Privacy as an Enabler of Customer Trust

CISCO 2024 DATA PRIVACY BENCHMARK STUDY

Table of Contents

Introduction

Over the past few years, privacy has evolved from relative obscurity to being a business imperative, a regulatory mandate, and a customer requirement. During this time, Cisco's Privacy Research has explored the value of privacy investment and its economic benefits for organizations who have learned to better inventory, manage, and protect data. Customers who were once resigned to accept the lack of transparency from organizations now demand that their data be used only in transparent, legal, and appropriate ways, including in Artificial Intelligence (AI) applications. As such, privacy has become a critical element and enabler of customer trust.

Methodology

This report, Cisco's seventh annual review of privacy perspectives for organizations, explores current privacy trends, challenges, and opportunities. It draws upon data gathered in summer 2023 from an anonymous survey in which the respondents did not know who was conducting the study and respondents were similarly unknown to the researchers. The survey respondents included 2,600 security and privacy professionals in 12 countries (5 Europe, 4 Asia, and 3 Americas)[1]. They were asked about their organizations' privacy practices and spending, reactions to privacy legislation, AI, and data localization requirements. The findings from this research demonstrate the continuing importance of privacy to businesses and how they serve their customers.

[1] Australia, Brazil, China, France, Germany, India, Italy, Japan, Mexico, Spain, United Kingdom, and United States.

Key findings:

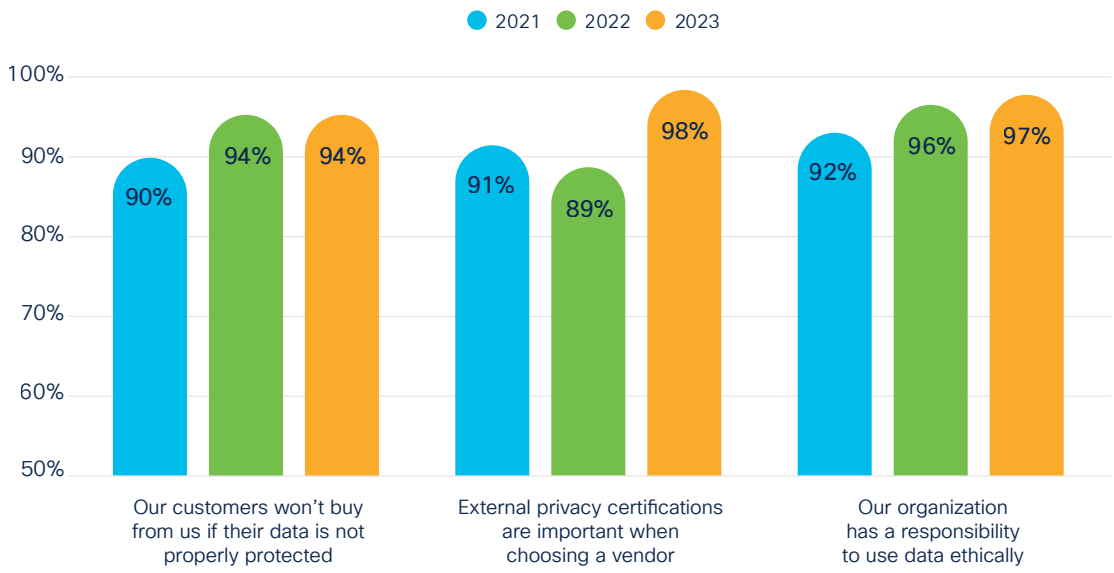
1. Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly.
2. Organizations strongly support privacy laws around the world, with 80% indicating legislation has had a positive impact on them.
3. The economics of privacy remain attractive, with 95% saying benefits exceed costs and the average organization realizing a 1.6x return on their privacy investment.
4. There has been relatively slow progress on building customer confidence with respect to AI; 91% of organizations still recognize they need to do more to reassure their customers.
5. Organizations are already getting significant value from generative AI applications, but they're also concerned about the risks to their intellectual property or that the data entered could be shared with competitors or the public.
6. Organizations believe that global providers, operating at scale, can better protect their data compared to local providers.

Results

1. Privacy as a critical enabler of customer trust

Customers increasingly want to buy from organizations they can trust with their data. Ninety-four percent of organizations in our survey said their customers would not buy from them if they did not adequately protect customer data. What's more, customers are looking for hard evidence that organizations can be trusted when it comes to privacy. Ninety-eight percent of respondents said that external privacy certifications, such as ISO 27701, Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules, and European Union (EU) Binding Corporate Rules, are important in their buying process. Organizations know these issues are important to customer trust, and nearly all organizations (97%) feel they have a responsibility to use data ethically. As indicated below, all of these percentages are at their highest levels from the surveys of the past three years. See Figure 1.

Figure 1. Privacy's importance to customer trust

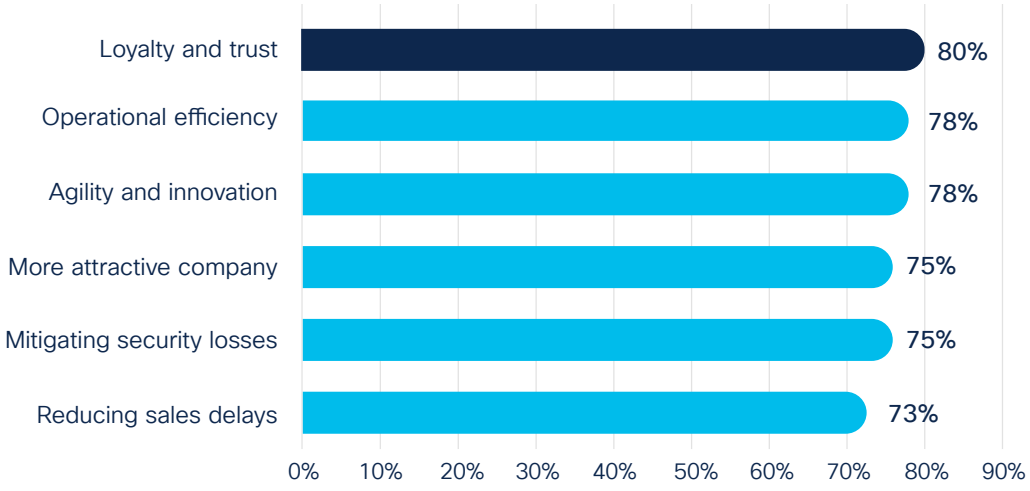


Source: Cisco 2024 Data Privacy Benchmark Study

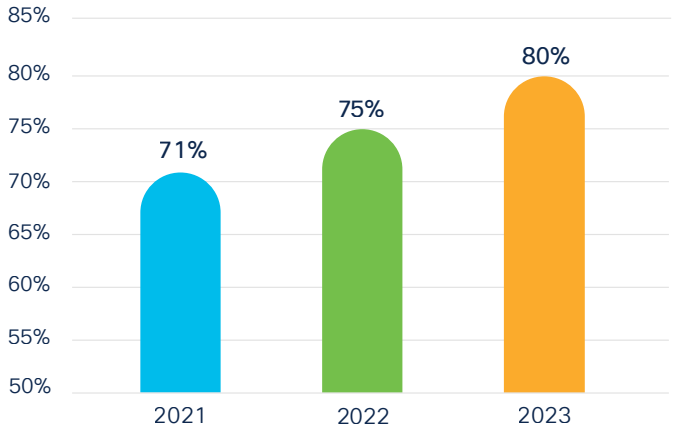
Organizations are also increasingly recognizing the connection between privacy investment and business benefits, especially in building brand trust and loyalty. For a number of years, we have asked respondents about the business benefits they are realizing from their privacy investment, including reducing sales delays, mitigating losses from data breaches, enabling innovation, achieving operational efficiency, building customer trust, and making their company generally more attractive. This year, over 70% indicated they were getting "significant" or "very significant" benefits from each of these six areas. Note that "Loyalty and Trust" received the highest percentage of responses (80%) and is up from 71% and 75% the past two years. See Figure 2.

