The Privacy Advantage: Building Trust in a Digital World

CISCO 2025 DATA PRIVACY BENCHMARK STUDY

Table of Contents

Introduction

Over the past decade, organizations have steadily increased their privacy resources and investments. While initially driven by the necessity of compliance, these efforts have revealed the broader value of privacy as a cornerstone for earning, building, and maintaining customer trust. With the rise of Generative Artificial Intelligence (GenAI), organizations face the next chapter in their privacy journey. The 2025 Data Privacy Benchmark Study explores key themes shaping the industry today: an emphasis on data localization alongside a preference for global providers, the trust-building power of privacy regulations, and the intersection of privacy and AI governance.

Methodology

This report draws upon data gathered in fall 2024 from an anonymous survey of security and privacy professionals in which the respondents did not know who was conducting the study and respondents were similarly unknown to the researchers. The survey included 2600+ respondents 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:

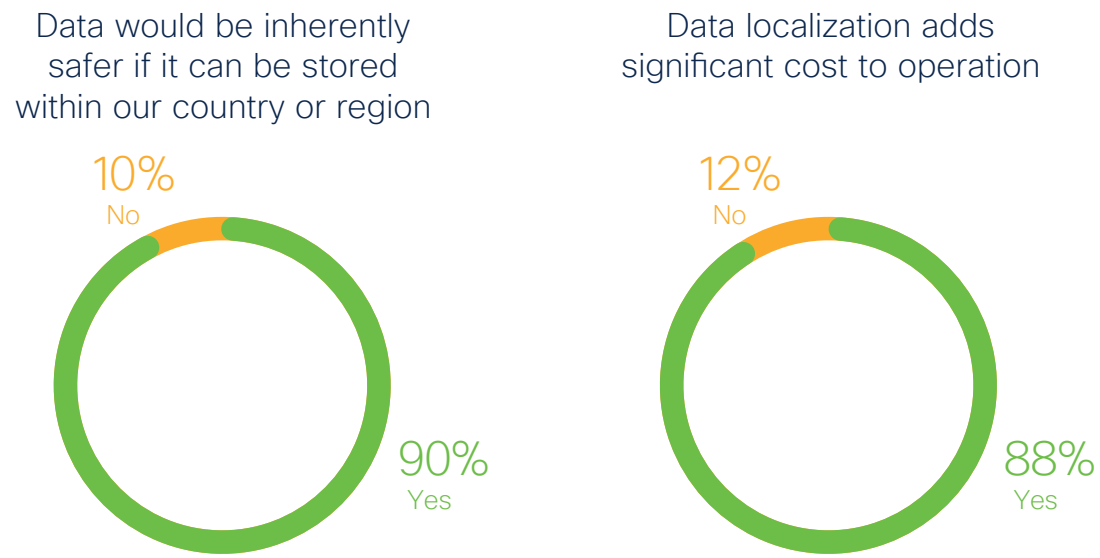
1. Amid global focus on data and AI, 90% of respondents believe storing data locally is inherently safer. And yet, 91% believe global providers are better at protecting data compared to local providers.
2. Support for privacy laws continues to grow with 86% (up 6% year over year) of organizations indicating legislation has had a positive impact.
3. Organizations continue to see the value generated from privacy investments. Funding remained steady year over year with 96% of respondents noting that the benefits outweigh the cost.
4. Familiarity with and value from AI are increasing, but concerns with potential risks remain. Interestingly, concerns around legal risks have decreased as respondents grow more familiar with the novel technology and have implemented AI governance frameworks.
5. Realizing the potential of AI, organizations expect AI focus and budgets to grow. This growth intersects with the ongoing needs of maintaining robust data privacy and cybersecurity programs.

Results

1. Perceptions around data safety and security drive localization

For decades, the digital economy has played a key role in driving economic growth with businesses across various sizes and sectors relying on data movement around the world. And yet, in recent years, there has been an increased focus on data localization in many geographies. Similar to the Cisco 2024 Data Privacy Benchmark Study, the vast majority of respondents (90%) indicated a belief that data would be safer when stored locally within—their own country's borders. When asked if localizing their data comes with significant cost—regardless of provider—88% said yes, compared with 85% in 2023. These two responses together indicate a willingness to spend more to keep data local. See Figure 1.

Figure 1. Data localization



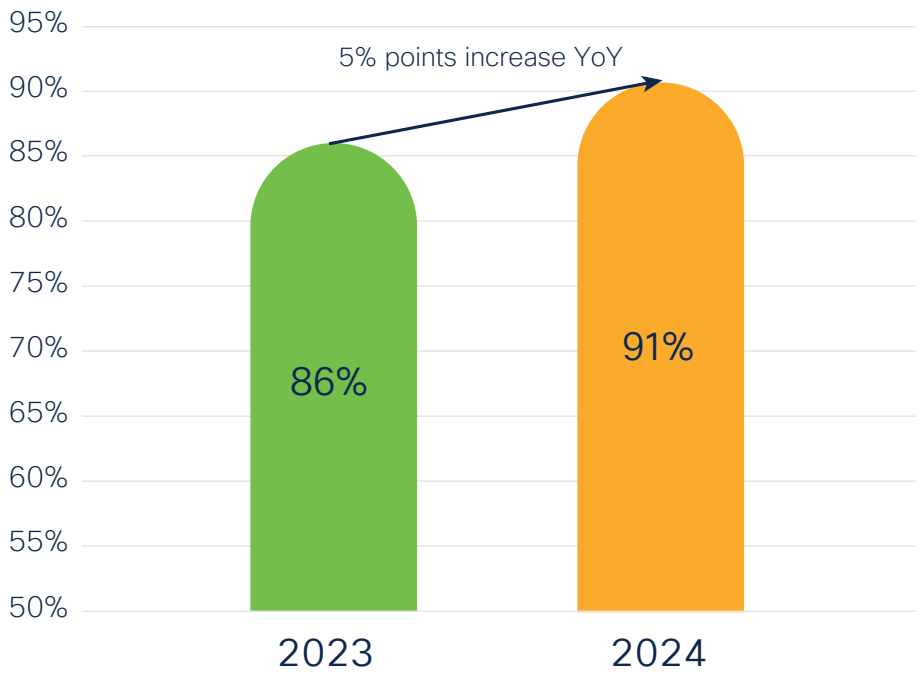
Source: Cisco 2025 Data Privacy Benchmark Study

"Privacy is core to trust and a competitive differentiator in today's digital economy."

