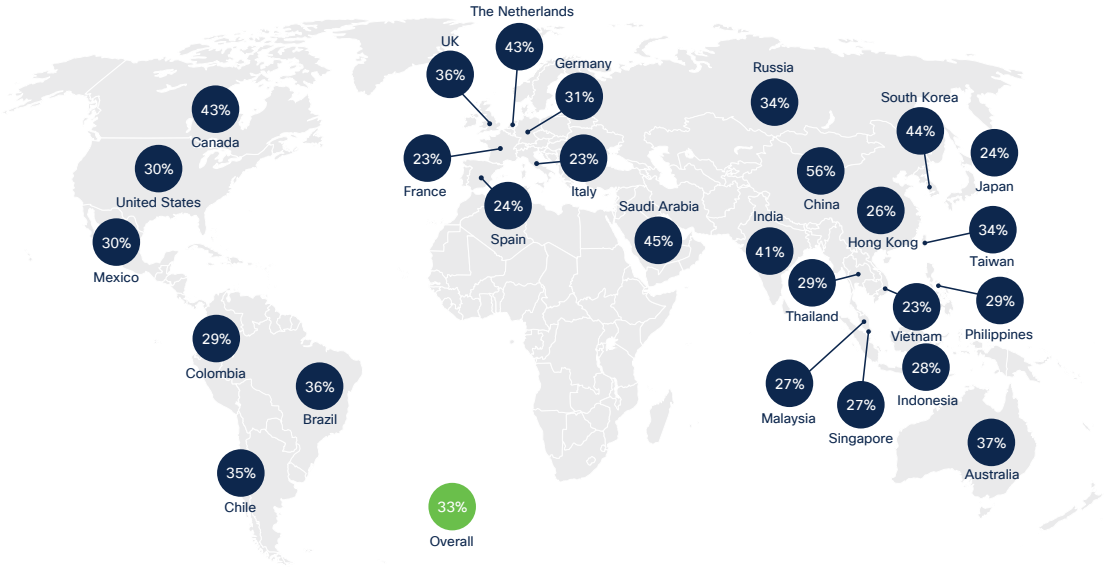
# Figure 6: Top job responsibilities among security professionals




Source: Cisco 2023 Data Privacy Benchmark Study

This data shows that organizations recognize the need for privacy skills among all employees and with specific competencies for security teams to ensure that those who are authorized to access and work with the data will handle it appropriately. Interestingly, this percentage was quite consistent across the globe with regional averages in the Americas, APJC, and EMEA at 32-33%. No country was lower than 23% and only China was above 50% as shown in Figure 7.

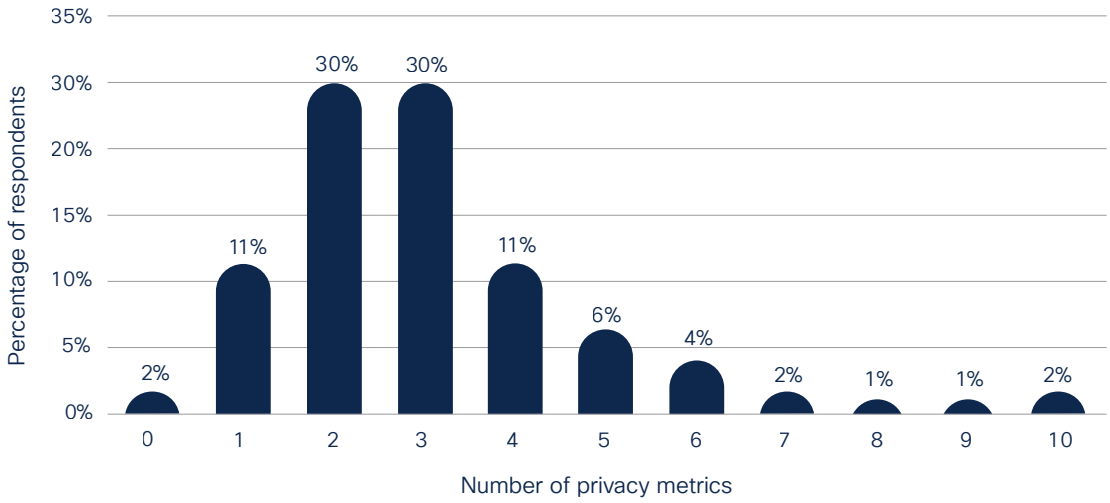
## Figure 7: Percentage of respondents identifying privacy as job responsibility, by geography




Source: Cisco 2023 Data Privacy Benchmark Study

Another important indication of privacy's importance to the organization is the use of privacy metrics, especially when they are reported to executive management and the Board of Directors. Among the organizations in this year's survey, 98% are reporting one or more privacy-related metrics to the Board, up from 94% in last year's survey. See Figure 8 below.

