



Forged by the Pandemic: The Age of Privacy

Contents

| | |
|--|----------|
| Introduction | 3 |
| Key Findings | 4 |
| Methodology | 5 |
| Supporting Quotes | 6 |
| Forged by the Pandemic: The Age of Privacy | 7 |
| 1. Helping Organizations Overcome the Challenges of the Pandemic | 7 |
| 2. Higher Privacy Investment and Attractive ROI | 9 |
| 3. Strongly Favorable Reaction to Privacy Legislation | 11 |
| 4. External Privacy Certifications as a Critical Buying Factor | 13 |
| 5. Privacy Maturity and Its Impact on Value. | 13 |
| 6. Privacy – a Core Competency for Security Professionals | 15 |
| 7. Reporting Privacy Metrics to the Board. | 17 |
| Conclusion | 18 |
| About the Cybersecurity Report Series | 19 |
| Appendix. | 20 |

Introduction

The COVID-19 pandemic led to dramatic changes in 2020, many of which involved sharing our personal lives, routines, social circles, health status, and data with governments, employers, and strangers while learning to interact remotely and in new, digital ways. It also put strains on privacy, as the need to protect individual's data was often in conflict with the need to protect public health. Fortunately, privacy protections established over the last decade helped decision makers strike the right balance between individual concerns and community needs.

In this year's **Data Privacy Benchmark Study**, we've found strong evidence that privacy has become an even more important priority during the pandemic. Privacy budgets have increased over the last year, organizations have more resources focused on privacy, and privacy investments going above and beyond the law are translating into real business value. Privacy legislation and external certifications are providing assurance in a business environment where it's hard to know whom to trust. Consumers are exercising their privacy rights and demanding enforcement of existing privacy protections. The reaffirmation of privacy's value even during the pandemic positions it as a priority for years to come. Privacy is no longer an afterthought; it is core to how we work and interact with each other. The Age of Privacy has arrived.

Key Findings

In this study, we continue our exploration of privacy practices and maturity levels at organizations around the world, their financial investments in privacy, business benefits from these investments, and the forces driving these behaviors. In this year's research, we also included several questions related to the pandemic and its impact.

Some of the key findings include:

- Ninety-three percent of organizations turned to their privacy teams to help navigate and guide their pandemic response
- Privacy budgets doubled in 2020 to an average of \$2.4 million
- ROI was slightly down compared to 2019, but remains attractive with 35% reporting benefits at least 2 times their investments
- Privacy laws are viewed very favorably around the world, with 79% of organizations indicating they are having a positive impact (and only 5% negative impact)
- External privacy certifications (e.g., ISO 27701, APEC Cross-Border Privacy Rules, and EU Binding Corporate Rules) are an important buying factor for 90% of organizations when choosing a product or vendor
- Organizations with more mature privacy practices are getting higher business benefits than average and are much better equipped to handle new and evolving privacy regulations around the world
- Data Privacy has become a top area of responsibility for security professionals, with 34% of survey respondents indicating privacy is one of their core competencies and responsibilities
- Ninety-three percent of organizations are reporting privacy metrics (e.g., privacy program audit findings, privacy impact assessments, and data breaches) to their Boards

These findings provide strong evidence that the commitment to privacy has been strengthened during the pandemic. Organizations that get privacy right improve trust with their customers, operational efficiency, and both top-line and bottom-line results.


Methodology

The data in this study is derived from the Cisco Annual Security Outcomes Study, where the 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 25 geographies¹ completed the survey in Summer 2020. Survey respondents represent all major industries and a mix of company sizes (See Appendix 1).

We directed privacy-specific questions to the more than 4400 respondents who indicated they are familiar with the privacy processes at their organizations. We also have included relevant results from Cisco's 2020 Consumer Privacy Survey, which was completed in Summer 2020 by 2600 adults in 12 countries².