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

A slightly higher percentage of respondents (91%) also believe that global providers would better protect their data compared to a local provider serving a specific country or region. Notably, this percentage is up five points from last year. This increase may reflect the growing trend of multinational providers introducing in-region data storage capabilities, allowing respondents to reap the benefits of both global scale and expertise while meeting specific data residency preferences and requirements. And, while it might initially appear paradoxical to see strong, equally weighted preferences for both data localization and global providers, the results are logical in today's landscape. As data becomes an increasingly valuable asset, both companies and consumers expect—and demand—robust protective measures. See Figure 2.

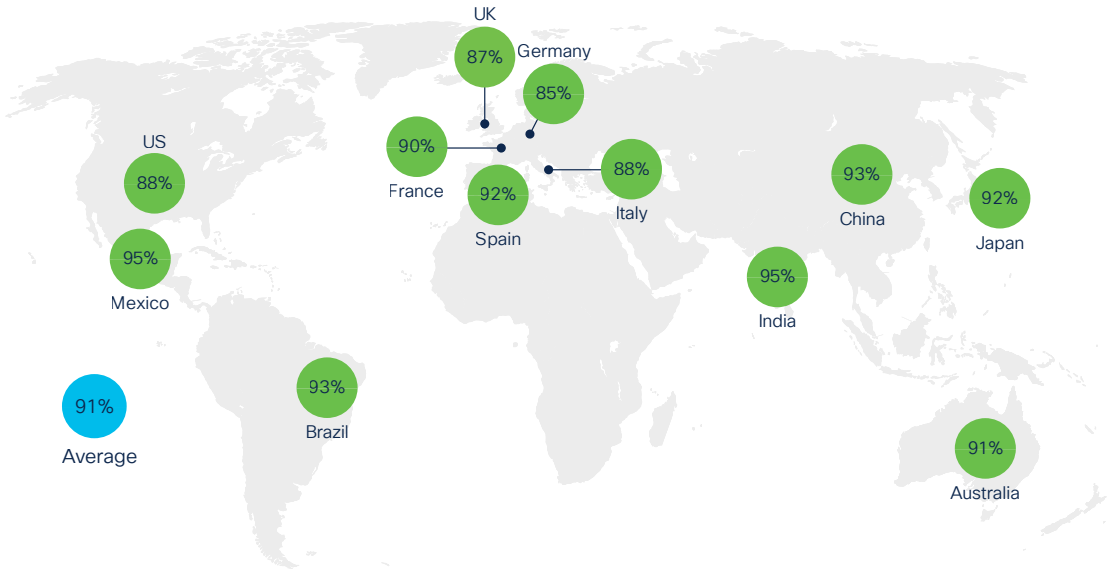
Figure 2. Global providers can protect data better than local providers



Source: Cisco 2025 Data Privacy Benchmark Study

Additionally, with the varying approaches to data localization across countries, one might expect preference for global data providers to differ based on local regulation. But preference for global providers over local ones remains relatively consistent across the surveyed regions. See Figure 3.

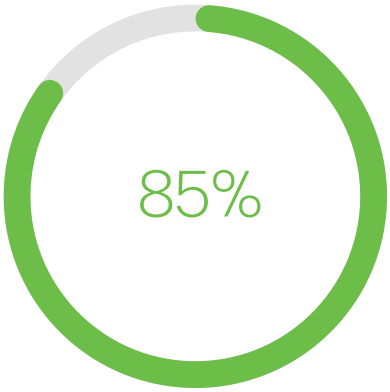
Figure 3. Agreement that a global provider can protect data better than a local provider, by country



Source: Cisco 2025 Data Privacy Benchmark Study

While respondents expressed a strong belief that data stored locally is safer, navigating differing regulatory regimes raises complexities for global businesses. According to the Organisation for Economic Co-operation and Development (OECD), more than 100 data localization requirements exist across 40 countries.[2] Amid this rise in localization, some governments are working to enable interoperable data flows through trade and digital agreements that are based on a consistent foundation of data protection. The G20's Data Free Flow with Trust (DFFT) initiative (supported by the OECD), the Global Cross-Border Privacy Rules Forum, EU-UK Trade and Cooperation Agreement, and others, aim to make national data governance systems interoperable and prohibit strict data and infrastructure localization. When respondents were asked if Data Free Flow with Trust could boost economic growth, 85% agreed, highlighting the interest and need for organizations to find safe ways to continue enabling cross-border data flows that are critical for today's global, digital economy. See Figure 4.