## Figure 8: Number of privacy metrics reported to the Board



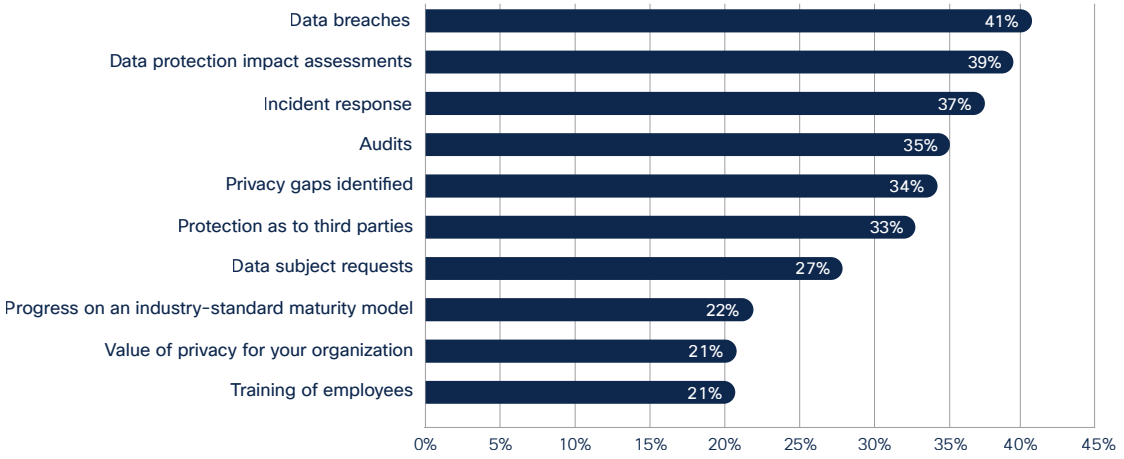

Source: Cisco 2023 Data Privacy Benchmark Study

**"When it comes to earning and building trust, compliance is not enough."**

Harvey Jang, Vice President and Chief Privacy Officer, Cisco

While some are reporting as many as 10 privacy metrics, the average number was 3.1, which is up 19% from 2.6 in last year's survey. The most-reported metrics include the status of any Data Breaches (41%), Data Protection Impact Assessments (39%), and Incident Response (37%) as described in Figure 9.