¹ Australia, Brazil, Canada, China, 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 "Protecting Data Privacy to Maintain Trust": https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

A black and white photograph of a man in profile, wearing a patterned face mask and glasses, looking at a laptop screen. The background is a blurred office setting with a desk and another person's hands typing on a keyboard.

“It is gratifying to see privacy teams and principles front and center in how companies have responded to the challenges of the pandemic.”

– Jules Polonetsky, CEO, The Future of Privacy Forum

“As this latest Cisco research shows, many organizations were unprepared for the shift to remote working during the pandemic. Robust privacy and security protections have become even more critical in enabling people to work and interact securely from anywhere.”

– Jeetu Patel, SVP and General Manager, Security and Applications, Cisco

“I’m thrilled that privacy investments are translating into higher business value and better preparedness in a rapidly evolving regulatory landscape. Designing and building privacy protections into products doesn’t hinder innovation – it enhances it!”

– Ruby Zefo, Chief Privacy Officer, Uber

Forged by the Pandemic: The Age of Privacy

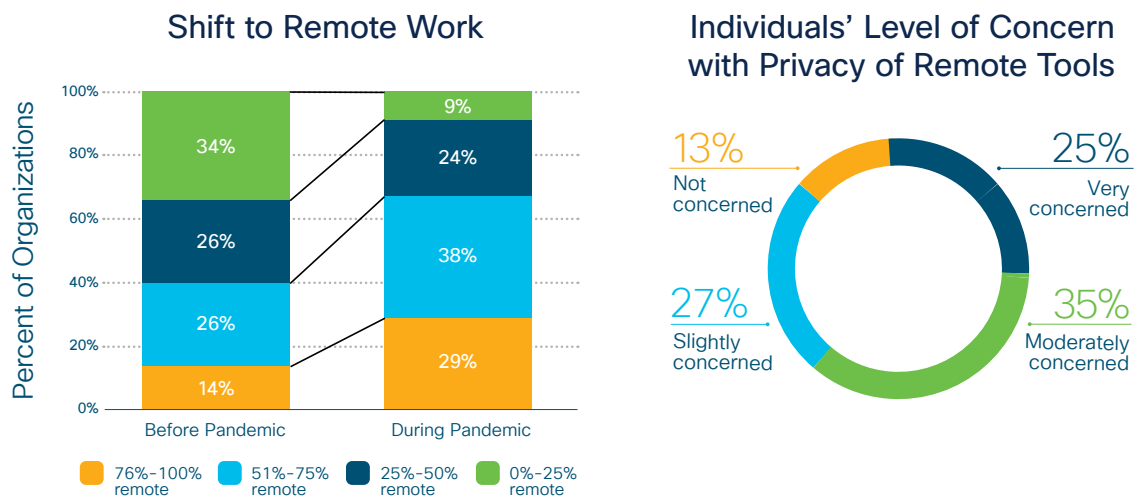
1. Helping Organizations Overcome the Challenges of the Pandemic

The COVID-19 pandemic forced many changes on society in 2020, including a rapid shift to remote working and an often-urgent need for personal health information to support public health initiatives. Rather than being pushed aside, privacy teams and privacy principles have attained greater prominence as they have helped organizations manage this shift and balance the competing interests of individual rights and public safety.

Ninety-three percent of organizations said their privacy teams played a significant role in helping them navigate and respond to the challenges brought on by COVID-19. These challenges included the shift to remote working, determining when and how to share personal information, and implementing controls to limit access and use of any shared personal data.

During the pandemic, the percentage of organizations where most employees were working remotely jumped from 40% to 67%, and 91% of organizations had at least a quarter of their employees working remotely. Unfortunately, many were unprepared for this transition. Only 41% of organizations described themselves as fully prepared for this shift from a privacy and security perspective, and 87% of individuals expressed concern with the privacy protections involved in the tools they needed to work and interact remotely. (See Figure 1.)