Figure 2. Privacy investment's impact on loyalty and trust

Percent getting significant benefits from privacy investment, 2023



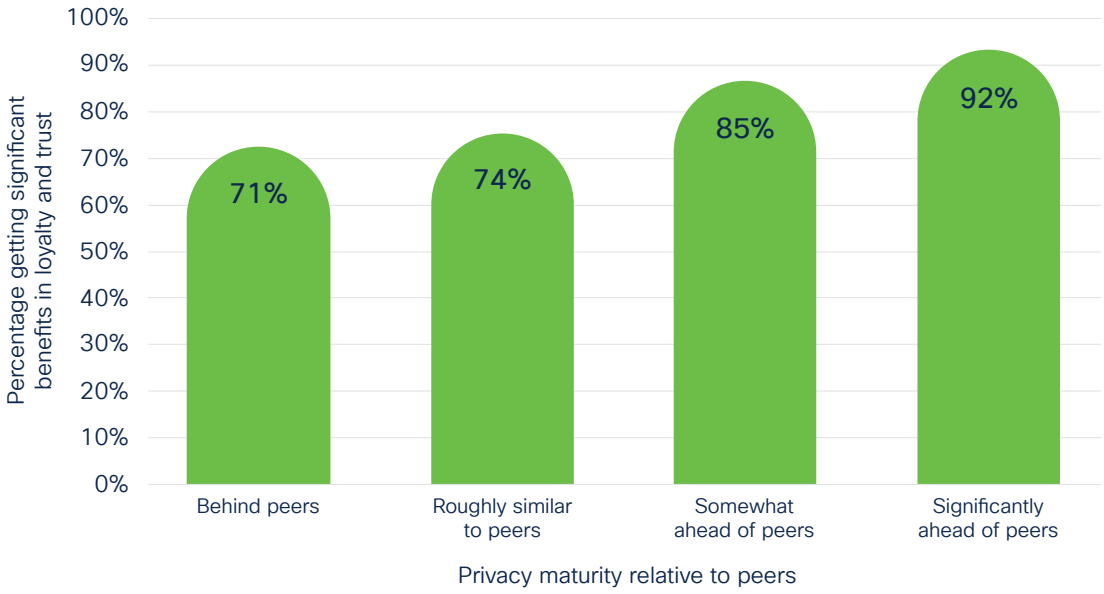
Percentage getting significant benefits in loyalty and trust from privacy investment, 2021–2023



Source: Cisco 2024 Data Privacy Benchmark Study

For privacy-mature organizations (i.e., those that consider their privacy programs to be ahead of their peers), the percentage getting benefits from "Loyalty and Trust" is even higher. Ninety-two percent of the most privacy-mature organizations indicated they are getting significant benefits in this area, compared with 71% of those that are the least mature. See Figure 3.

Figure 3. Privacy maturity's correlation with loyalty and trust



Source: Cisco 2024 Data Privacy Benchmark Study

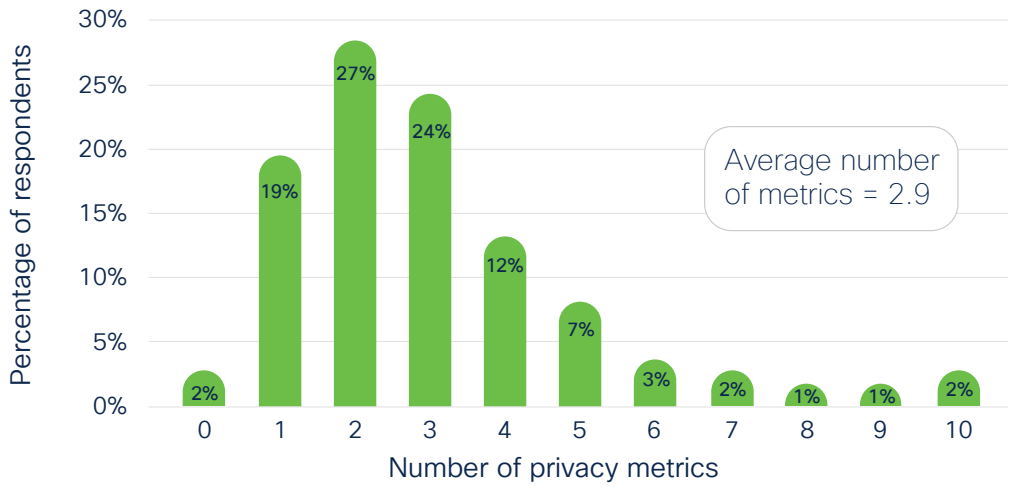
"Privacy has become inextricably tied to customer trust and loyalty."

Harvey Jang, Vice President, Deputy General Counsel and Chief Privacy Officer, Cisco

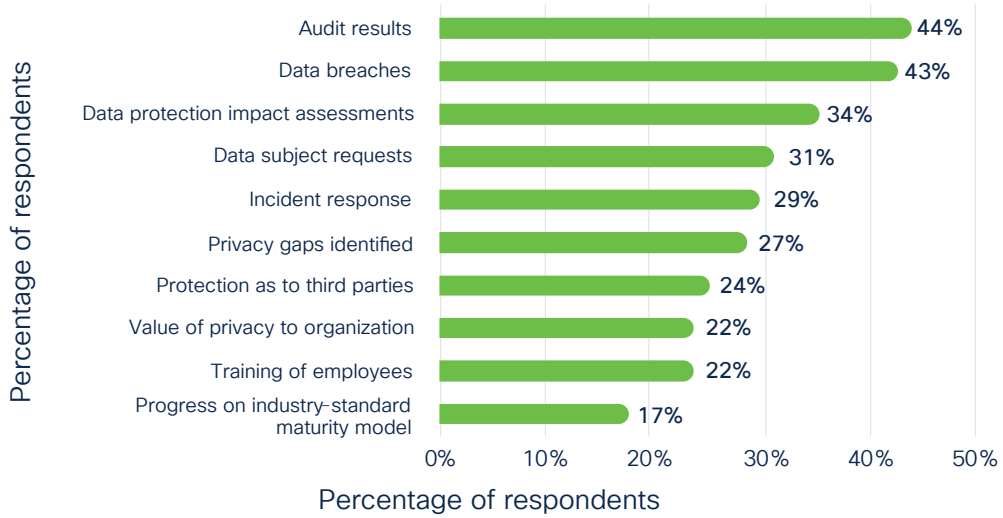
Translating privacy objectives to organizational activities can be difficult. One way for organizations to implement them is through the use of privacy metrics, especially when those metrics are reported to executive management and the Board of Directors. Among this year's respondents, nearly all (98%) are reporting one or more privacy metrics to the Board, and over half are reporting three or more. Many of the top privacy metrics tie very closely to issues of customer trust, including audit results (44%), data breaches (43%), data subject requests (31%), and incident response (29%). See Figure 4.

