CISCO
SECURE

cisco The bridge to possible

Privacy Becomes Mission Critical

Cisco 2022
Data Privacy Benchmark Study

Contents

Introduction 3

Key Takeaways 3

Methodology 4

1. Privacy Becomes Mission Critical 5

2. Privacy Investment and Benefits 10

3. Data Ethics and Automated Decision Making 14

4. Data Localization 16

5. Organizational Options for Privacy 18

Recommendations 20

Appendix 21

About the Cybersecurity Report Series 22

Introduction

Over the past few years, privacy has become mission critical for organizations around the world. More than two-thirds of countries have enacted privacy laws, customers are not buying from organizations who don't protect their data, and privacy metrics are regularly being reported to Boards of Directors. In addition, privacy skills are becoming more important, especially among security professionals, and organizations are benefitting financially from their investments in privacy. This report, our fifth annual review of key privacy issues for organizations, examines privacy's impact on business around the world.

Key Takeaways From the Report Include:

1. Privacy has become essential to organizations' culture and business practices, including their buying processes, management metrics, and employee areas of responsibility.
2. Privacy's Return on Investment (ROI) remains high for the third straight year, with increased benefits, especially for small-to medium-size organizations and higher ROI for more privacy-mature organizations.
3. Most organizations recognize their responsibility to treat data ethically, but many customers want more transparency and are concerned about the use of data particulary in Artificial Intelligence (AI) and automated decision making.
4. Data localization requirements are seen as important but costly.
5. Aligning privacy with security seems to create financial and maturity advantages, compared to other organizational models.

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 5300 security professionals from 27 geographies[1] completed the survey in Summer 2021. Survey respondents represent all major industries and a mix of company sizes (See Appendix 1). We directed privacy specific questions to the more than 4900 respondents who indicated they are familiar with the privacy processes at their organizations. In this report, we also have included relevant results from the Cisco 2021 Consumer Privacy Survey, which was completed in Summer 2021 by 2600 adults in 12 countries[2].

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

[2] *For additional information on this survey, please see Building Consumer Confidence Through Transparency and Control: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf*

1. Privacy Becomes Mission Critical

Privacy has become a business imperative and a critical component of customer trust for organizations around the world. For the second year in a row, 90% of the respondents in our global survey said they would not buy from an organization that does not properly protect its data, and 91% indicated that external privacy certifications are important in their buying process. The COVID-19 pandemic further strengthened privacy's role, as 91% of organizations said their privacy teams have helped them deal with the many complex workforce personal data issues that have arisen in the past few years. Perhaps it is not surprising then that 92% of organizations said that respecting privacy is integral to their culture. See Figure 1.

Figure 1. Privacy's Overall Importance

Source: Cisco 2022 Data Privacy Benchmark Study

Strongly Favorable View of Privacy Laws

Privacy legislation continues to be very well received around the world. These laws play an important role in providing assurances that governments and organizations are being held accountable for how they manage personal data, and over two-thirds (128 of 194) of countries now have privacy laws in place[1]. 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. Eighty-three percent of all corporate respondents said privacy laws have had a positive impact, 14% were neutral,

[1] United Nations Conference on Trade and Development

and only 3% indicated the laws have had a negative impact. Despite the additional complexity brought on by more legislation over the past year, this result is even more positive than in last year's survey (where respondents were 79% positive, 7% negative). Also noteworthy is how strong this is across the world. Many geographies, including Philippines, Mexico, Thailand, Indonesia, China, and Vietnam, had 90% or more of respondents saying privacy regulation has had a positive impact, and every geography in our survey had at least two-thirds of respondents indicating the same. See Figure 2. As discussed in our previous reports, both consumers and organizations expect and value a strong governmental role in protecting privacy. The regulations can provide a more consistent standard of care, greater clarity on the rights and recourses of data owners, and guidelines as to what data processing activities are permitted or prohibited.