Figure 4. "Data Free Flow with Trust" can boost economic growth



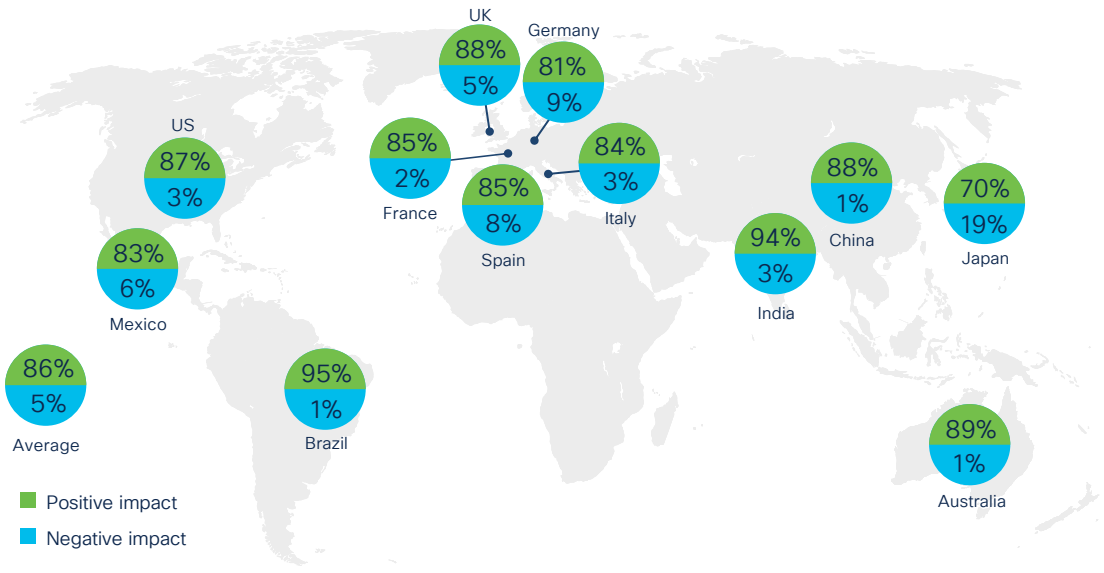
Source: Cisco 2025 Data Privacy Benchmark Study

[2] Del Giovane, C., J. Ferencz and J. López González (2023), "The Nature, Evolution and Potential Implications of Data Localisation Measures", *OECD Trade Policy Papers*, No. 278, OECD Publishing, Paris, https://doi.org/10.1787/179f718a-en.

2. Regulation continues to be a trust driver

While compliance with privacy laws does require investment–a theme explored later in this report–these regulations are widely seen as beneficial, notably for providing a structured framework that boosts trust and credibility with customers. This positive view is supported by data, showing that 86% of respondents reported a positive impact from privacy laws on their organization, up from 80% in the Cisco 2024 Data Privacy Benchmark Study. See Figure 5.

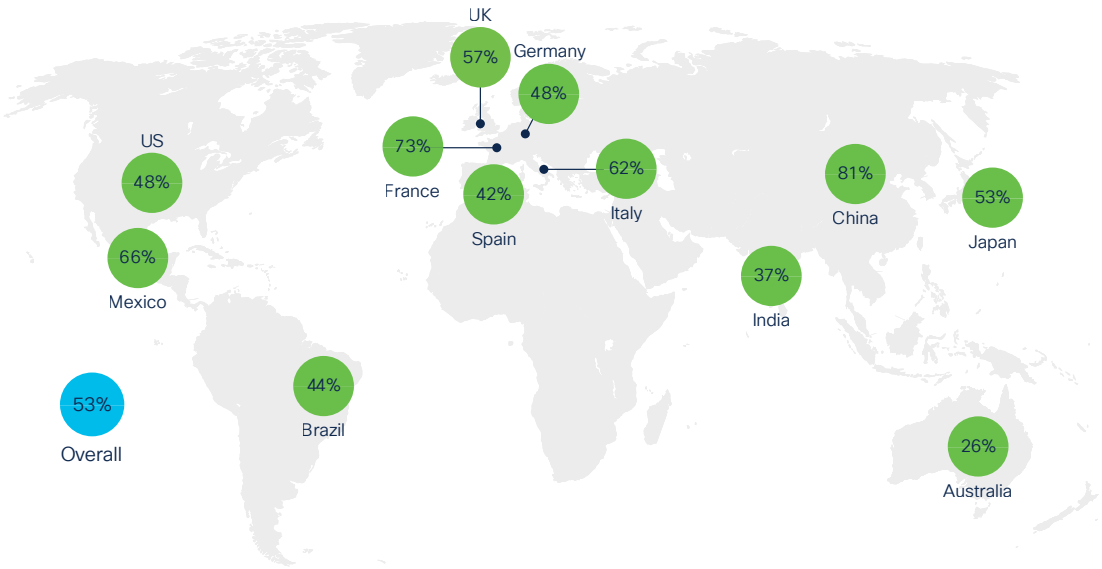
Figure 5. Impact of privacy laws on organizations



Source: Cisco 2025 Data Privacy Benchmark Study

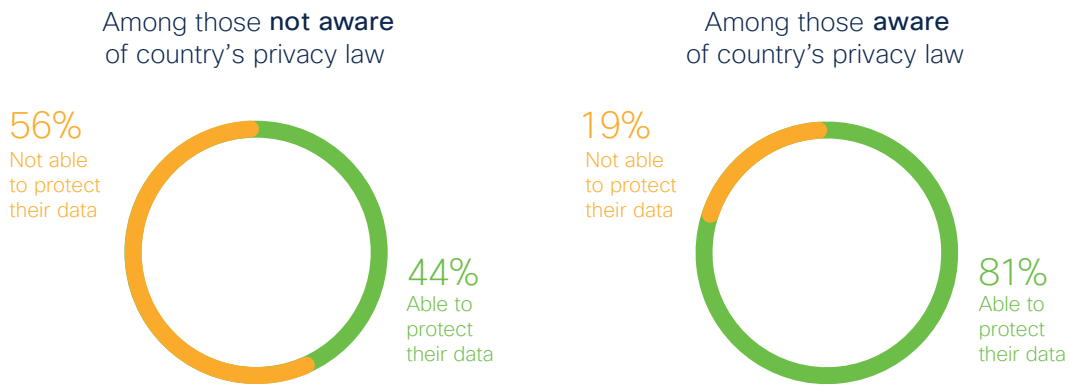
Drawing insights from the Cisco 2024 Consumer Privacy Survey adds a fascinating layer of context to this data. For the first time since the consumer survey's inception in 2019, a majority of global consumers (53%) reported being aware of their country's privacy laws. Awareness of privacy laws highly correlates with consumer confidence. Among respondents who were not aware of their country's privacy laws, only 44% said they are able to protect their personal data. By contrast, among those who are aware of these laws, 81% said they can protect their data, emphasizing the role of regulation as a trust driver for consumers. See Figures 6 and 7.