Figure 4. Number and type of privacy metrics reported to the Board

Number of privacy metrics



Types of privacy metrics



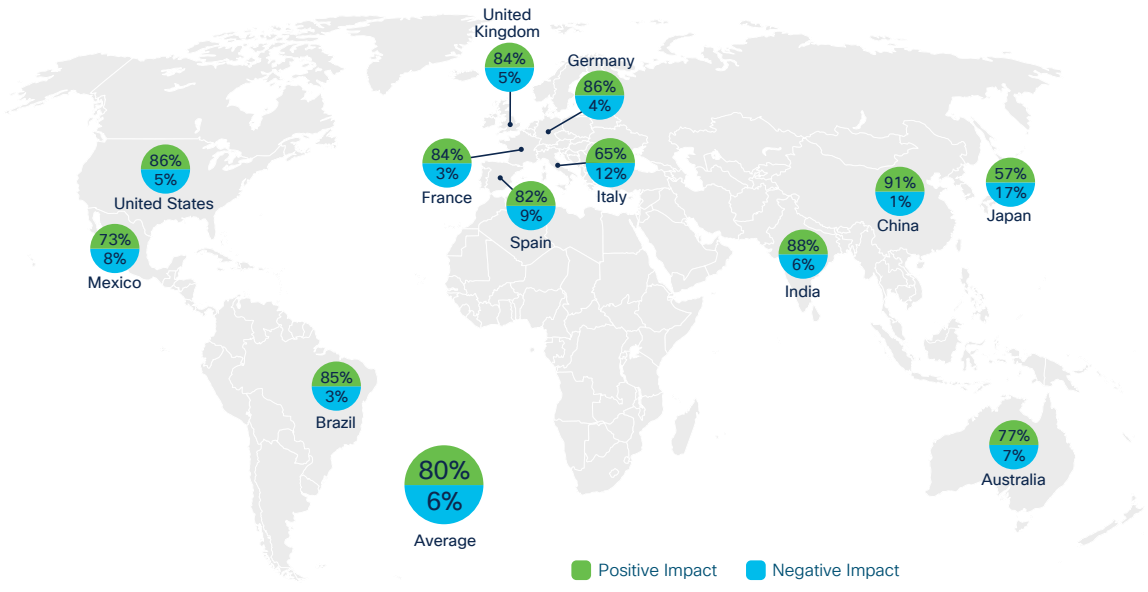
Source: Cisco 2024 Data Privacy Benchmark Study

2. Strong support for privacy laws globally

While governments, organizations, and individuals all have roles to play in protecting personal data, 50% of the Cisco 2023 Consumer Privacy Survey respondents indicated they wanted governments to take the lead. Sixty-six percent of respondents also said privacy laws had a positive impact, compared to only 4% who said they have had a negative impact.

For this year's Benchmark Study, we asked organizations a similar question, and they were even more supportive of privacy laws than the consumers. Eighty percent of all corporate respondents said privacy laws have had a positive impact on their organizations, with 14% neutral, and only 6% indicating the laws have had a negative impact. This is despite the significant effort and cost involved in privacy compliance, for example, cataloging data, implementing controls, and responding to user requests. Note that this sentiment was quite consistent across regions, with 78% in Asia, 80% in Europe, and 83% in the Americas indicating the privacy laws have been positive. By country, the highest average percentages were in China (91%), India (88%), Germany (86%), and the U.S. (86%). Even though the U.S. does not yet have a federal omnibus privacy law, U.S. companies are still subject to sectoral laws, state and local laws, and the laws in the countries in which they operate. See Figure 5.

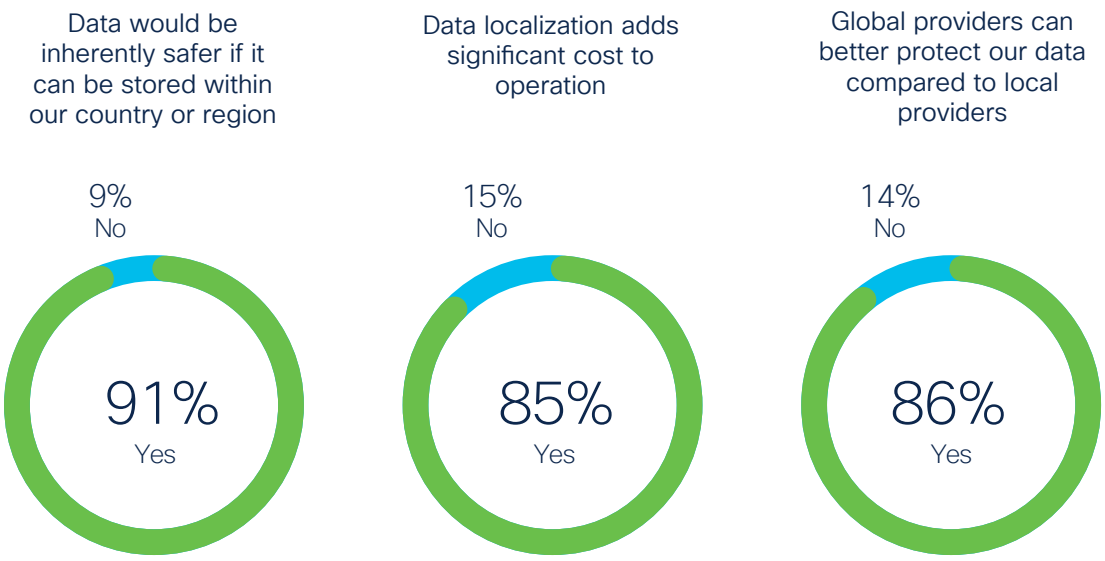
Figure 5. Impact of privacy laws on organizations



Source: Cisco 2024 Data Privacy Benchmark Study

Many governments and organizations are putting in place data localization requirements to ensure that certain data is kept within a specific country or region. Among organizations, most (91%) believe that their data would be inherently safer if it is only stored within their country or region. But almost the same number (86%) also said that a global provider, operating at scale, can better protect their data compared to a local provider. These responses indicate that organizations would ideally like to keep their data local, but they still prefer and trust a global provider over a local provider. See Figure 6.