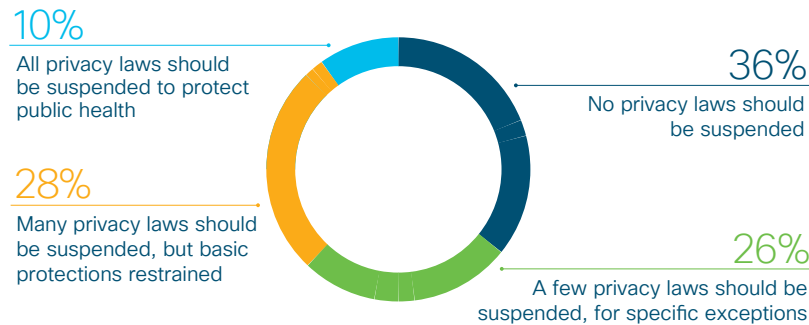
Figure 1. Shift to Remote Work and Associated Privacy Concerns (N=4673, 2115)



Source: Cisco Data Privacy Benchmark Study - 2021 ; Cisco Consumer Privacy Study - 2020

In responding to the pandemic, governments and organizations needed health-related personal data to understand co-morbidity factors and exposure risk to keep their communities and workplaces safe. Despite the need, consumers generally supported few if any exceptions to the privacy protections for their data. Thirty-six percent of respondents in the Consumer Survey wanted no change to existing privacy laws, with another 26% supporting only limited exceptions. Only 10% thought privacy should take a back seat to safety during the pandemic. (See Figure 2.)

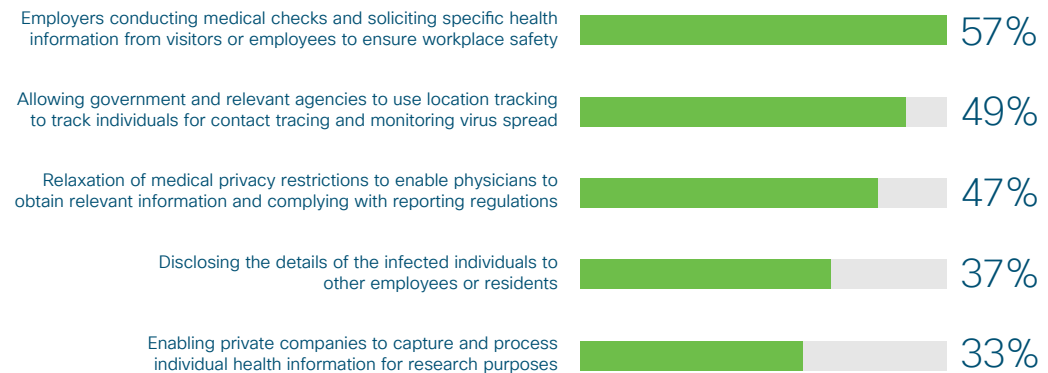
Figure 2. Retaining Privacy Laws During the Pandemic (N=2602)



Source: Cisco Consumer Privacy Study - 2020

In considering specific use cases, 57% were supportive of employers' need for health information to keep their workplaces safe, but most other use cases were only supported by a minority of respondents. These included location tracking, contact tracing, relaxing medical restrictions, disclosing information about infected individuals, and using individual information for research. (See Figure 3.)

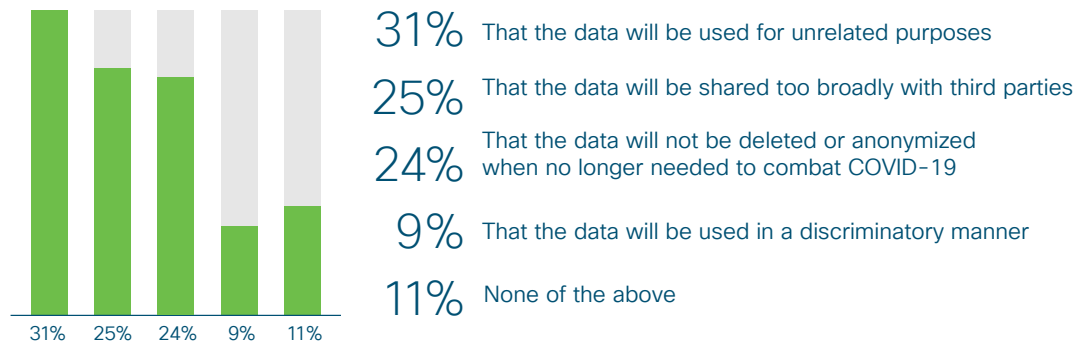
Figure 3. Limited Support for Specific Use Cases of Data Sharing (N=2602)