Figure 6. Awareness of privacy laws, by country



Source: Cisco 2024 Consumer Privacy Survey (Figure 3, page 6)

Figure 7. Awareness of privacy laws and ability to protect data



Source: Cisco 2024 Consumer Privacy Survey (Figure 2, page 6)

3. Privacy investments deliver organization benefits

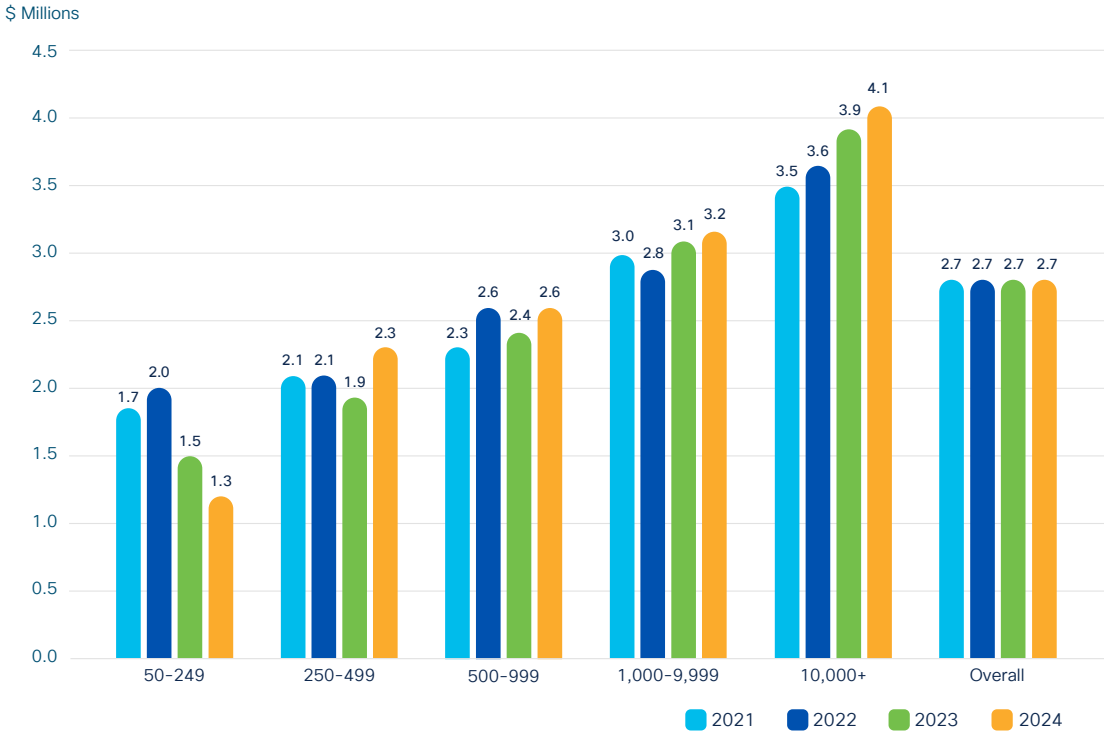
Significant resources are required to comply with data privacy regulations—including cataloging data, implementing controls, conducting impact assessments and interests balancing, and enhancing lines of communication with customers and stakeholders—but most respondents understand the role regulation can play in creating business value. This year, 96% of respondents from the organizations surveyed said that the benefits from this investment outweigh the costs. See Figure 8.

Figure 8. Benefits from privacy investment are greater than the cost

Source: Cisco 2025 Data Privacy Benchmark Study

Organizations' appreciation for the benefits associated with compliance helps explain why overall spending on data privacy has remained consistent over the past four years, with an average spend of $2.7 million across the organizations represented. Medium-sized organizations (250-499 employees), larger organizations (500-999 employees), large enterprises (1,000-9,999 employees), and very large enterprises (10,000+ employees) have all increased their spending year over year. In contrast, smaller organizations (50-249 employees) have decreased their spending. See Figure 9.

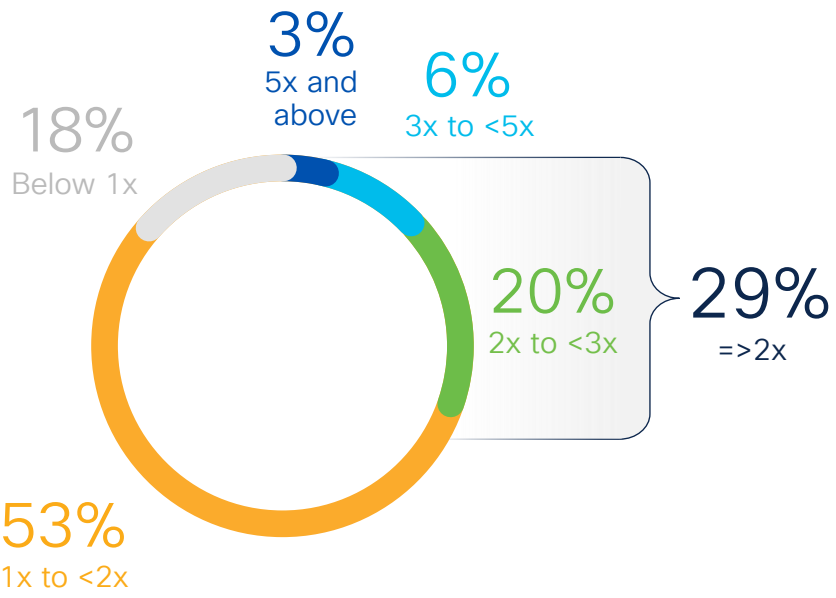
Figure 9. Privacy spending



Notes: For consistency, the 2023 overall spending ($2.7M) is based on historical mix of company size.
Source: Cisco 2025 Data Privacy Benchmark Study

As for the value of those investments, the majority of organizations surveyed (53%) reported an estimated 1x to 2x return (1.6x median) on investment from privacy spending. See Figure 10.