## Figure 9: Privacy metrics reported to the Board

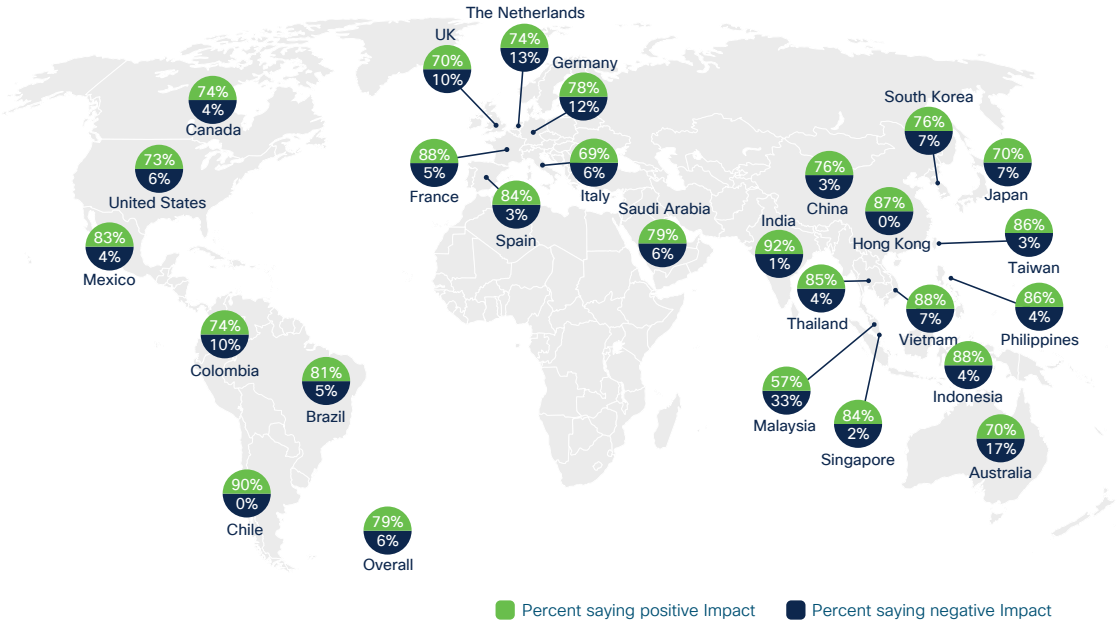



Source: Cisco 2023 Data Privacy Benchmark Study

Privacy legislation continues to be very well-received around the world. These laws play an important role in helping to ensure that governments are holding organizations accountable for how they manage personal data, and 157 countries (up from 145 last year) now have privacy laws in place[3].

Even though complying with these laws often involves significant effort and cost (e.g., cataloging data, maintaining records of processing activities, implementing controls – privacy by design, responding to user requests), organizations recognize the positive impact on their organizations. Seventy-nine percent (79%) of all corporate respondents said privacy laws have had a positive impact, 14% were neutral, and only 6% indicated that the laws have had a negative impact. The positive percentages were quite consistent across regions, with 77% in the Americas, 79% in EMEA, and 81% in APJC. By country, the highest average percentages were in India (92%), Chile (90%), France, Indonesia and Vietnam (88%). See Figure 10.

## Figure 10: Reaction to privacy laws globally




Source: Cisco 2023 Data Privacy Benchmark Study

[3] Source: Privacy Laws & Business 2022. https://www.privacylaws.com/reports-gateway/articles/int176/int176newdplaws/

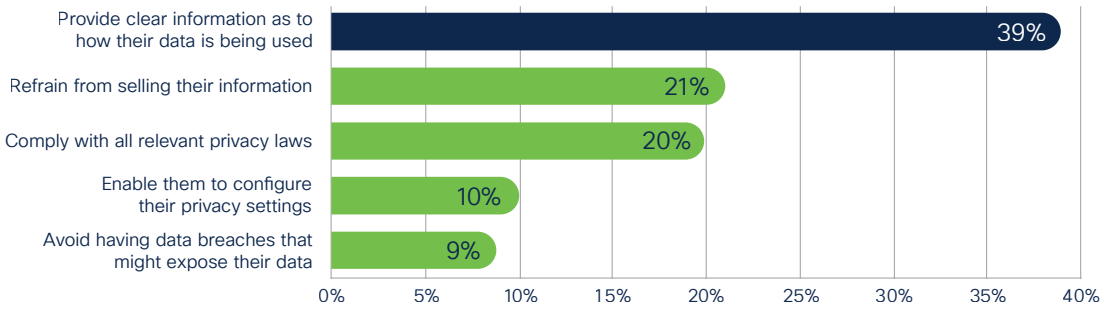
### 3: Disconnect between organizations and consumers regarding data and trust

Customers willingly share their personal data with organizations to obtain goods and services along with a tailored, personalized experience. Customers expect organizations to be transparent about their practices and treat personal data properly – a significant aspect of earning and building trust. As described in the Cisco 2022 Consumer Privacy Survey, 76% of consumers said they would not buy from an organization they did not trust with their data, and 81% agreed that the way an organization treats their data is indicative of how it views and respects its customers.