Source: Cisco Consumer Privacy Study - 2020

Individuals continued to want any use of their personal data to be very limited and strictly controlled. Their top concerns were consistent with fundamental privacy principles – transparency, fairness, and accountability. Specifically, they were worried that their data would be used for undisclosed, unrelated purposes, that it would be sold or shared with third parties for marketing purposes, or that it would not be deleted when it is no longer needed (See Figure 4.).

Figure 4. Top Privacy Concerns about Sharing Data During Pandemic (N=2602)



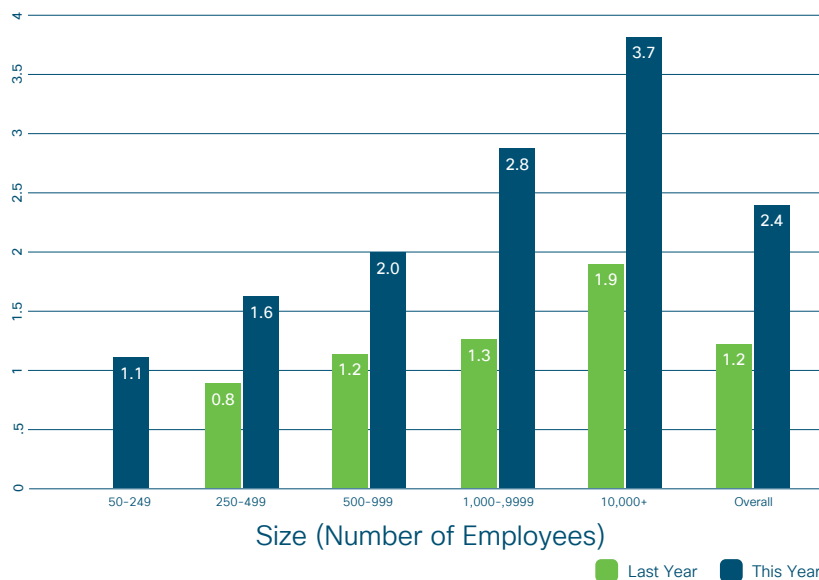
Source: Cisco Consumer Privacy Study - 2020

Privacy principles and protections helped governments, organizations, and consumers navigate appropriate uses of data during the pandemic, and many see the positive impact longer term. Forty percent of individuals felt the pandemic would further strengthen the importance of respecting data privacy once the pandemic was over.

2. Higher Privacy Investment and Attractive ROI

With the increasingly critical role of privacy, one would expect privacy budgets to rise. In fact, the average privacy budget doubled from \$1.2 million among last year's respondents to \$2.4 million this year. The increase was fairly consistent across organizations of different sizes. For smaller organizations (250-499 employees), the average budget grew from \$0.8 million to \$1.6 million, and for larger organizations (10,000+ employees), the average budget grew from \$1.9 million to \$3.7 million. (See Figure 5.)