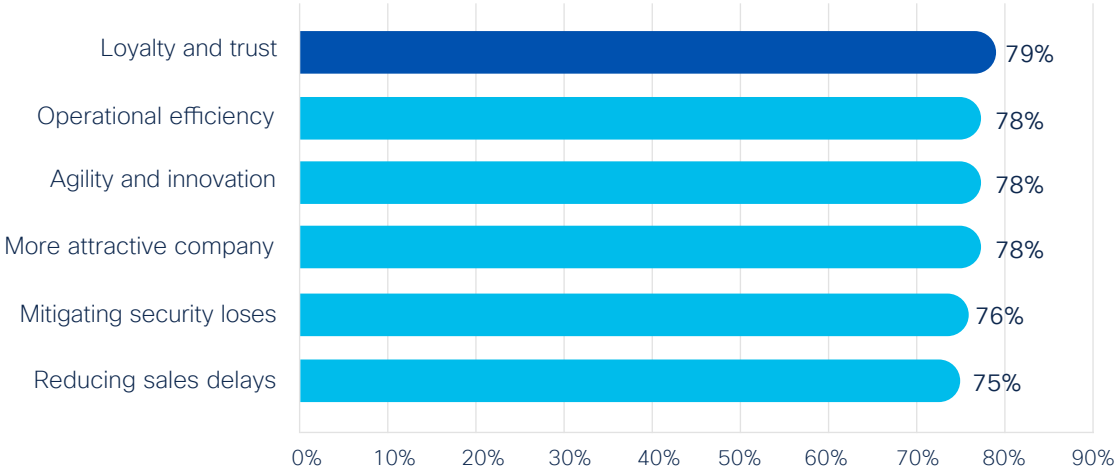
Figure 10. Estimated ROI ranges for respondents, 2024



Source: Cisco 2025 Data Privacy Benchmark Study

To better understand the nature of return on privacy investments, respondents weighed in on specific benefits. At least 75% of respondents cited benefits that included reduced sales delays, mitigation of security losses, increased company attractiveness, increased agility and innovation, improved operational efficiency, and enhanced loyalty and trust among customers. Notably, the percentage of respondents that indicated privacy investments make their organization more attractive to the public increased from 75% to 78% year over year. This makes sense in the context of the 2024 Consumer Privacy Survey where 75% of respondents shared they will not purchase from a provider they do not trust with their data. See Figure 11.

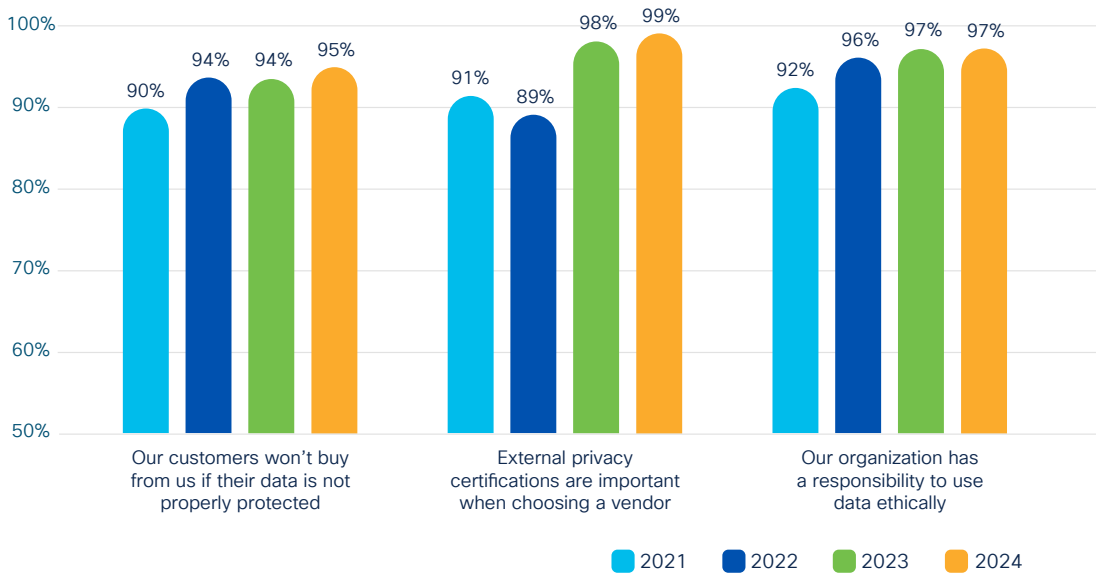
Figure 11. Percentage getting significant benefits from privacy investment, 2024



Source: Cisco 2025 Data Privacy Benchmark Study

Organizations widely recognize that privacy policies and transparency are essential for building customer trust. Most believe customers are increasingly unlikely to purchase goods or services without robust data protection measures in place. Furthermore, nearly all organizations acknowledge their obligation to handle customer data responsibly. External privacy certifications continue to be an important consideration when selecting vendors. This perception held steady in this year's survey with 99% of respondents emphasizing their significance. Organizations are not only prioritizing privacy as a trust driver, but also use independent, third-party validations as proof of their and others' robust data protection practices. See Figure 12.