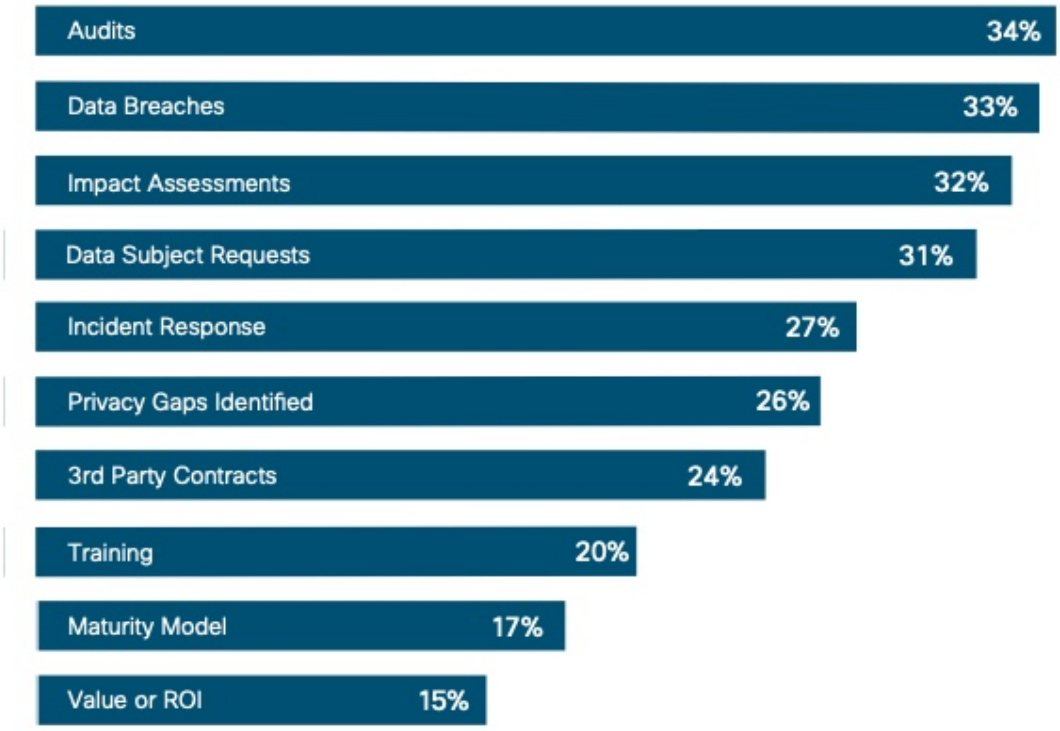
Figure 2. Impact of Privacy Laws, by Geography

Source: Cisco 2022 Data Privacy Benchmark Study

Vast Majority are Reporting Privacy Metrics to their Board of Directors

An 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, 94% are reporting one or more privacy-related metrics to the Board. While some are reporting as many as 10 privacy metrics, most are reporting between 1 and 3, with the overall average 2.6. The most reported metrics include Privacy Program Audit findings (34%), Personal Data Breaches (33%), and the results of Privacy Impact Assessments (32%). See Figure 3.

Figure 3. Privacy Metrics Reported to Board of Directors

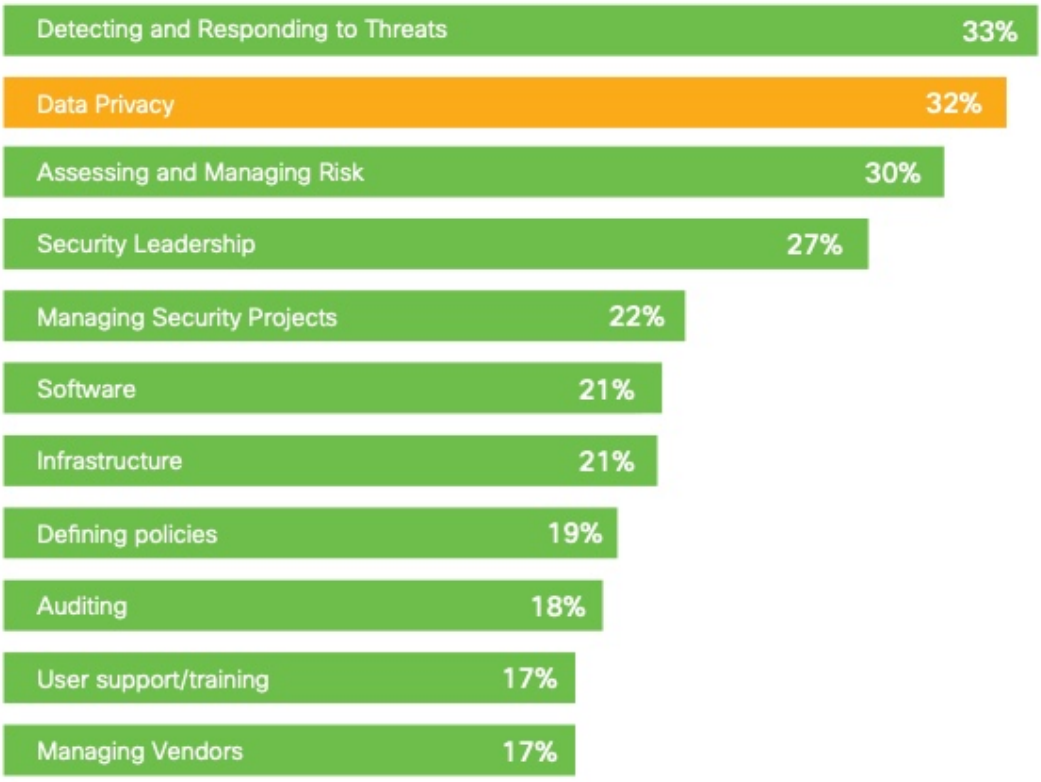


Source: Cisco 2022 Data Privacy Benchmark Study

Privacy is a Core Area of Responsibility for Security Professionals

Privacy skills have become increasingly critical, especially 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. "Data Privacy and Governance" was selected by 32% of these respondents, making it second only to "Detecting and Responding to Threats" and just ahead of "Assessing and Managing Risk". See Figure 4. Data privacy has become a core competency for these security teams, and integrating privacy skills can help ensure that those who are authorized to access data will handle it appropriately.