Figure 5. Privacy Spending, By Organization Size (N=3815)

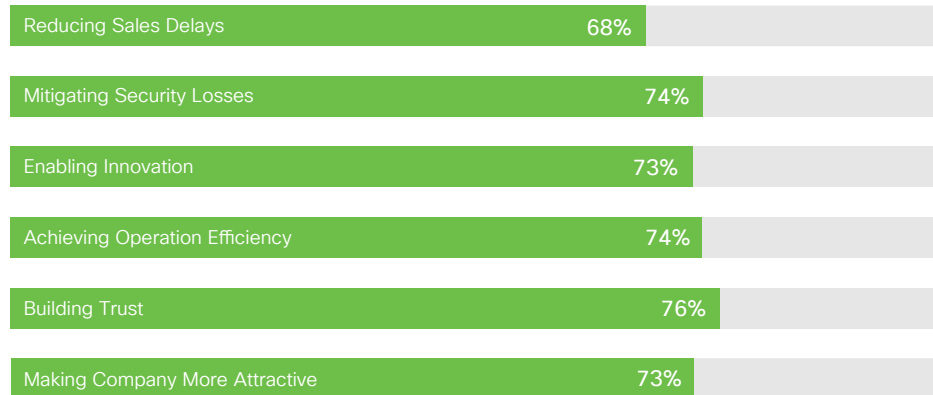


Source: Cisco Data Privacy Benchmark Study - 2021.

Note: The 50-249 employee segment was not surveyed last year.

The business value associated with these investments also remained high. We asked respondents about any 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. In each of these areas, more than two-thirds of respondents felt they were getting significant benefit, which is consistent with last year's results and up significantly from around 40% from the year before. (See Figure 6.)

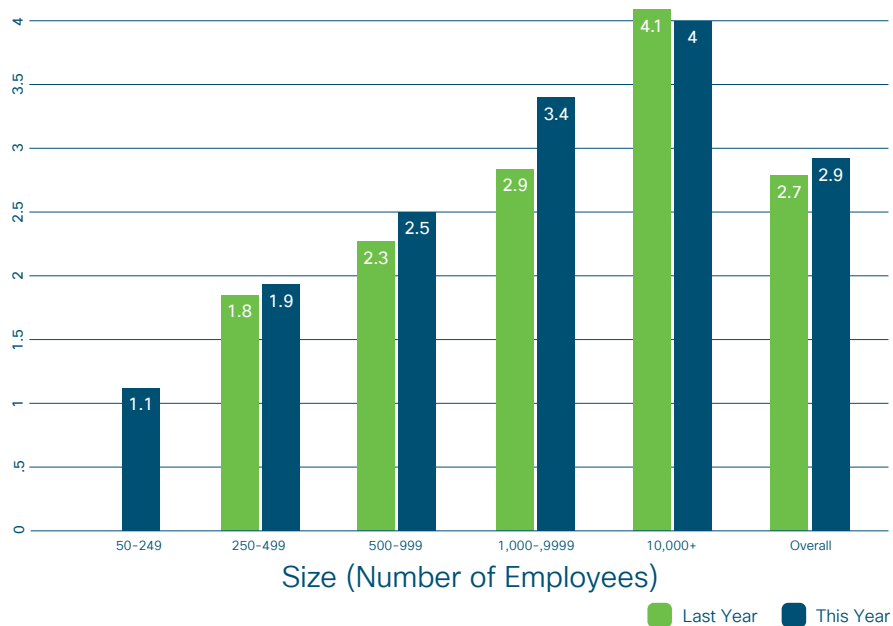
Figure 6. Percentage Getting Significant Benefits in Each Area (N=4446)



Source: Cisco Data Privacy Benchmark Study - 2021

The overall value of these benefits, based on respondents' estimates, rose 10% on average to \$2.9 million. Again, the increases were fairly consistent for different sized organizations, except for a slight decline among the largest organizations. (See Figure 7.)