Figure 12. Privacy's importance to customer trust

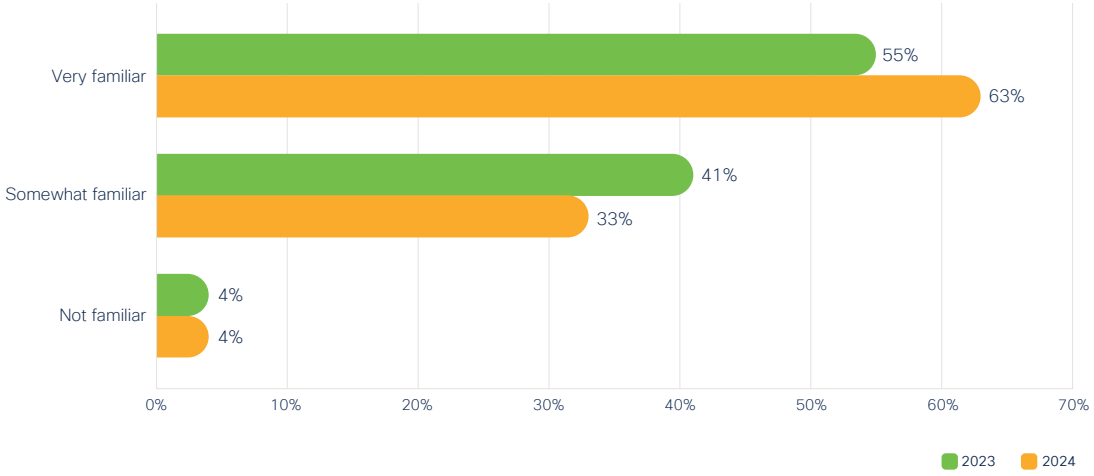


Source: Cisco 2025 Data Privacy Benchmark Study

4. GenAI use increases yet uncertainty remains

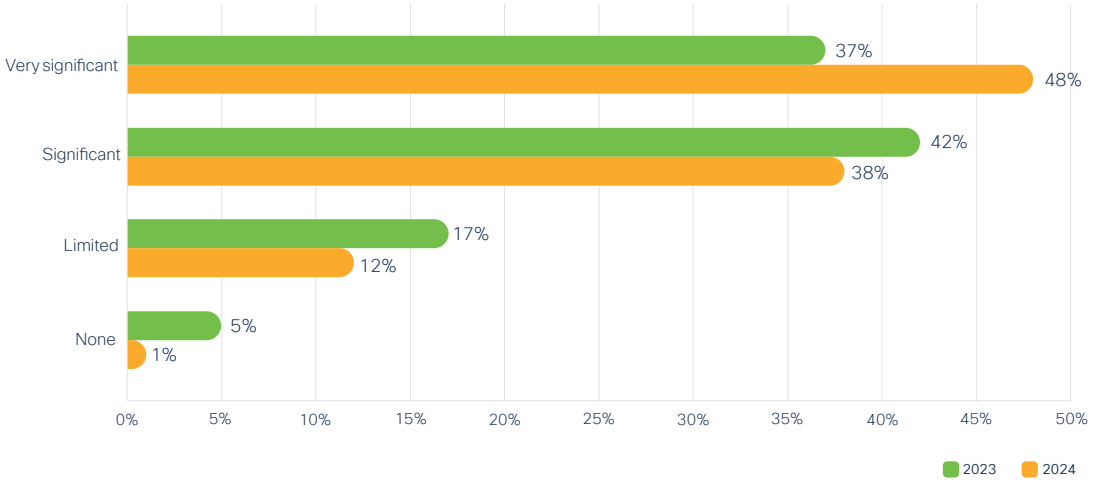
As GenAI use increases, managing privacy risk is paramount. Since the rise of GenAI in late 2022, there has been a rapid adoption of the technology by organizations and individuals alike. People are becoming increasingly comfortable using GenAI. Among those surveyed in 2024, 63% said they were very familiar with GenAI, up from 55% in 2023, and those stating they were only somewhat familiar decreased from 41% in 2023 to 33% in 2024. Only 4% stated they were not familiar with this technology. As awareness grew, so did value. Forty-eight percent of respondents, up from 37% in 2023, said that they are deriving very significant value from GenAI. See Figures 13 and 14.

Figure 13. Familiarity with GenAI



Source: Cisco 2025 Data Privacy Benchmark Study

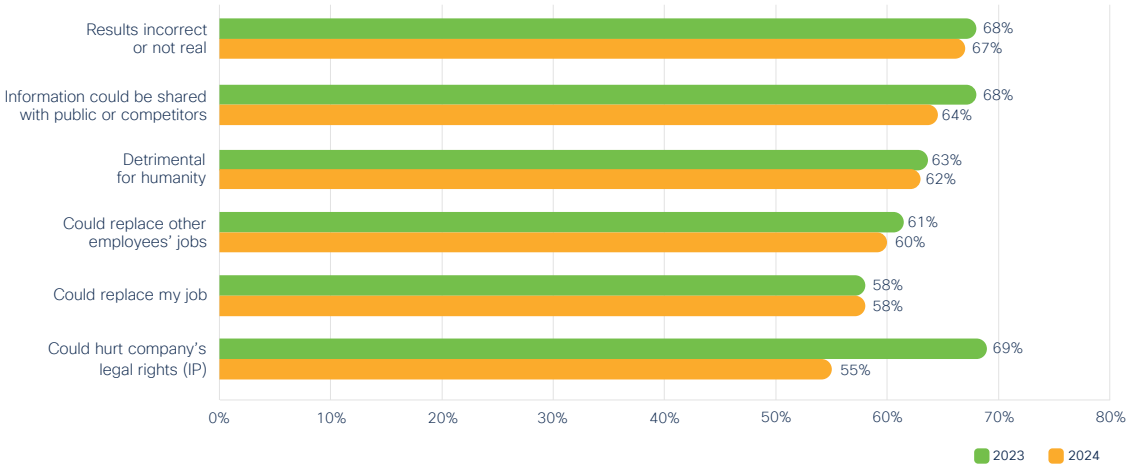
Figure 14. Value from GenAI



Source: Cisco 2025 Data Privacy Benchmark Study

While an increasing number of organizations around the world are using GenAI, respondent concerns about the nascent technology remain relatively steady year over year. One outlier relates to the risk that GenAI could hurt a company's legal rights in the form of copyright or intellectual property. This concern decreased from 69% in 2023 to 55% in 2024. This decline suggests that there is growing awareness of Responsible AI and better governance and controls regarding the input of sensitive data into GenAI tools. Similarly, as organizations become more skilled in using GenAI, worries about the potential for sensitive information leaks have reduced slightly, from 68% to 64% of respondents. Interestingly, while the concern has decreased, nearly half of respondents still reported inputting personal employee information or non-public information into GenAI tools. See Figures 15 and 16.