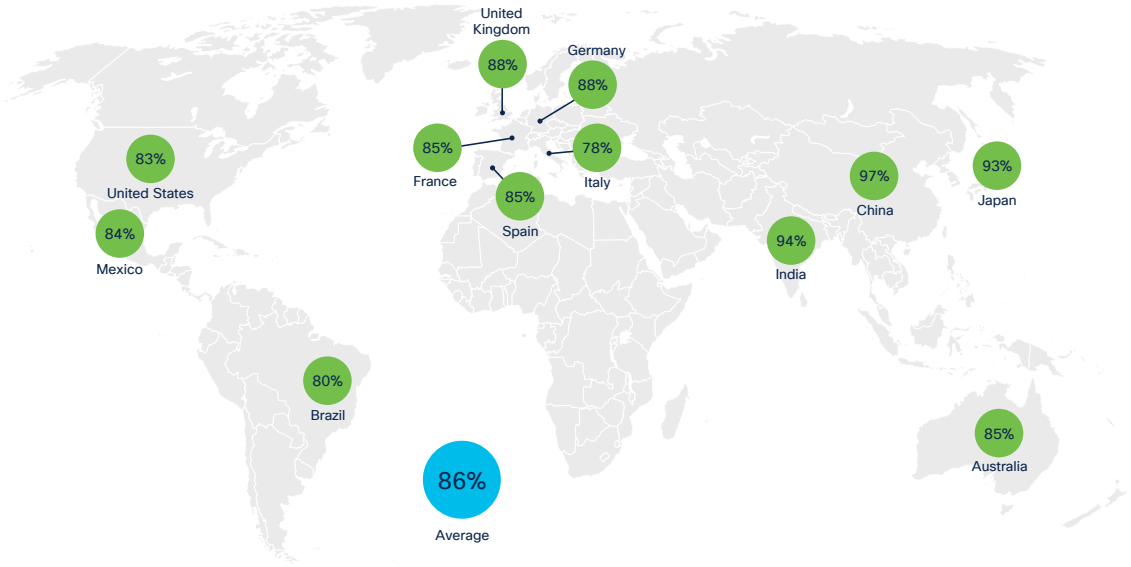
Figure 6. Data localization



Source: Cisco 2024 Data Privacy Benchmark Study

Interestingly, this preference for global providers held true by geography. The percentage saying "a global provider can better protect data compared to a local provider" was 78% or higher in all 12 geographies of survey respondents. See Figure 7.

Figure 7. Percentage agreeing that a global provider can protect data better than a local provider, by country

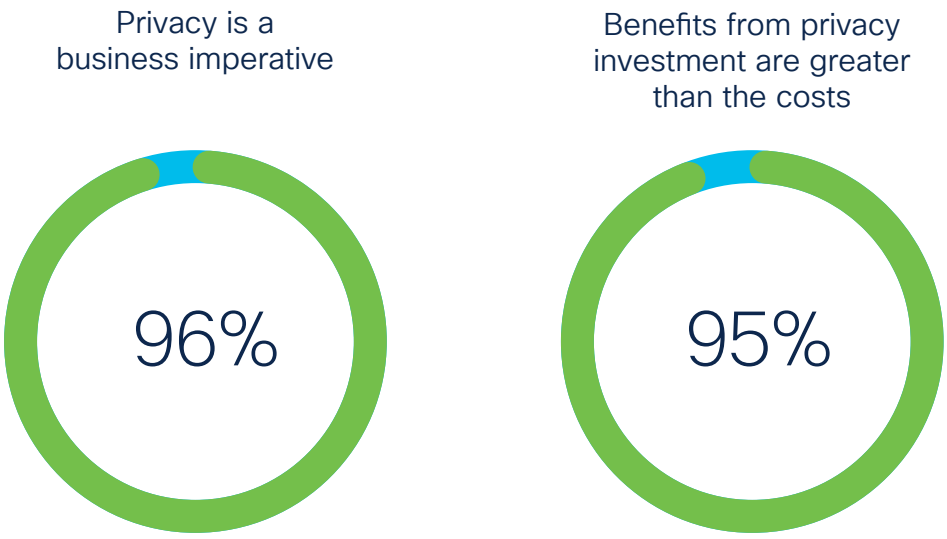


Source: Cisco 2024 Data Privacy Benchmark Study

3. Privacy economics remain attractive

Privacy continued to provide attractive economic returns for organizations around the world in 2023. Ninety-six percent of respondents agreed that privacy is a business imperative, not just a compliance burden, and 95% indicated that privacy's benefits are greater than its costs. See Figure 8.

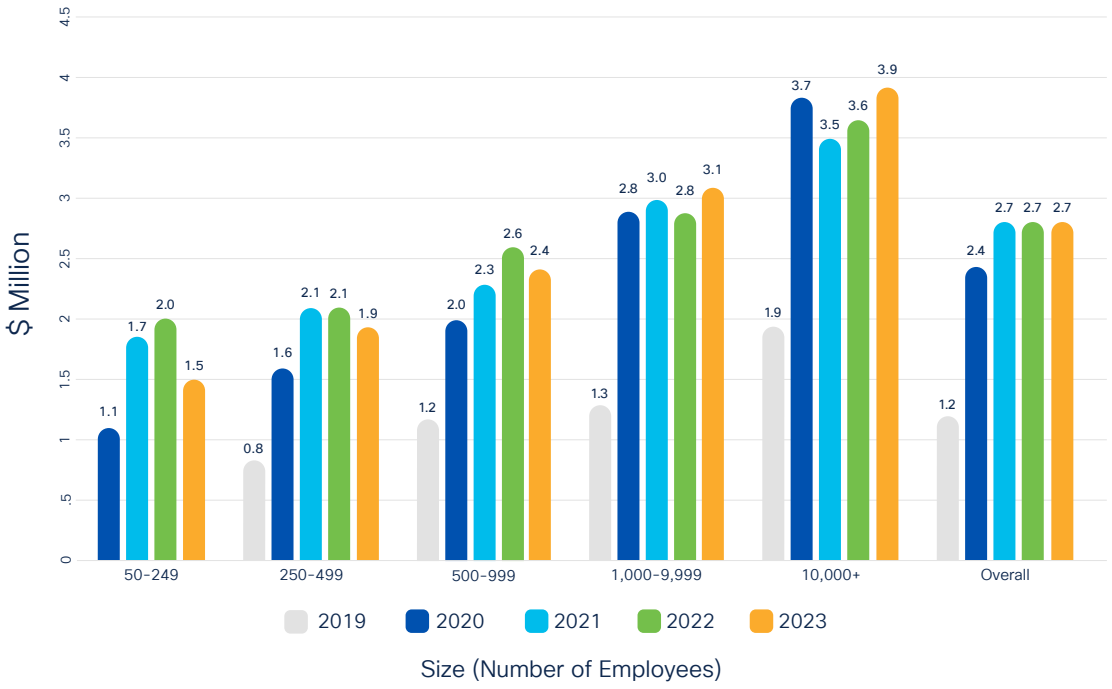
Figure 8. Business benefits of privacy investment



Source: Cisco 2024 Data Privacy Benchmark Study

In our research, we've been tracking privacy spending, estimated financial benefits, and return on investment for organizations over the past five years. During this time, spending has more than doubled, benefits have trended up, and returns have remained strong. For 2023, average spending overall was similar to 2021 and 2022 at $2.7 million. Average spending rose at the largest organizations (10,000+ employees) to $3.9 million from $3.6 million last year. At large organizations (1,000 to 9,999 employees), spending rose to $3.1 million from $2.8 million. Smaller organizations saw lower spending, including those with 50-249 employees, decreasing from $2.0 million to $1.5 million this year. See Figure 9.