Figure 7. Estimated Privacy Benefits, By Organization Size (N=3815)

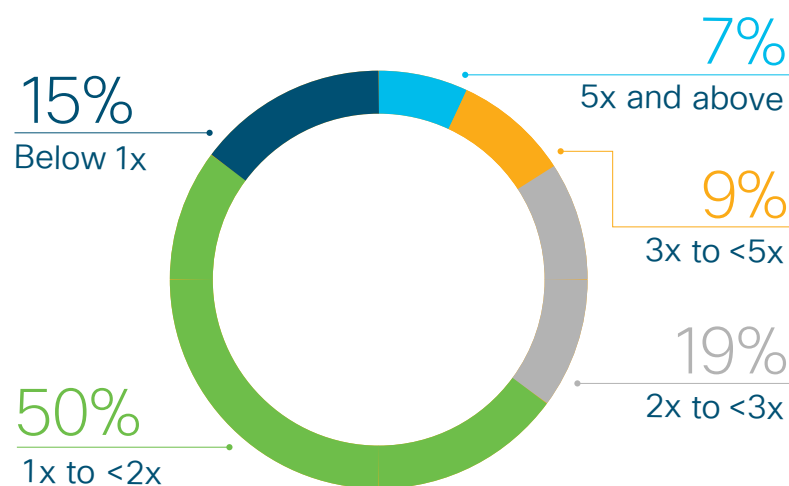


Source: Cisco Data Privacy Benchmark Study - 2021

Note: The 50-249 employee segment was not surveyed last year.

From a return-on-investment perspective, the average organization was getting benefits 1.9 times spending, which is down from 2.7 in last year's survey. We believe the higher growth in budgets is at least partially due to unanticipated needs in responding to the pandemic, adapting to new and evolving privacy legislation, responding to an increasing number of data subject access requests (DSARs), and meeting increasing customer requirements related to data localization. (In future research, we plan to explore and validate these hypotheses.) Nonetheless, most companies continue to see a very attractive return on their privacy investments. Thirty-five percent of organizations are getting benefits at least 2x spend, and only 15% feel they are not at least breaking even. (See Figure 8.)

Figure 8. Ratio of Privacy Benefits to Investment (N=3796)



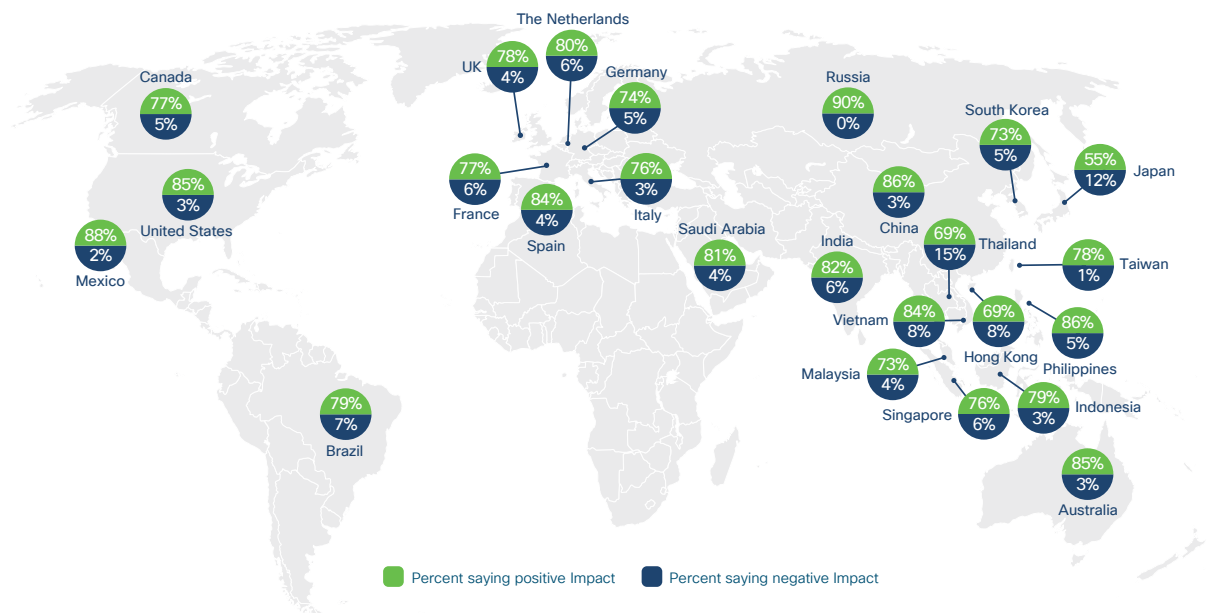
Source: Cisco Data Privacy Benchmark Study - 2021