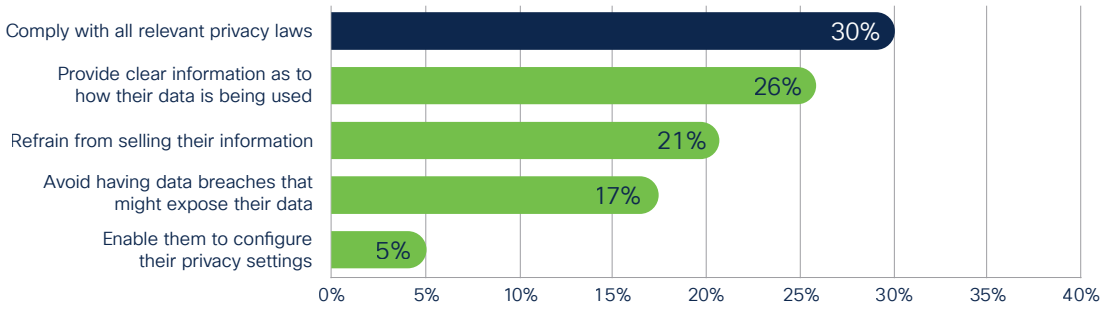
Among organizations responding to this year's Data Privacy Benchmark Survey, 96% agreed they have an ethical obligation to treat data properly, up from 92% in last year's survey. However, their priorities are not fully consistent with those expressed by consumers. Transparency – providing easily accessible and clear information about how their data is being used – was the top priority for respondents (39%) in the consumer survey. Nearly twice as many respondents selected transparency as the top priority compared with not selling personal information or compliance with privacy laws. Yet, in this year's survey of organizations, respondents felt compliance is the most important priority for building customer trust (cited by 30%), followed by transparency (26%). Certainly, organizations need to comply with privacy laws, but when it comes to earning and building trust, compliance is not enough. Consumers consider legal compliance to be a "given," with transparency more of a differentiator. See Figure 11.

## Figure 11: Priorities for building consumer trust

### Consumer view




### Organizational view

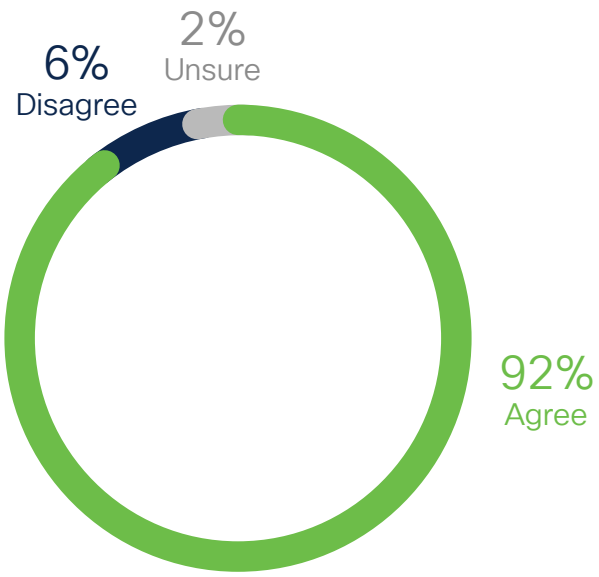



Source: Cisco 2023 Data Privacy Benchmark Study

This disconnect can also be seen when it comes to the use of Artificial Intelligence (AI). While consumers are generally supportive of AI and many are even willing to share their anonymized data to help build better AI solutions, automated decision-making remains an area of concern. It can be difficult for consumers to understand the algorithms and automated decisions that may impact them directly, such as when qualifying for a loan or getting a job interview. Ninety-six percent (96%) of organizations in our survey believe they have processes already in place to meet the responsible and ethical standards that customers expect, which is up from 87% last year. Yet, the majority of consumers don't see it that way.

As reported in the Cisco 2022 Consumer Privacy Survey, 60% of consumers are concerned about how organizations apply and use AI today, and 65% already have lost trust in organizations over their AI practices. Fortunately, organizations may be starting to get the message that they aren't doing enough. Ninety-two percent (92%) of respondents said that when it comes to the application and use of AI in their solutions, their organization needs to be doing more to reassure customers that their data is only being used for intended and legitimate purposes. See Figure 12.