Figure 9. Privacy spending, 2019-2023



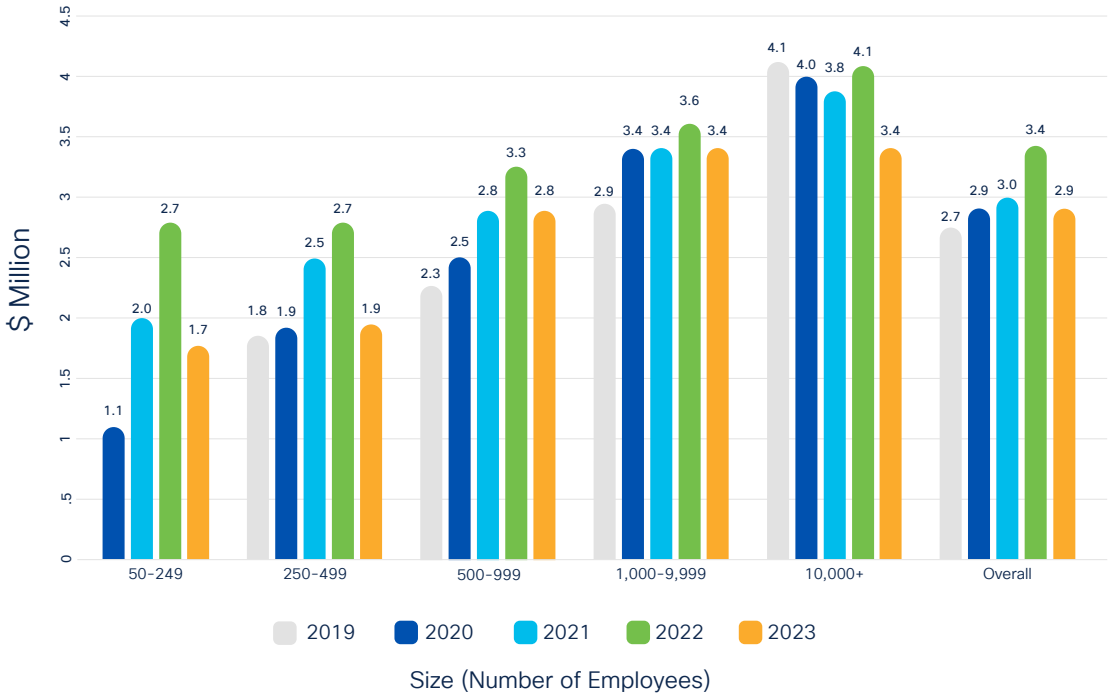
Note: The 50-249 employee category was initiated in 2020.

Note: For consistency, the 2023 overall spending ($2.7 million) is based on historical mix of company size

Source: Cisco 2024 Data Privacy Benchmark Study

Estimated financial benefits remain higher than when we started tracking it four years ago, with an average estimated benefit in 2023 of $2.9 million. This is lower than last year's peak of $3.4 million, with similar reductions in large and small organizations. The causes of this are unclear, since most of the other financial-oriented metrics, such as respondents saying privacy benefits exceed costs, respondents getting significant financial benefits from privacy investment, and ROI (return on investment) calculations, all point to more positive economics. We will continue to track this in future research to identify if this is an aberration or a longer-term trend. See Figure 10.

Figure 10. Estimated financial benefits, 2019-2023



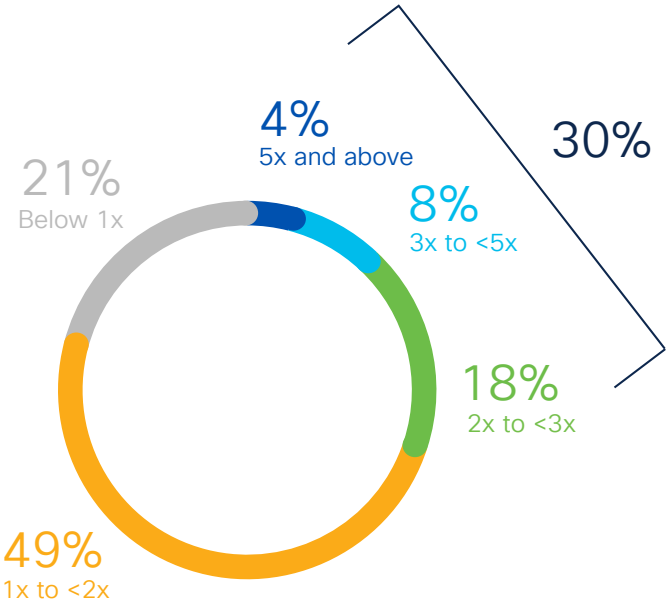
Note: The 50-249 employee category was initiated in 2020.

Note: For consistency, the 2023 overall spending ($2.9 million) is based on historical mix of company size

Source: Cisco 2024 Data Privacy Benchmark Study

Comparing spending and benefits together, privacy remains a very attractive financial investment for most organizations. The average organization reports getting privacy benefits of 1.6 times their investment. In addition, 30% of organizations estimate returns at least two times with some (12%) realizing returns upwards of three times their investment. See Figure 11.

Figure 11. Estimated ROI ranges for respondents, 2023

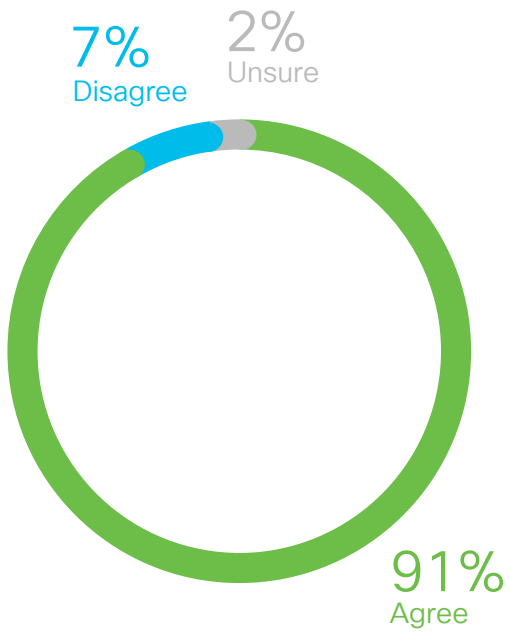


Source: Cisco 2024 Data Privacy Benchmark Study

4. Slow progress on transparency and AI readiness

According to the Cisco 2023 Consumer Privacy Survey, 62% of consumers are concerned about how organizations apply and use AI, and 60% already have lost trust in organizations over their AI practices. We asked organizations about this in last year's Data Privacy Benchmark Study, and 92% of respondents said their organizations needed to do more to reassure customers that their data was only being used for intended and legitimate purposes when it comes to AI. When we asked the same question in this year's survey, the percentage had only dropped to 91%, indicating not much progress has been made during the past year. See Figure 12.

Figure 12. Organizations who say they need to do more to reassure customers about their data use with AI