3. Strongly Favorable Reaction to Privacy Legislation

A top concern of individuals over the past few years has been the lack of transparency when it comes to what data is being collected and how it's being used. Businesses and governments have not been as clear as they could be, and even when they try to be transparent, the complexity of the analytics, algorithms, insights, and inferences are often too complex for the general public to understand. Many consumers are now taking matters into their own hands, and nearly a third of them, which we call "Privacy Actives", already have stopped buying from a company over their data policies or practices. See **Cisco Consumer Privacy Survey**. Organizations are increasingly recognizing this challenge, and 90% of organizations in this year's Benchmark Survey said that their customers will not buy from them if they are not clear about data practices and protection.

Against this backdrop, privacy legislation has played an important role in providing assurances that governments and organizations are being held accountable for how they manage their data. More than 130 countries now have omnibus privacy legislation and many of them have been passed in the past few years. These laws are anchored around the core principles of transparency, fairness, and accountability, and for the most part, align to the OECD Privacy Guidelines¹. Most businesses and consumers see privacy regulation as an effective way to set a consistent standard baseline for data protection and to boost confidence that personal data is being treated properly. Among respondents in this benchmark survey, 79% believe privacy regulations have had a positive impact, 16% were neutral, and only 5% said that privacy laws have had a negative impact. Interestingly, this positive reaction is quite consistent across the world, including 70–90% of respondents from almost all countries represented in the survey. (See Figure 9).

Figure 9. Perceived Impact of Privacy Regulations on Organizations, by Country (N=4446)

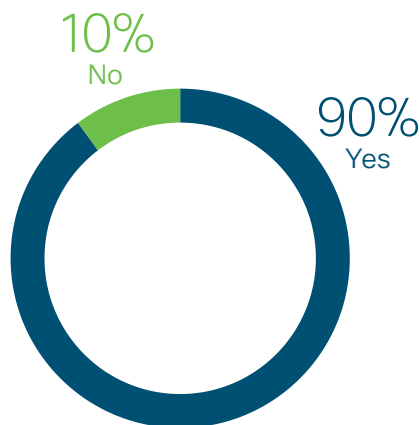


Source: Cisco Data Privacy Benchmark Study - 2021

4. External Privacy Certifications as a Critical Buying Factor

One important way for organizations to validate they are handling personal data properly is by obtaining independent, external certifications for their privacy program and practices. These include ISO 27701 (a privacy extension for ISO 27001), APEC Cross-Border Privacy Rules (demonstrating compliance with the APEC privacy framework and enabling international data transfers), and EU Binding Corporate Rules (demonstrating adherence to EU standards and enabling global data transfers). Having these certifications in place can save time and effort in contract negotiations, and they have become increasingly critical in today's business environment. When asked whether these certifications represented a buying factor when selecting a vendor or product, the vast majority (90%) said yes. (See Figure 10.)

Figure 10. External Privacy Certifications* as a Factor When Selecting a Product or Vendor (N=4446)



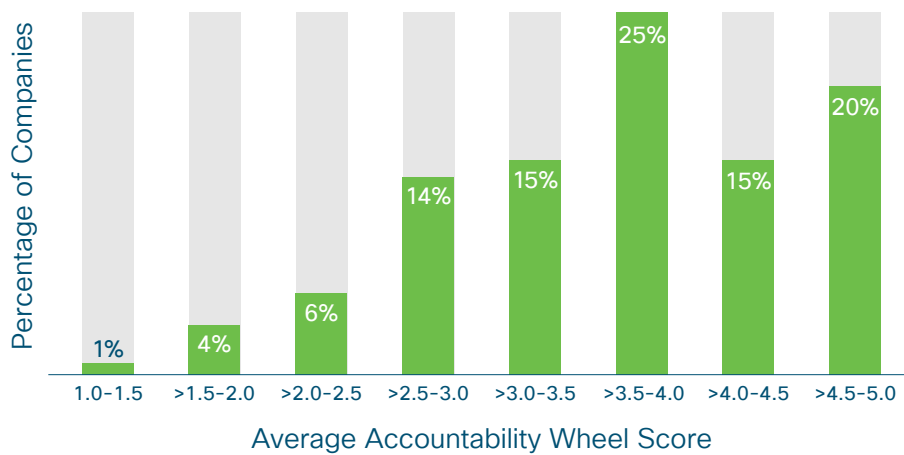
* e.g., ISO 27701, APEC Cross Border Privacy Rules, EU Binding Corporate Rules
Source: Cisco Data Privacy Benchmark Study - 2021