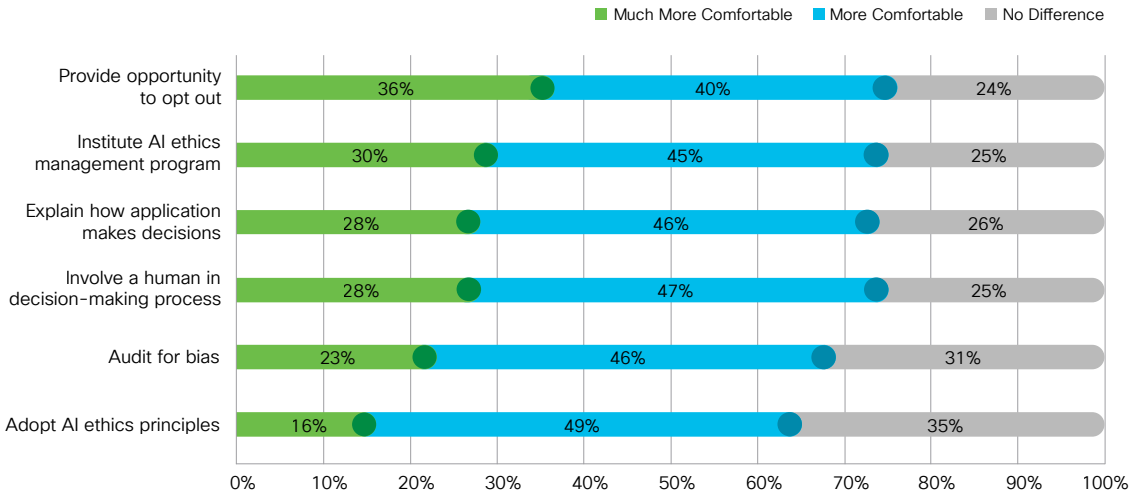
## Figure 12: Percentage agreeing that their organization needs to do more to reassure customers that their data is only being used for legitimate purposes




Source: Cisco 2023 Data Privacy Benchmark Study

What can organizations do? The top approach for making consumers much more comfortable would be to provide opportunities for them to opt out of the solution in which AI is applied or used, cited by 36% of respondents to the consumer survey. See Figure 13.