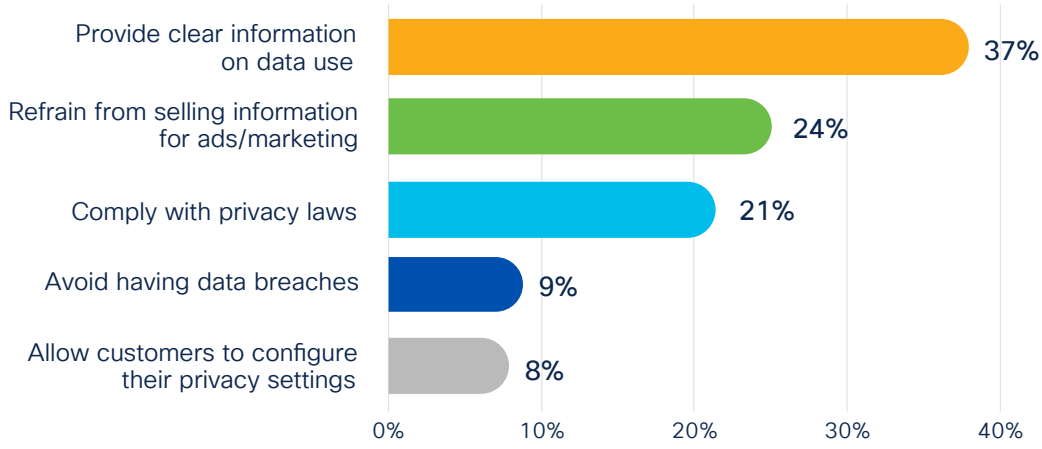


Source: Cisco 2024 Data Privacy Benchmark Study

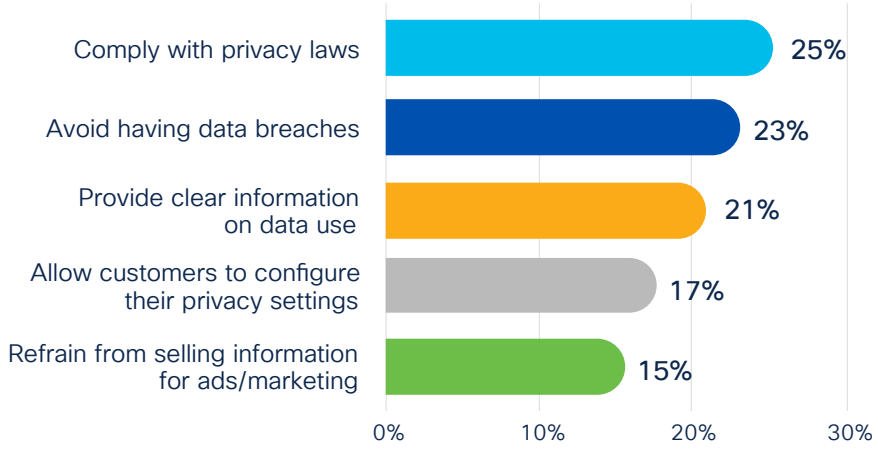
One challenge facing organizations when it comes to building trust with data is that their priorities may differ somewhat from their customers. Consumers identified their top priorities as getting clear information on exactly how their data is being used (37%), and not having their data sold for marketing purposes (24%). When asked the same question, organizations identified their top priorities as complying with privacy laws (25%) and avoiding data breaches (23%). While these are all important objectives, it does suggest additional attention on transparency would be helpful to customers – especially with AI applications where it may be difficult to understand how the AI algorithms make their decisions. See Figure 13.

Figure 13. What organizations can do to build and maintain trust when it comes to customer data

Consumer view



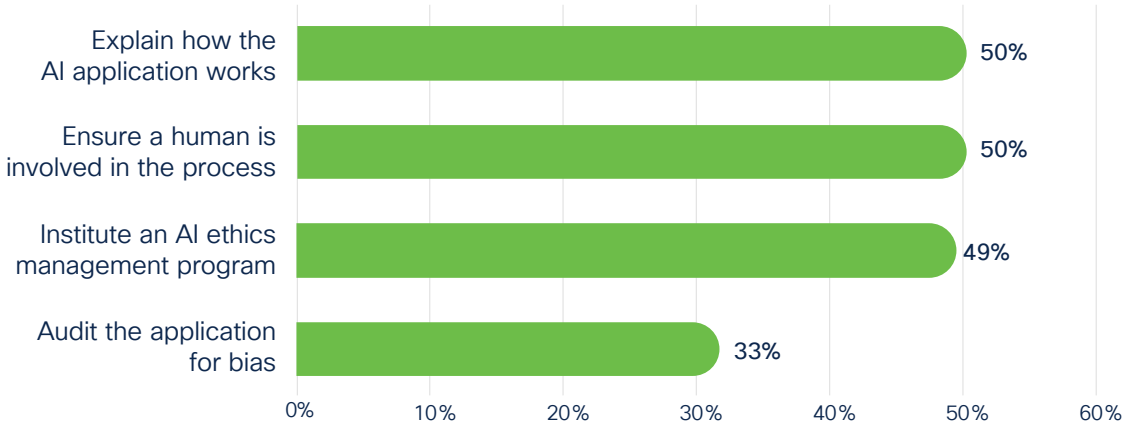
Organizational view



Source: Cisco 2024 Data Privacy Benchmark Study

In the Cisco 2023 Consumer Privacy Survey, we asked respondents what actions organizations could take to reassure their customers about data use and AI. Over 70% of them said that auditing the AI applications for bias, improving transparency, ensuring a human was involved in the process, and instituting an AI ethics management program would make them more comfortable. When we asked the same question to organizations in this privacy benchmark, their top responses were explaining how the AI application works (50%), ensuring a human is involved in the process (50%), instituting an AI ethics management program (49%), and auditing the application for bias (33%). These differences in responses between the two survey audiences suggest there is more to be done in this space. See Figure 14.

Figure 14. Steps taken by organizations regarding their use of AI



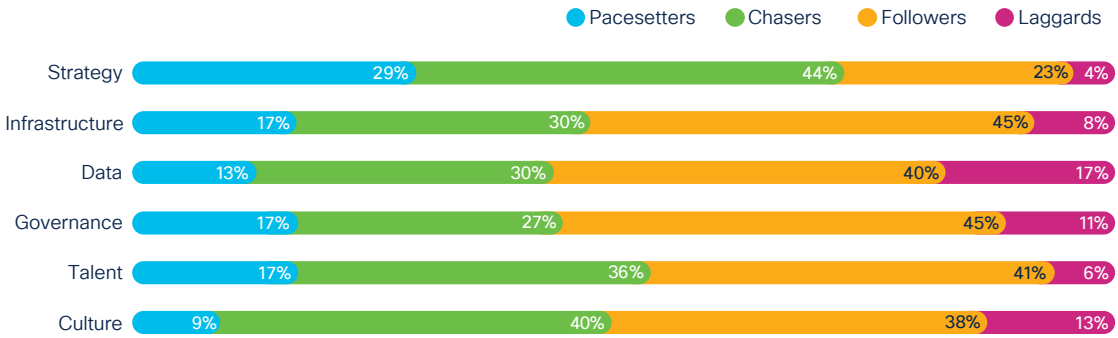
Source: Cisco 2024 Data Privacy Benchmark Study

"The risks of AI are real, but they are manageable when thoughtful governance practices are in place as enablers, not obstacles, to responsible innovation."

Dev Stahlkopf
Executive Vice President and Chief Legal Officer, Cisco

Of course, even with the best of intentions, it often takes time to put in place the necessary elements for AI applications. The Cisco AI Readiness Index, published in fall 2023, evaluated more than 8,000 organizations and assessed their readiness across six domains: strategy, infrastructure, data, governance, talent, and culture. The analysis showed that only 14% of organizations worldwide believed they were fully ready to integrate AI into their businesses. Organizations interested in benchmarking themselves should review that publication and its associated online materials. See Figure 15.