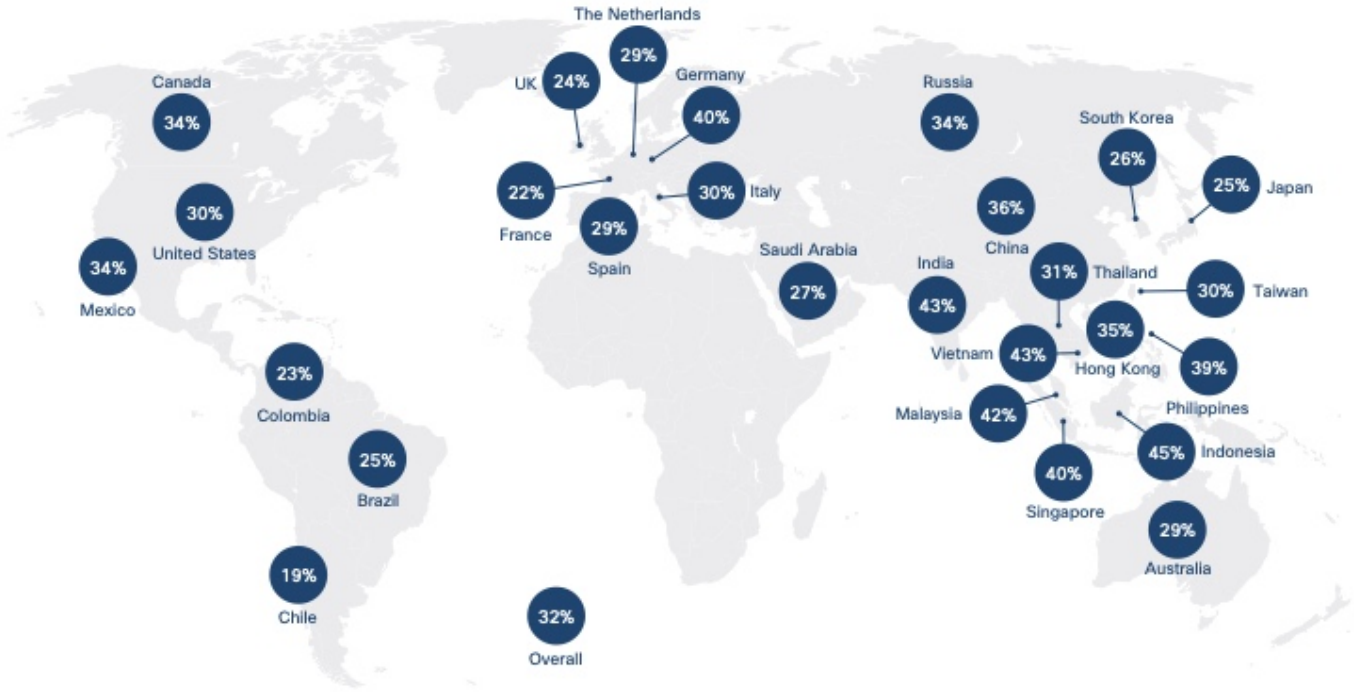
Figure 4. Primary Areas of Responsibility among Security Professionals (could choose up to 3)



Source: Cisco 2022 Data Privacy Benchmark Study

Interestingly, several Asia-Pacific geographies had the highest percentage of respondents where privacy was identified as an area of responsibility, i.e., Indonesia (45%), Vietnam (43%), India (43%), and Malaysia (42%). The lowest percentages were in Chile (19%), France (22%), Columbia (23%), and the UK (24%). See Figure 5. The differences may reflect stronger integration between security and privacy in many countries in Asia-Pacific. It may also be due to organizations in countries with longer-standing privacy regimes assigning privacy responsibilities to areas other than the Security function, but more research will be needed on this issue.

Figure 5. Percentage of Security Professionals Identifying Privacy as an Area of Responsibility, by Geography