## Figure 13: Approaches for making consumers more comfortable with AI, consumer view

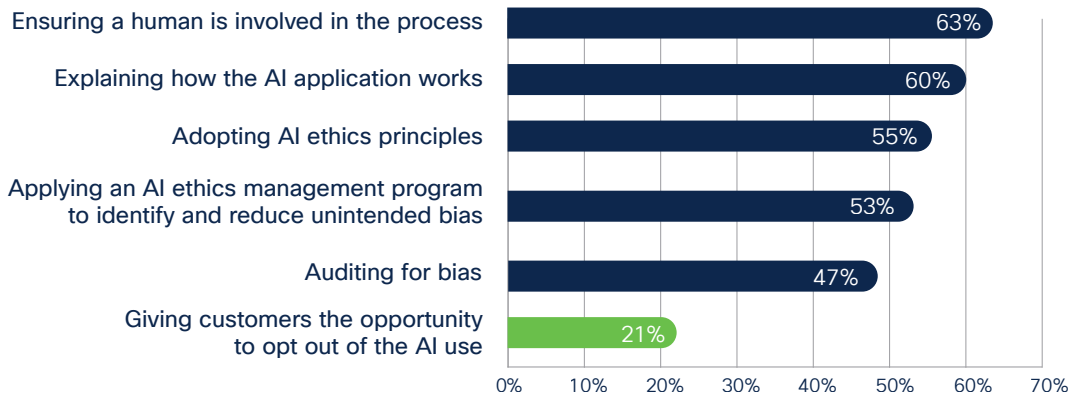



Source: Cisco 2023 Data Privacy Benchmark Study

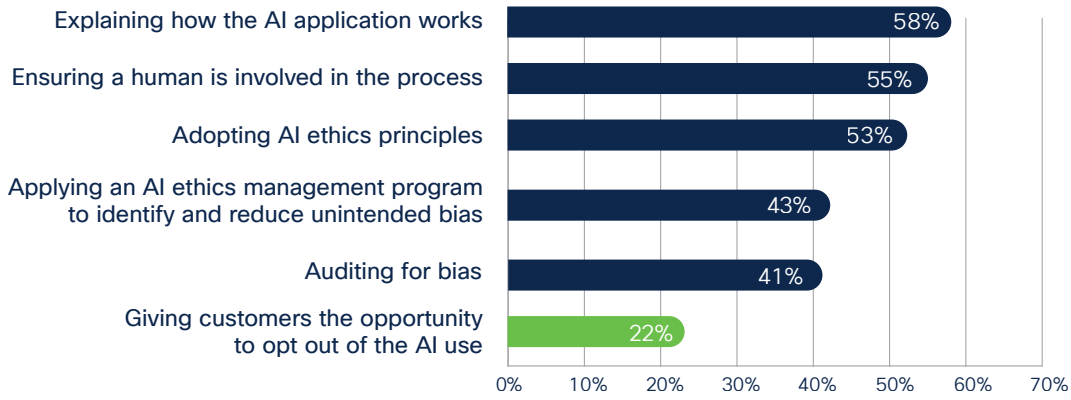
Yet, what actions have organizations actually put in place and what do they think would most reassure the customer? For both of these questions, providing opt-out opportunities was selected least among the six options. Sixty-three percent (63%) of organizations are ensuring that a human is involved in the decision-making process, 60% provide greater transparency, and 55% have adopted AI ethics principles into their operations. Only 21% said that they give customers the opportunity to opt out. The responses are quite similar to what organizations believe is the most-effective approach. Most options were selected by 41% to 58% of the respondents, and only 22% selected "giving customers the opportunity to opt out," as shown in Figure 14.

## Figure 14: Approaches for making consumers more comfortable with AI, organizational view

### What organizations have done




### What organizations say would be most effective




Source: Cisco 2023 Data Privacy Benchmark Study

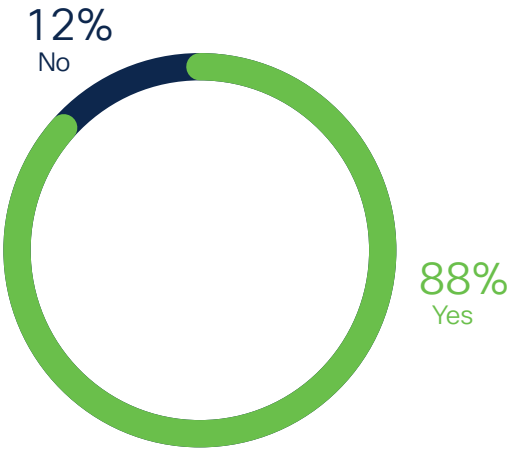
### 4: Despite the desire for data localization, global providers are seen as safer than local providers

Many governments and organizations are putting in place data localization requirements, which force data to be kept within a country or region. To many, these requirements seem like a good idea at first, but our research indicates this view does not hold up once costs, security, privacy, and other tradeoffs are considered. In the Cisco 2022 Consumer Privacy Survey, for example, 78% of consumers initially said that they thought data localization was a good idea, but support dropped to 41% when including the added cost for goods and services. According to 89% of the organizations in this year's survey, data localization does add significant cost to their operations.

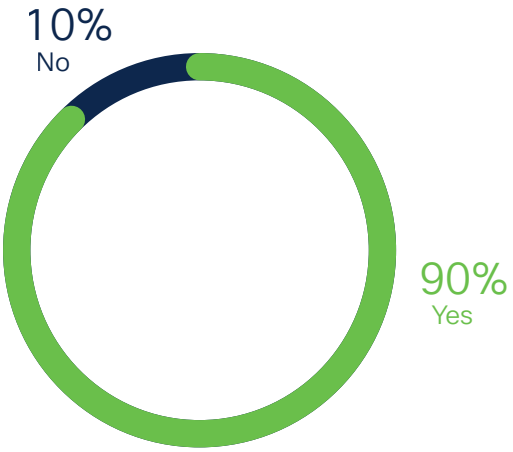
Results from this current study show that the vast majority (88%) of respondents believe that their data would be inherently safer if it is only stored within their country or region. Remarkably, an even larger number (90%) also said that a global provider, operating at scale, can better protect the data compared to local providers. When viewing these two statements together, it seems that while organizations would ideally like to keep their data local, they still prefer and trust a global provider over a local provider. Of course, their ideal solution would be to get both – a local instance that retains the data locally set up by a global provider. See Figure 15 below.