Figure 15. User concerns with GenAI

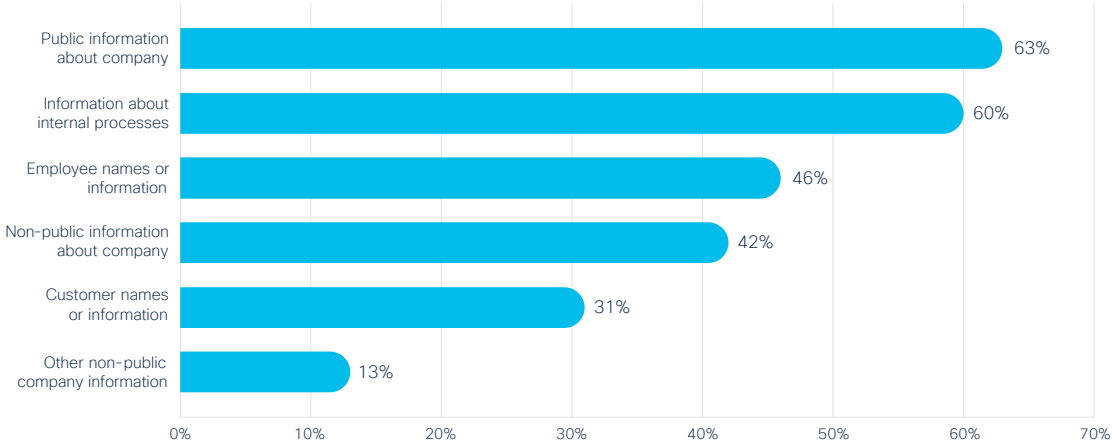


Source: Cisco 2025 Data Privacy Benchmark Study

"For organizations working toward AI readiness, investing in privacy establishes essential groundwork, helping to accelerate effective AI governance."

Dev Stahlkopf
Executive Vice President and Chief Legal Officer, Cisco

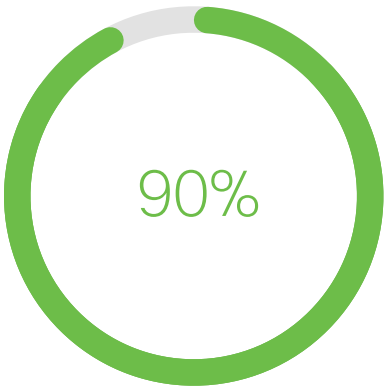
Figure 16. Types of information entered into GenAI applications



Source: Cisco 2025 Data Privacy Benchmark Study

Building on the earlier findings, an overwhelming 90% of respondents agree that strong privacy laws enhance customer comfort in sharing their data with GenAI tools. Privacy laws mandate transparency, fairness, and accountability, ensuring that users understand how their data is used and that it is used appropriately and responsibly. This transparency allows individuals to engage with GenAI technologies with greater confidence, knowing that legal safeguards are in place to protect their personal data. See Figure 17.

Figure 17. Strong privacy laws make customers more comfortable sharing their data in AI applications



Source: Cisco 2025 Data Privacy Benchmark Study

5. Organizations expect to allocate more resources to AI

The Cisco 2024 AI Readiness Index found that there is an overwhelming urgency to invest in AI around the world. Of those surveyed, 98% felt an increase in this urgency from the previous year, while only 13% feel ready to leverage this technology to its full potential.[3] The Index also expects that IT budget allocations will nearly double in the coming years.

In this context, it makes sense that there was nearly unanimous agreement among this year's Data Privacy Benchmark Study respondents (99%) that resources will be reallocated from privacy budgets to AI budgets in the coming year. See Figure 18.

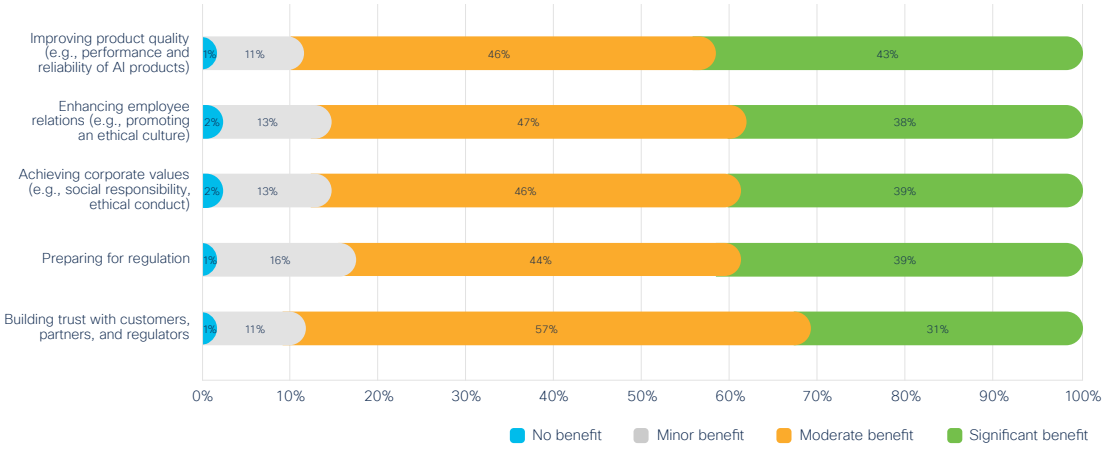
Figure 18. Privacy resources and spending will likely be shifted to AI in the coming year

Source: Cisco 2025 Data Privacy Benchmark Study

[3] Cisco 2024 AI Readiness Index

As organizations race to implement AI, they are seeing the benefits of investing in strong AI governance, including the establishment of ethical, legal, and operational frameworks to manage risk, protect stakeholders, build trust, and avoid fines. Among those surveyed, more than three-quarters acknowledged moderate or significant benefits from robust AI governance in product quality, enhanced employee relations, achievement of corporate values, preparation for regulation, and stakeholder trust. As organizations look to scale their AI governance programs to reap these benefits, they need to determine how these programs will build upon or complement existing privacy investments and weigh any potential decisions on the impact to customer trust. See Figure 19.