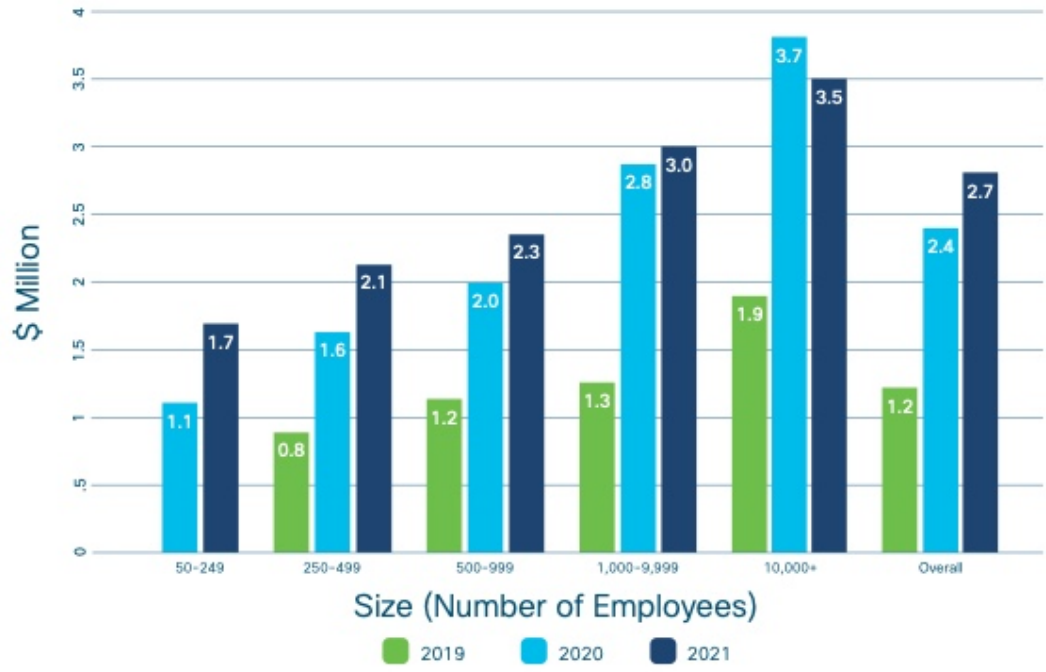


Source: Cisco 2022 Data Privacy Benchmark Study

2. Privacy Investment and Benefits

As privacy becomes more integrated into organizational priorities, investment continues to rise. The average privacy budget was up 13% from $2.4 Million last year to $2.7 Million this year. Spending at smaller organizations of 50-249 employees increased from $1.1 Million to $1.7 Million, and those with 250-499 employees increased from $1.6 Million to $2.1 Million. Meanwhile, the largest organizations (10,000+ employees) saw a slight decrease in spending from $3.7 Million to $3.5 Million this year after a steep increase last year. See Figure 6. In future research, we will explore where the spending growth is coming from, be it headcount, technology, or outside counsel.

Figure 6. Privacy Spending, By Organization Size



Note: 50-249 category initiated in 2020
Source: Cisco 2022 Data Privacy Benchmark Study

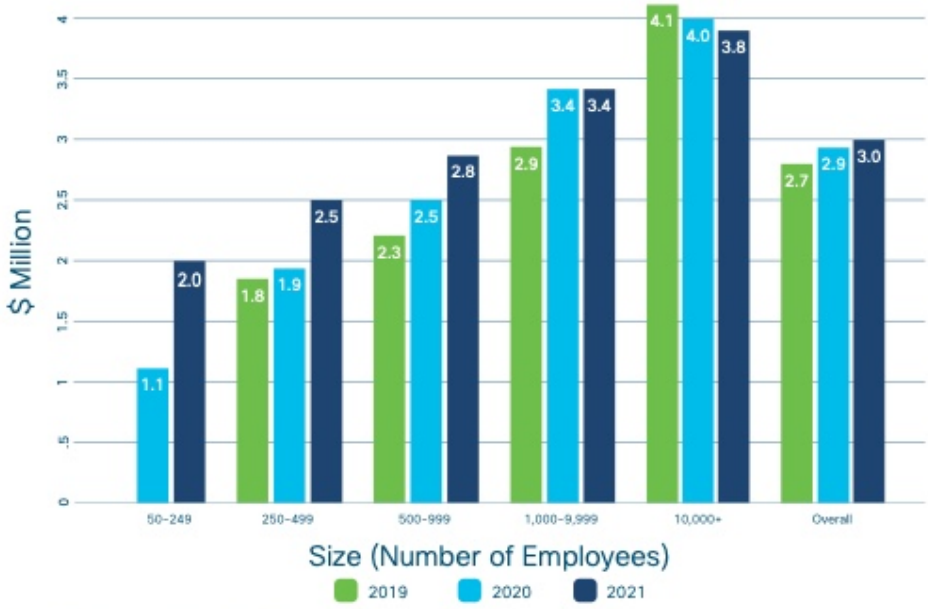
The business value associated with these investments remains high. Ninety percent of all respondents said they consider privacy a business imperative. More specifically, we asked respondents about the potential benefits in 6 areas: reducing sales delays, mitigating losses from data breaches, enabling innovation, achieving operational efficiency, building trust with customers, and making their company more attractive. For each of these six areas, greater than 60% of respondents felt they were getting significant or very significant benefits, and this measure has been broadly consistent for the past two years. See Figure 7.