## Figure 15: Data localization

Data would be inherently safer if it can be stored within our country or region



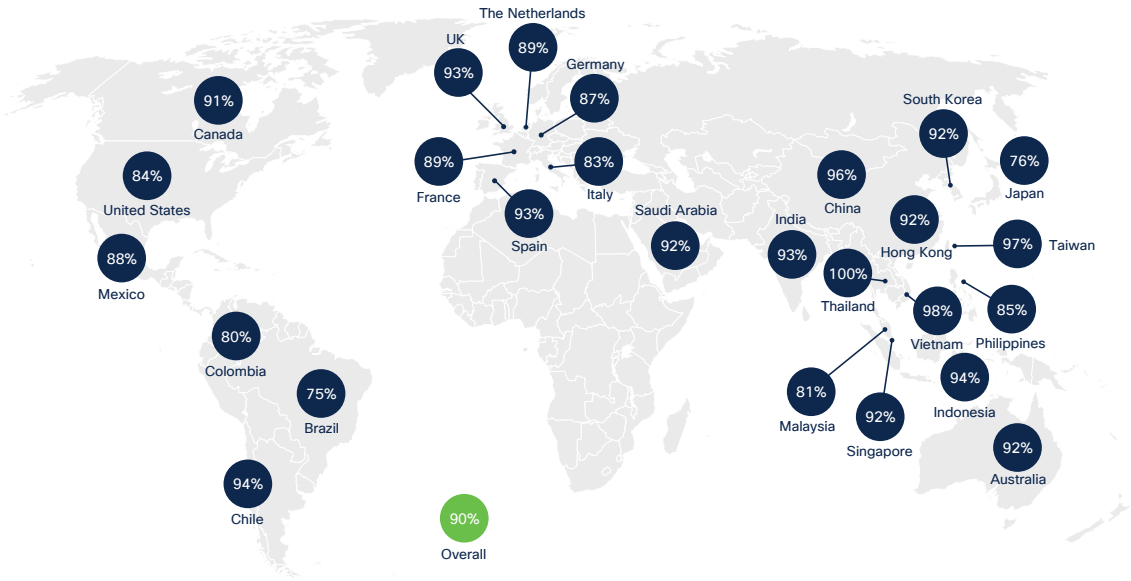

Global providers can better protect our data compared to local providers




Source: Cisco 2023 Data Privacy Benchmark Study

While data localization is often driven by national laws and attitudes, there was not substantial variation across respondents in different geographies. The percentage of respondents saying "a global provider can better protect data compared to a local provider" was between 75% and 100% in all 26 geographies of respondents. See Figure 16.

## Figure 16: Percentage agreeing that a global provider can protect data better than a local provider




Source: Cisco 2023 Data Privacy Benchmark Study

## Conclusion and recommendations

This research highlights the importance of privacy to organizations and the growing economic value of privacy investments. Even as privacy is further integrated into organizational priorities and processes, it will be important for organizations to meet more of consumer's expectations regarding transparency and the use of personal information in AI-driven decision making. Doing so will help improve an organization's privacy posture, demonstrate trustworthiness, and maximize the benefits of privacy investments. The findings in this research point to these specific recommendations:

1. Continue to invest in privacy and build privacy capabilities throughout your organization, especially among security and IT professionals and those who are involved directly with personal data processing and protection.

2. Be more transparent with your customers about how their personal data is being used by the solutions and services your organization delivers. While organizations need to comply with the law, compliance alone is not enough; transparency is key to trust.

3. When using AI in your solutions, design with AI ethics principles in mind, provide preferred management options to reassure customers, deliver greater transparency to the automated decision, and ensure that a human is involved in the process when the decision is consequential to a person.

4. Consider the costs and consequences of data localization and recognize that local providers may be more expensive and degrade the functionality, privacy, and security of your data than global providers operating at scale.