Figure 19. Benefits of an AI Governance program



Source: Cisco 2025 Data Privacy Benchmark Study

Conclusion and recommendations for organizations

This research provides a global perspective from privacy and security professionals on data privacy in 2024, emphasizing its critical role in earning, building, and maintaining customer trust for organizations of various sizes and geographies. As GenAI becomes increasingly prevalent, organizations are leveraging existing privacy practices as a foundation for its safe and trustworthy use. However, there is a growing recognition that further investments will be necessary to address emerging risks. Against this backdrop, it would be wise for organizations to consider the following recommendations:

1. Develop a compliance strategy to effectively navigate the complex landscape of data localization regulations and transfer mechanisms when doing business across geographies.
2. Embrace privacy regulation and the growing awareness of these laws among the public. While compliance requires substantial investment, the level of customer trust generated as a result is necessary to mitigate reticence risk and should more than offset its cost.
3. Take a broad view of how investments in privacy can reap business dividends. Certainly, public trust is one, but agility, innovation, speed to market, and operational efficiency also yield significant value.
4. Deploy AI with governance and controls to respect privacy and manage unintended externalities. While there is unquestionable business value to be derived from AI, one must balance both opportunities and risks.
5. Expect budgets and focus to shift toward AI, and make sure AI investments continue to support the underlying privacy and security foundations that are in place and require ongoing resources.

Meeting our customers' standard of trust

Organizations have always required security to protect assets, help manage risk, and build customer confidence and loyalty. Privacy is a critical element of customer trust in today's complex business environment. 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.

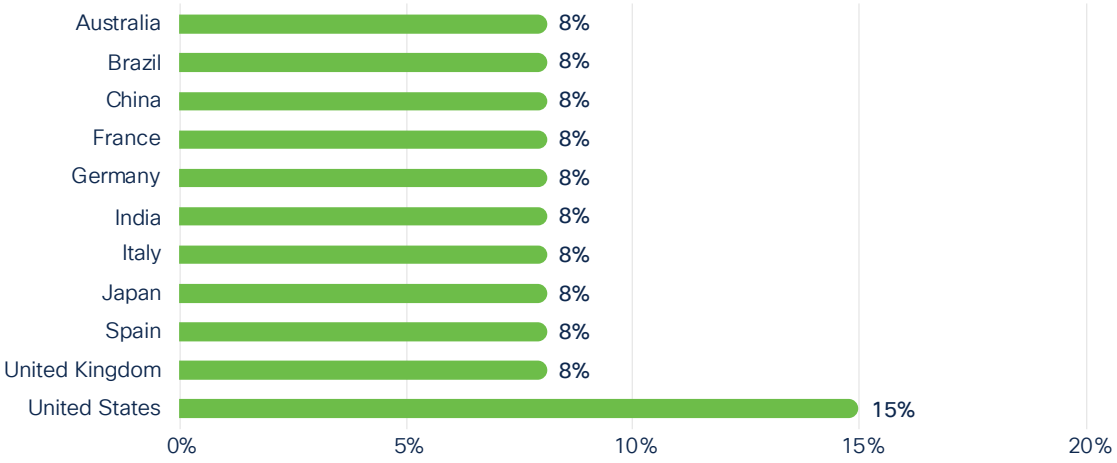
In addition to the annual Data Privacy Benchmark and Consumer Privacy reports, Cisco also publishes Privacy Data Sheets and Privacy Data Maps for its major products and services, enabling anyone interested to understand what personal data is used, who has access to it and how long it is retained. Our Responsible AI Principles and Framework show how these principles and practices form our broad AI governance framework. And the Cisco Purpose Report and Cisco Purpose 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 the Cisco Privacy Center of Excellence by email to ask_privacy@cisco.com.

Appendix

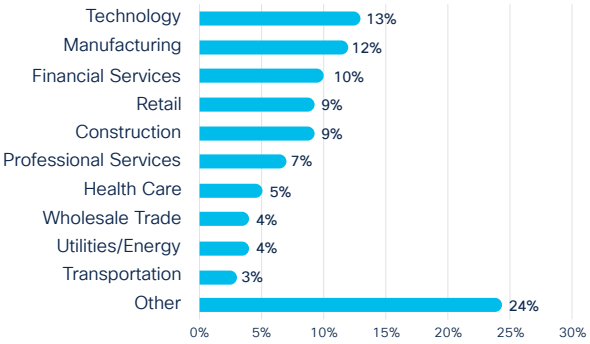
Appendix A. Demographics of survey respondents, by geography



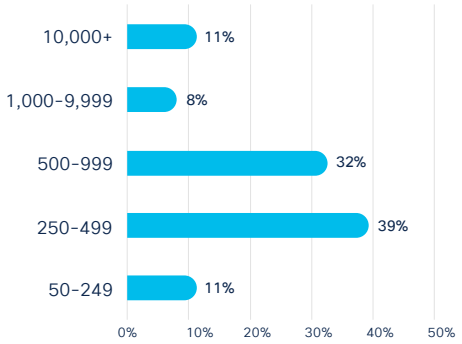
Source: Cisco 2025 Data Privacy Benchmark Study

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

By industry



By company size (# employees)



Source: Cisco 2025 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 Consumer Privacy Survey, Data Privacy Benchmark Study, Threat Insights, and Prioritization to Prediction, with others published throughout the year.


CISCO