Figure 7. Percentage Getting Significant Benefits in Each Area

Source: Cisco 2022 Data Privacy Benchmark Study

Respondents were also asked to estimate the financial value of the benefits from their privacy investments, and the average estimate was up 3% from $2.9 Million last year to $3.0 Million this year. Interestingly, the smaller organizations saw the largest percentage increases this year. Those with 50-249 employees increased from $1.1 Million to $2.0 Million, and those with 250-499 employees increased from $1.9 Million to $2.5 Million. Benefits at organizations with 1000-9999 employees remained constant at $3.4 Million and at the largest organizations with more than 10,000 employees, benefits fell slightly from $4.0 Million to $3.8 Million.
See Figure 8.

Figure 8. Estimated Privacy Benefits, by Organization Size



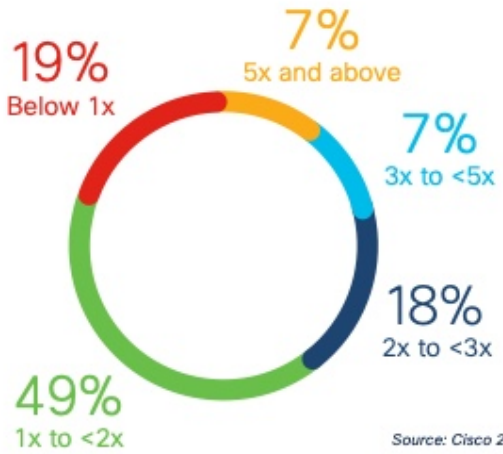
Note: 50–249 category initiated in 2020

Source: Cisco 2022 Data Privacy Benchmark Study

ROI Declines Slightly, but Remains Strong

From a return-on-investment perspective, the average organization estimated benefits at 1.8 times spending, which is down from 1.9 in last year's survey. We believe this is due to ongoing needs in responding to the pandemic, adapting to new legislation, uncertainly over international data transfers, and increasing requirements for data localization (see below). Nonetheless, most organizations continue to get a very attractive return on their privacy investments. Thirty-two percent of organizations are getting benefits at least 2x spend, and only 19% are estimating they are not breaking even on their privacy investments. See Figure 9.

Figure 9. Ratio of Privacy Benefits to Investment

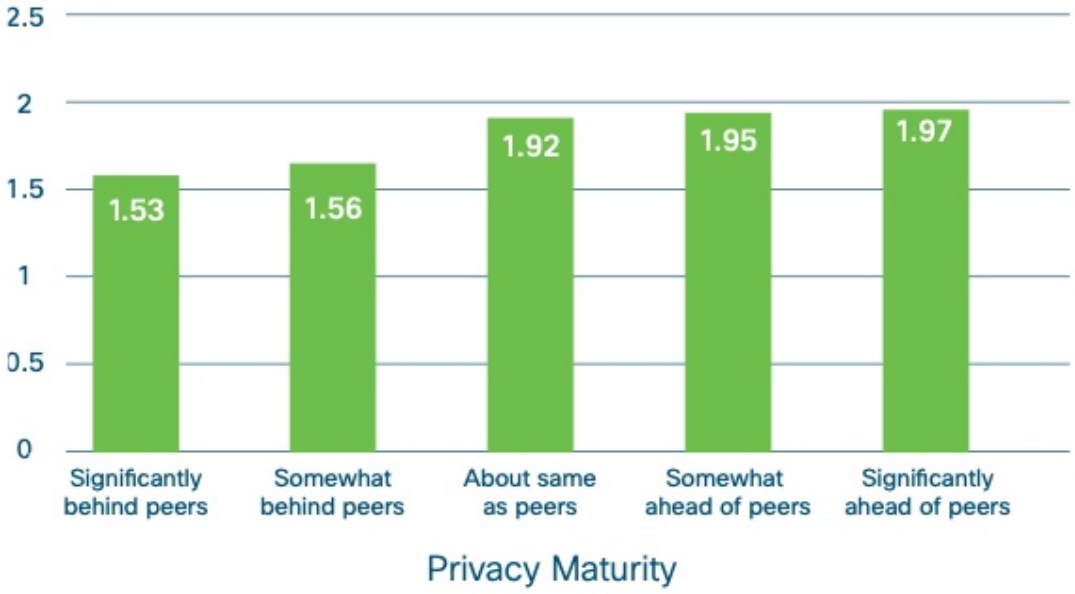


Source: Cisco 2022 Data Privacy Benchmark Study

Returns Higher for More Mature Organizations and Where Privacy is Integrated with Security

It is also interesting to note the correlations between return and other factors like privacy maturity. Respondents who felt their privacy program was behind that of their peers were getting a lower return than those who felt they were the same or ahead of their peers. Specifically, the least mature had an average return of 1.53, compared to an average return of 1.97 for the most mature. This further demonstrates the value of privacy investment, as the most mature organizations are also realizing the greatest returns. See Figure 10.