## Meeting our customers' standard of trust

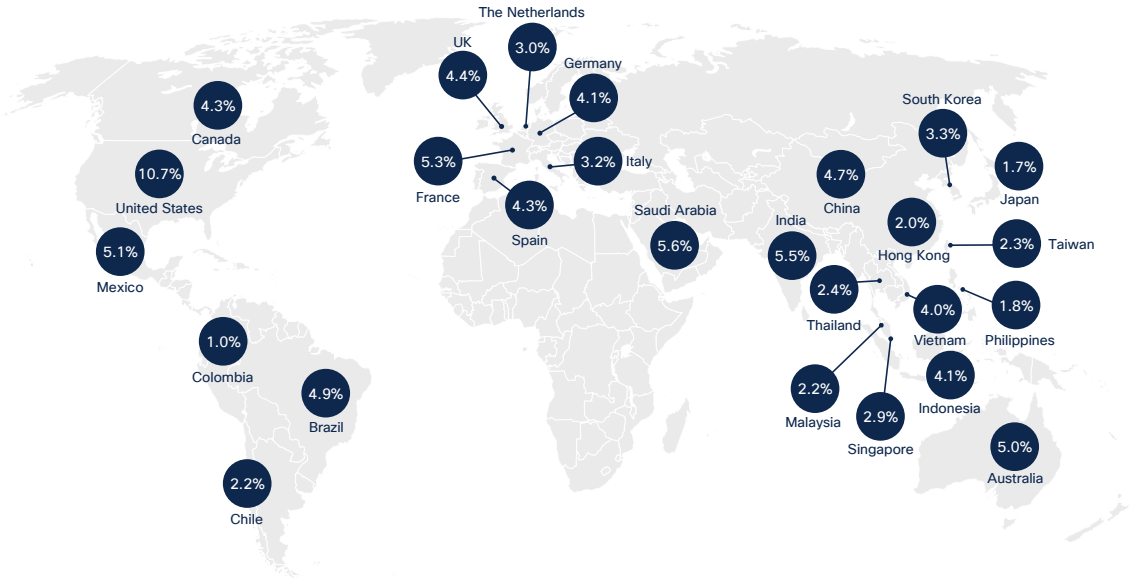
While organizations have always needed security and privacy to earn and build customer trust, today's business environment have made them mission-critical. As customers set their standard of trust, Cisco continues to listen, learn, and evolve to meet their needs. Our holistic approach to security and privacy – prioritizing trustworthiness, transparency, and accountability – sets us apart.

Learn how Cisco is prioritizing these recommendations in our operations, policies, processes, and in the solutions we deliver:

- Cisco Trust Center: www.cisco.com/go/trust
- Cisco 2022 Purpose Report – Power: http://cs.co/9008MhQMp
- Cisco ESG Reporting Hub – Integrity and Trust: http://cs.co/9004JSD1O

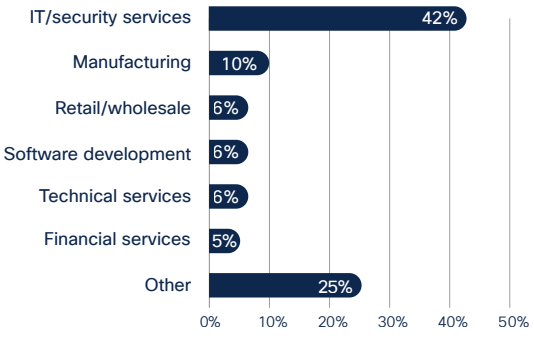
Cisco will continue to monitor these trends and issues and share our findings. For additional information about Cisco's privacy research, contact Robert Waitman, Cisco Director of Privacy Research and Economics at rwaitman@cisco.com.

# Appendix A: Demographics by geography

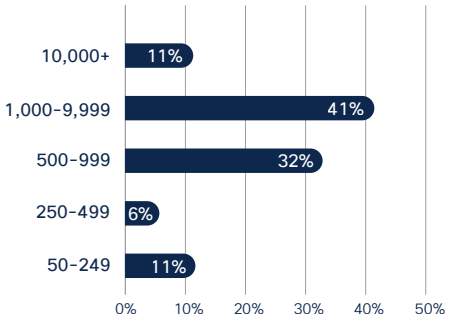



# Appendix B: Demographics by industry/size

## By industry




## By company size (# of employees)




Source: Cisco 2023 Data Privacy Benchmark Study

SECURE

## About the cybersecurity report series

Over the past decade, Cisco has published a wealth of security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their effects on organizations, as well as best practices to defend against the adverse impacts of data breaches.

In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven studies. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise from threat researchers and innovators in the security industry, the reports in each year's series include the Security Outcomes Report, Threat Report and Blogs, and Data Privacy Benchmark Study, and Consumer Privacy Survey, with others published throughout each year.


cisco SECURE