Figure 15. Cisco AI Readiness Index

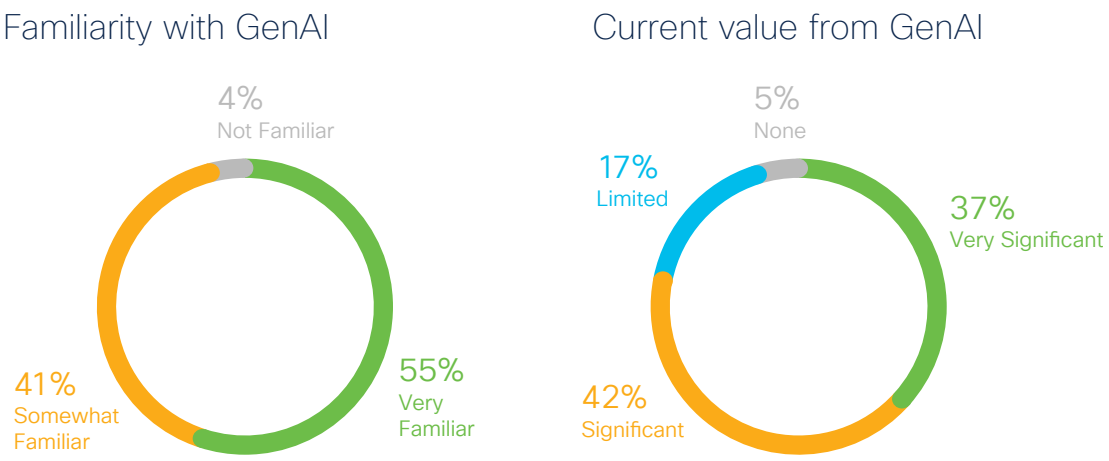


Source: Cisco AI Readiness Index

5. Data concerns with GenAI

Generative AI (GenAI) applications have the power to use AI and machine learning to create new content based on user prompts, including text, sound, music, images, video, and code. Like many new technologies, AI brings opportunities as well as challenges for how best to manage and control it. While the majority (52%) of consumers in the Cisco 2023 Consumer Privacy Survey indicated they were unfamiliar with GenAI, most organizations have now become very familiar (55%) or somewhat familiar (41%) with it. Most are already deploying it in their organizations, as 79% of respondents said they are getting significant or very significant value from GenAI today. See Figure 16.

Figure 16. Familiarity and value from GenAI

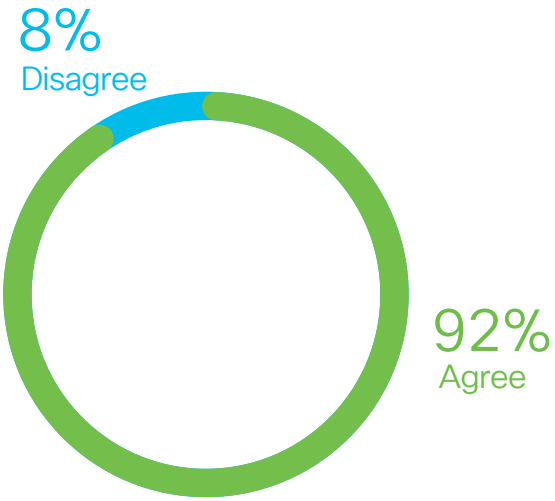


Source: Cisco 2024 Data Privacy Benchmark Study

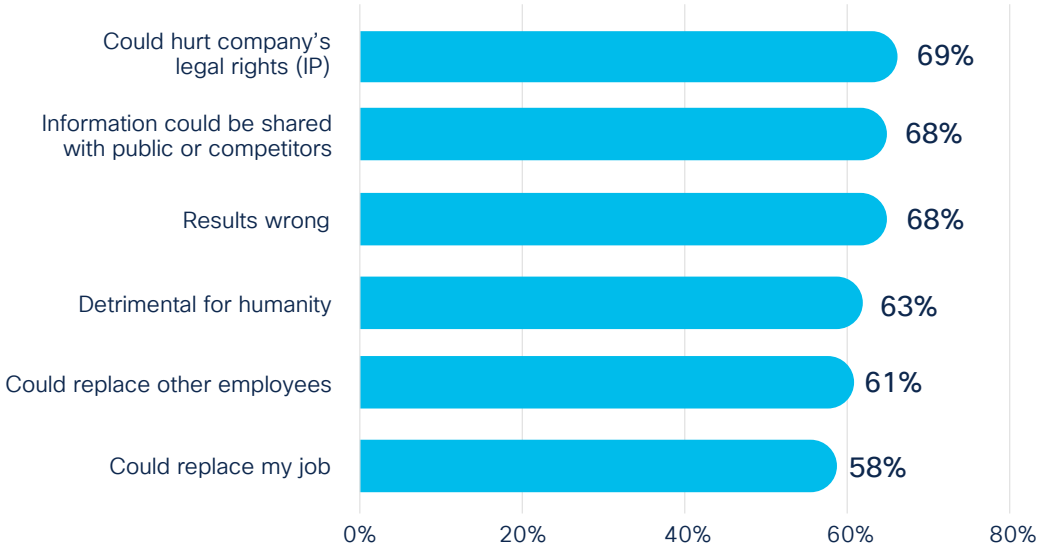
Generative AI puts AI capabilities in the hands of many more users, and 92% of organizations said they see it as a fundamentally different technology with novel challenges and concerns requiring new techniques to manage data and risk. Among the top concerns cited were that the use of GenAI could hurt the organization's legal and intellectual property rights (69%), the information entered could be shared publicly or with competitors (68%), and that the information it returns to the user could be wrong (68%). See Figure 17.

Figure 17. Concerns with GenAI

Organizations seeing GenAI as fundamentally different, requiring new techniques to manage data and risks



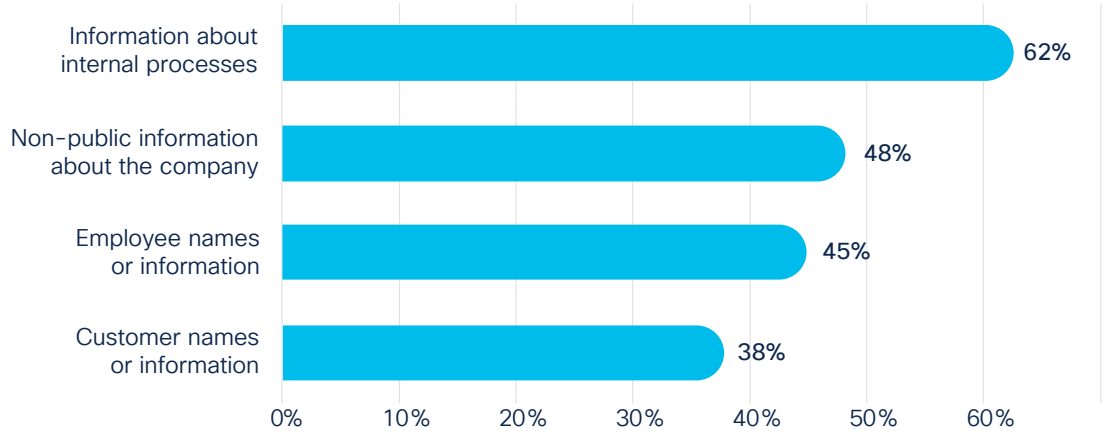
User concerns with GenAI



Source: Cisco 2024 Data Privacy Benchmark Study

Nonetheless, many GenAI users are entering information that could be problematic if it were to be shared externally. Sixty-two percent of respondents said they have entered information about internal processes, 48% have entered non-public information about the company, and 45% have entered employee names or information. See Figure 18.