Figure 10. Estimated Returns (Benefits divided by spending)



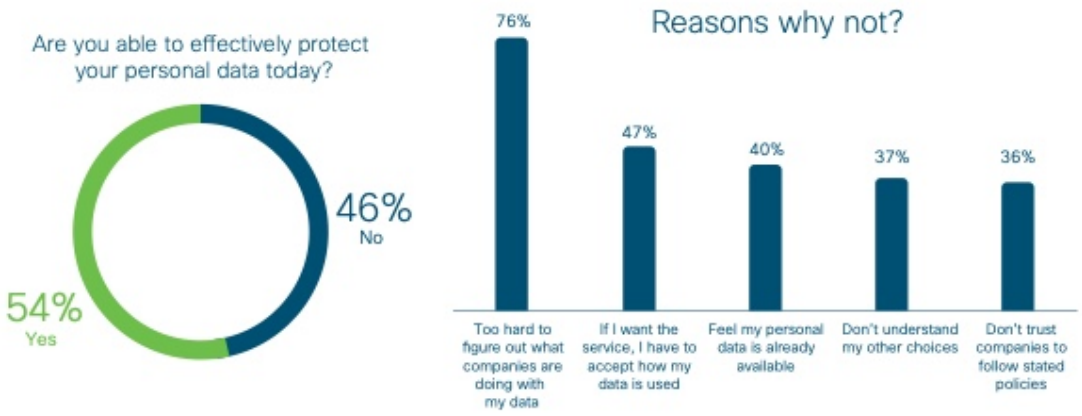
Source: Cisco 2022 Data Privacy Benchmark Study

Another relevant correlation was between the privacy return and whether the respondent identified privacy as a core responsibility of their job as security professionals. Organizations where the respondent identified privacy as a responsibility had an average return of almost 2x compared with 1.71x where the respondent did not identify privacy. This result suggests there is business value with having privacy and security working hand in hand.

3. Data Ethics and Automated Decision Making

Artificial Intelligence (AI) and automated decision-making raise particular challenges for organizations and consumers regarding the use of personal data. Ninety-two percent of survey respondents recognize that their organization has a responsibility to only use data in an ethical manner. And nearly as many (87%) believe they already have processes in place to ensure automated decision-making is done in accordance with customer expectations. Consumers do not agree. Drawing on results from the Cisco 2021 Consumer Privacy Survey, nearly half (46%) of consumers feel they cannot adequately protect their data, and the primary reason is that they don't understand exactly what organizations are collecting and doing with their data. See Figure 11.

Figure 11. Ability of Consumers to Protect Their Data



Source: Cisco Consumer Privacy Study - 2021

Consumers value transparency when it comes to how their data is used, and decision-making with AI can be particularly difficult to explain. In fact, 56% of survey respondents expressed concerns about how businesses are using AI today. What's more, when asked about using personal data in a number of typical AI use cases (e.g., selection of a sales representative, setting prices, determining credit worthiness), a large percentage, ranging from 37% to 55%, said that they would trust a company less that used AI for these decisions. See Figure 12. Organizations need to do more to ensure customers understand how their data is being used and built trust. This will likely be a significant challenge with respect to AI-based decisions.

Figure 12. AI Use Cases and Loss of Trust

Source: Cisco Consumer Privacy Study - 2021

4. Data Localization

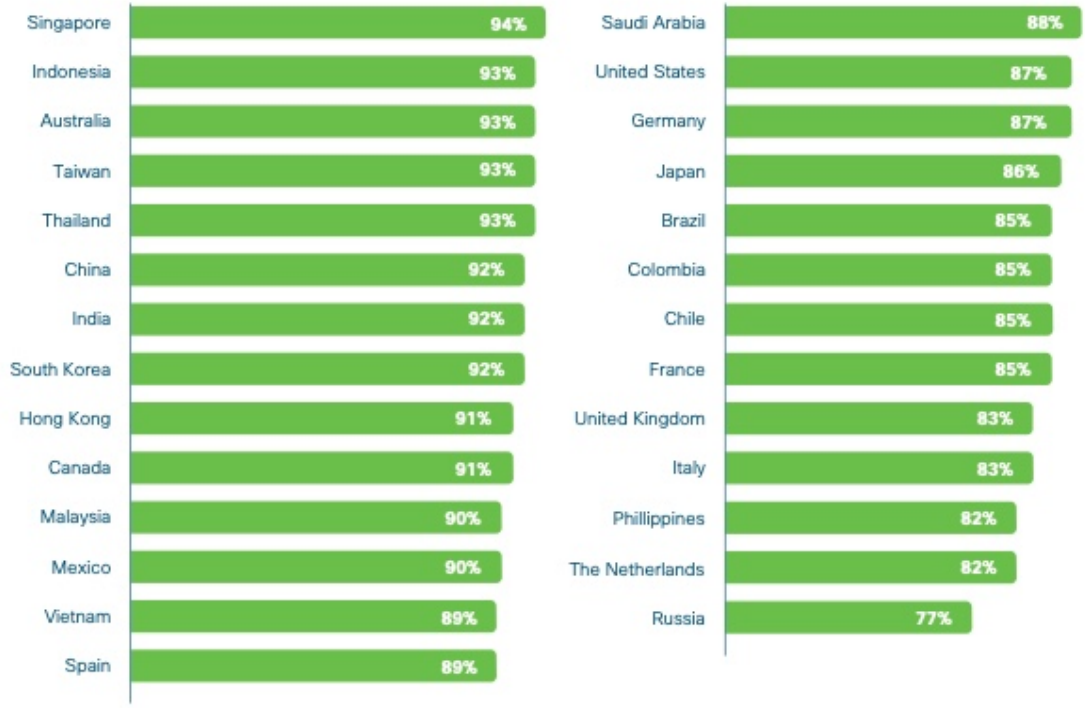
As governments and organizations continue to demand protections and commitments for data transferred outside their national borders, more are putting in place data localization requirements. In a new area of research this year, 92% percent of survey respondents said this has become an important issue for their organizations, and the same percentage indicated they believe it is needed to help safeguard personal data. But it comes at a price. Eighty-eight percent said that localization requirements are adding significant cost to their operation. See Figure 13.

Figure 13. Data Localization

Source: Cisco 2022 Data Privacy Benchmark Study

While this requirement is often driven by national laws and attitudes, there was not substantial variation across respondents in different geographies. The percentage of respondents saying data localization was adding cost to their operation was between 77% and 94% in all geographies. See Figure 14.

Figure 14. Percentage Saying Data Localization is Adding Significant Cost, by Geography

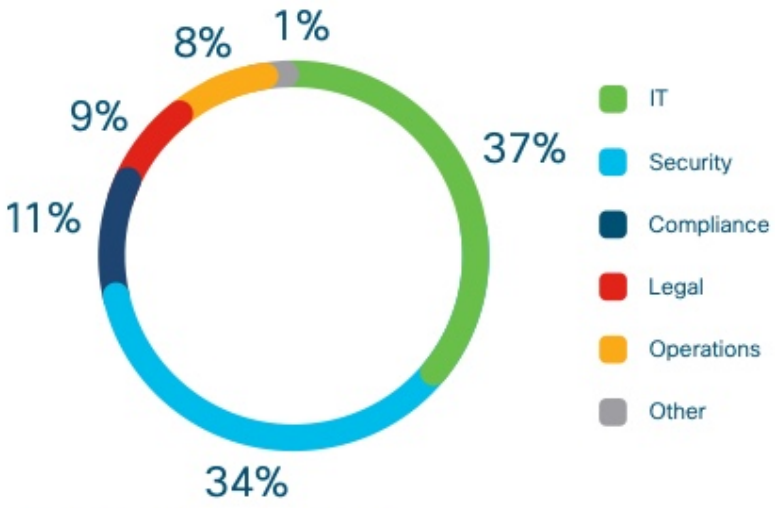


Source: Cisco 2022 Data Privacy Benchmark Study

5. Organizational Options for Privacy

In benchmarking exercises, privacy professionals are particularly interested in understanding where the privacy function sits within other organizations, and where might be the best fit. Across the respondents in our survey, there did not appear to be one dominant model. Privacy was most often located in IT (37% of respondents), followed by Security, Compliance, Legal, and Operations. See Figure 15.

Figure 15. Organizational Location of Privacy Office



Source: Cisco 2022 Data Privacy Benchmark Study

As to where might be the best fit, one factor would be which model is consistent with the higher estimated returns on privacy investment. Among survey respondents, the highest average return was among organizations where Privacy is located in Security, with a return of 1.91. Those located in IT had an average return of 1.87, and those in Legal had 1.77. See Figure 16.

Figure 16. Average Return, by Location of Privacy Office

Source: Cisco 2022 Data Privacy Benchmark Study

From the standpoint of privacy maturity, those where Privacy is located in Security were more likely (43%) to say they were ahead of their competitors, compared to those where Privacy is located in IT (37%), Legal (37%), Compliance, or Operations. See Figure 17. These correlations again suggest there is significant business value from tighter integration between Privacy and Security.

Figure 17. Percentage of Respondants Saying their Privacy Maturity is Ahead of their Peers, by Location of Privacy Office

Source: Cisco 2022 Data Privacy Benchmark Study

Recommendations

Privacy continues to be integrated into organizational priorities, and the findings in this research point to specific recommendations on how to demonstrate trust and maximize the benefits of privacy investments, including:

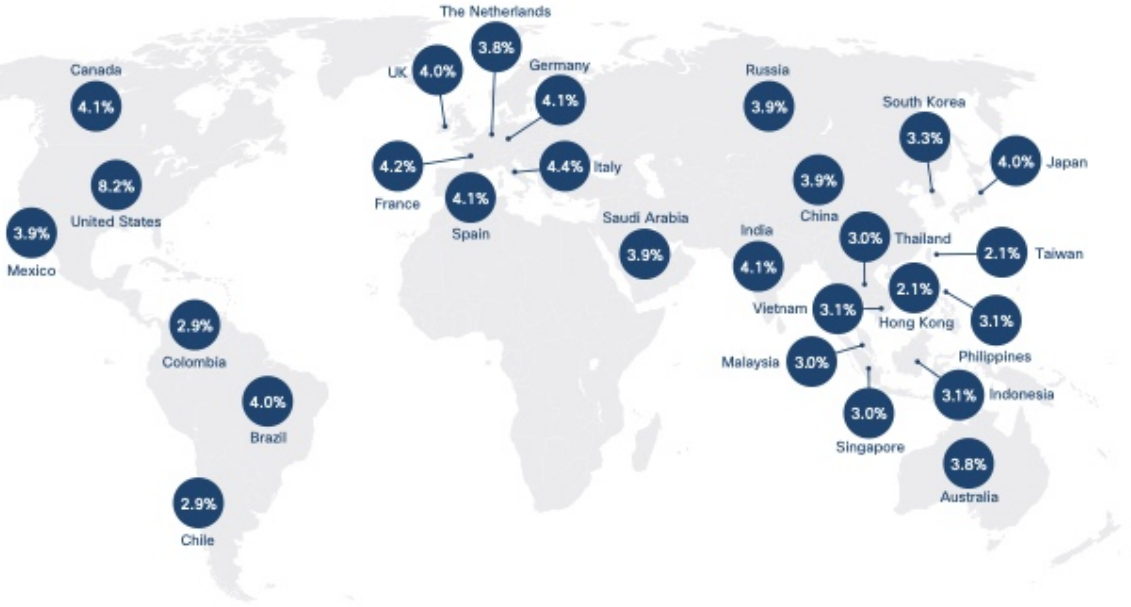
1. Continue to build privacy capabilities throughout your organization, particularly among security and IT professionals and those who are involved directly with personal data processing and protection.
2. Be transparent about how personal data is being used by the products and services your organization delivers. Customers want to know – and be reassured – that their data is not being abused and used in ways they don't expect, know about, or understand.
3. Proceed carefully and thoughtfully when using personal data in AI and automated decision-making that materially affects customers. Designing and building with an ethical framework by design, establishing governance and oversight over your AI program, and providing transparency on when and how you are using automated decision-making are all positive steps organizations can take.
4. Invest in privacy – it pays off!

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

Cisco recently published "The New Trust Standard" that provides a framework on how to demonstrate and communicate trust. This is a paradigm for the zero-trust architecture and includes a set of principles for keeping data safe, being transparent, and demonstrating accountability via certifications.

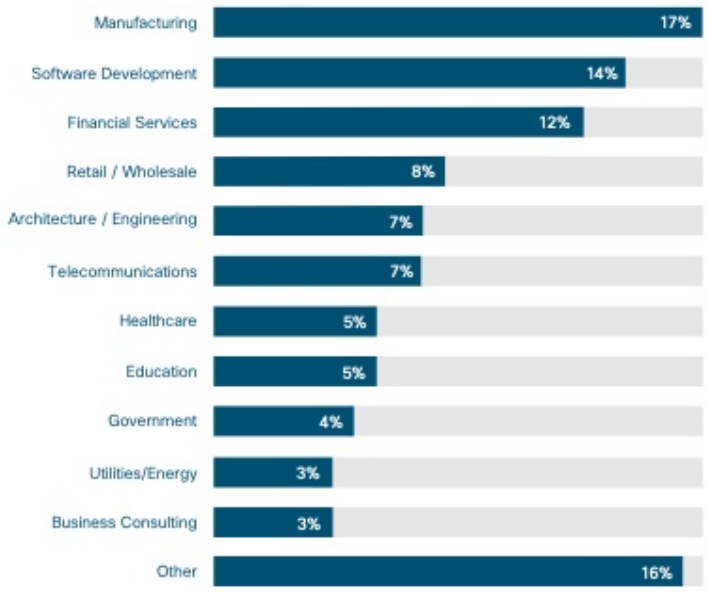
Appendix: Demographics

By Country / Geography



Source: Cisco 2022 Data Privacy Benchmark Study

By Industry



Source: Cisco 2022 Data Privacy Benchmark Study

By Company Size (# Employees)

Source: Cisco 2022 Data Privacy Benchmark Study

About the Cybersecurity Report Series

Throughout the past decade, Cisco has published a wealth of definitive 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 organizational implications, as well as leading and proactive practices to defend against cyber criminals. In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. 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 of threat researchers and innovators in the security industry, the reports in the 2021–22 series include the Consumer Privacy Study, Threat Report, and Security Outcomes Study, with others published throughout the year. For more information, and to access all the reports and archived copies, www.cisco.com/go/securityreports.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published January 2022 RPT_01_2022

cisco SECURE

SECURE

The bridge to possible