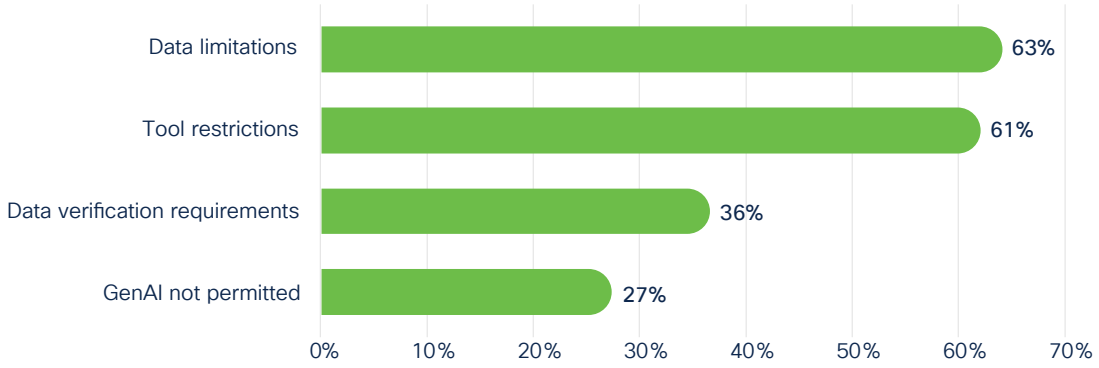
Figure 18. Types of information entered into GenAI applications



Source: Cisco 2024 Data Privacy Benchmark Study

Most organizations have become aware of these risks, with many working to put in place controls that would limit their exposure. Sixty-three percent have established limitations on what data can be entered, 61% have limits on which GenAI tools can be used by employees, and 27% have banned GenAI applications altogether, at least for the time being. Almost all organizations reported having at least one of these controls in place. As this technology is still evolving rapidly, we expect the type and nature of the controls to also evolve as organizations seek to harness the power of GenAI without risking unauthorized sharing of confidential or personal information. We will continue to follow this matter in future research. See Figure 19.

Figure 19. GenAI controls



Source: Cisco 2024 Data Privacy Benchmark Study

Conclusion and recommendations for organizations

This research highlights many of the essential aspects of privacy for organizations today. Privacy has become a critical element and enabler for building and maintaining customer trust. It also represents an attractive economic investment and provides important ground rules as organizations prepare for expanded use of AI and GenAI. Governments, organizations, and individuals must continue to play their respective roles, ensuring that personal data is protected and used only when legal and appropriate. The findings in this research point to these specific recommendations for organizations:

1. Provide greater transparency in how your organization applies, manages, and uses personal data as this will go a long way towards building and maintaining customer trust.
2. Establish protections, such as AI ethics management programs, involving humans in the process, and working to remove any biases in the algorithms when using AI for automated decision-making involving customer data.
3. Apply appropriate control mechanisms and educate employees regarding the risks associated with GenAI applications.
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 when compared to global providers operating at scale.
5. Continue to invest in privacy to realize the significant business and economic benefits for your organization.

Meeting our customers' standard of trust

Organizations have always required security to protect assets, help manage risk, and build customer confidence and loyalty. Today's complex business environment, novel technological innovation, and customer expectations have privacy emerging as another critical element of customer trust. As customers set their standards of trust, Cisco continues to listen, learn, and evolve to meet those standards, prioritizing trustworthiness, transparency, and accountability throughout our holistic approach.

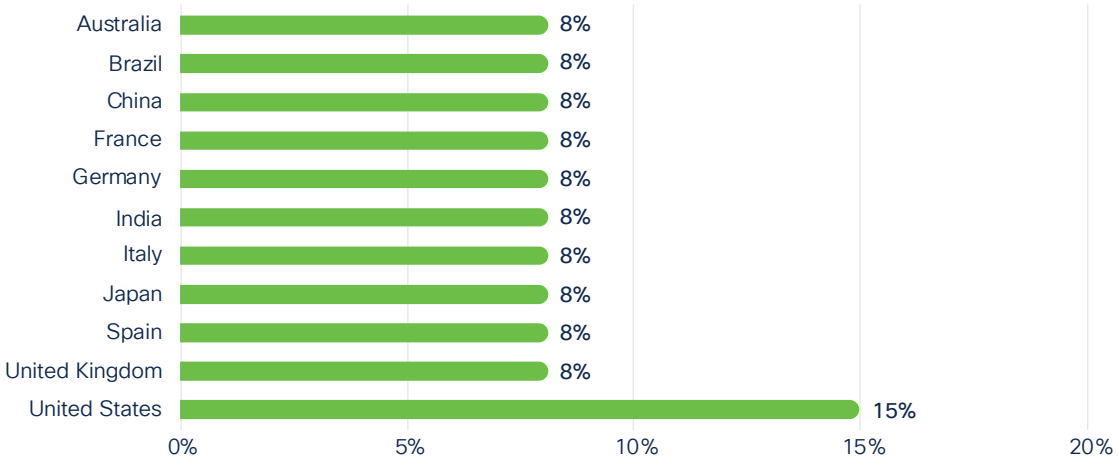
In addition to the annual Privacy Benchmark and Consumer reports, Cisco also publishes Privacy Data Sheets and Privacy Data Maps for its major products and services, enabling anyone interested to understand what personal data is used, who has access to it, and how long it is retained. Our Responsible AI Principles and Framework show how these principles and practices form our broad AI governance framework. And the Cisco Purpose Report and ESG Reporting Hub offer relevant resources related to how we prioritize trustworthiness, transparency, and accountability in our environmental, social, and governance (ESG) initiatives.

All of this and more are available on the Cisco Trust Center.

For additional information about our privacy research, contact Robert Waitman, Cisco Director of Privacy, at rwaitman@cisco.com.

Appendix

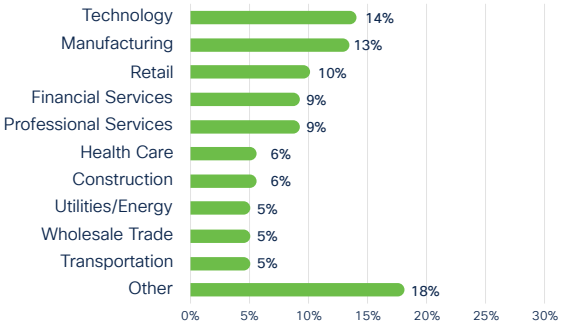
Appendix A. Demographics of survey respondents, by geography



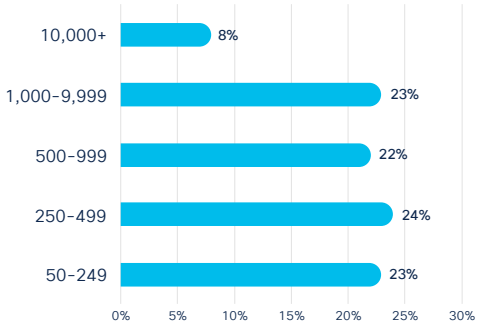
Source: Cisco 2024 Data Privacy Benchmark Study

Appendix B. Demographics of survey respondents, by industry and size

By industry



By company size (# employees)



Source: Cisco 2024 Data Privacy Benchmark Study

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 have 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 Data Privacy Benchmark Study, the Security Outcomes Report, Threat Insights, and Prioritization to Prediction, with others published throughout the year. For more information, and to access all the reports, visit www.cisco.com/go/securityreports.