5. Privacy Maturity and Its Impact on Value

As in last year's survey, we asked respondents to assess their current maturity level across the seven dimensions of the "Accountability Wheel" developed by the Centre for Information Policy Leadership (CIPL)³. The overall average maturity score this year was 3.68, up slightly from 3.65 last year. Organizations continue to be widely spread in their privacy maturity, with 25% scoring 3.0 or lower, 40% scoring above 3.0 up to 4.0, and 35% scoring above 4.0. (See Figure 11.) Besides tracking the maturity increases over time, it is helpful for organizations to understand the business value associated with higher privacy maturity as they consider their own investments.

³ See Appendix 2 for diagram and scoring methodology.

Figure 11. Distribution of Accountability Wheel Scores (N=4446)

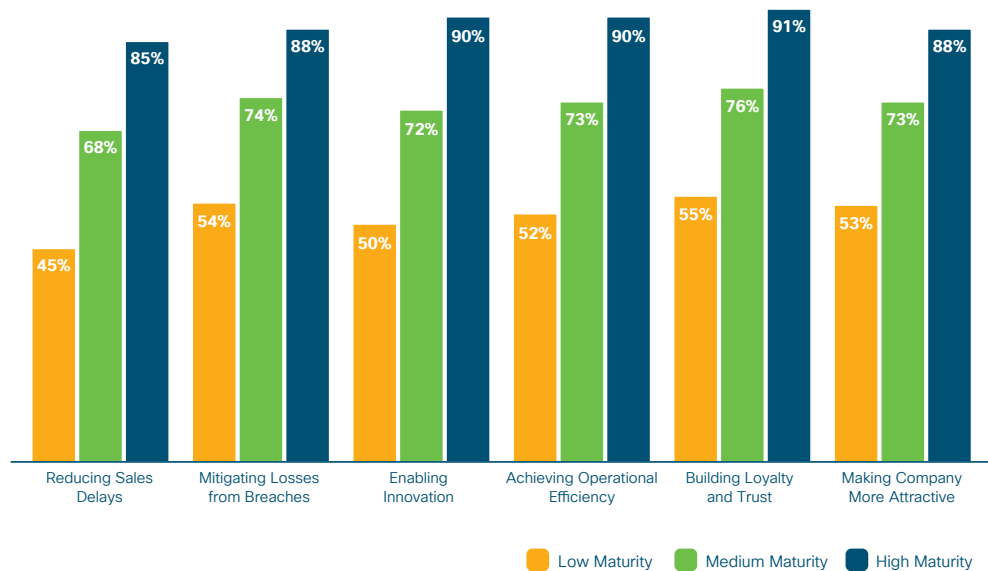


Source: Cisco Data Privacy Benchmark Study - 2020

Two of these benefits, in particular, are worth highlighting:

- (1) Organizations with more mature privacy practices are realizing much greater business benefits from privacy than those less mature. Across the six areas of benefits that we measured, 85% to 91% of mature organizations are realizing these benefits, compared with 68% to 74% of medium-maturity organizations, and only 45% to 55% of those with low maturity (See Figure 12.). The implication is that privacy investment continues to return significant value, and we expect increased investment in privacy to continue for some time.

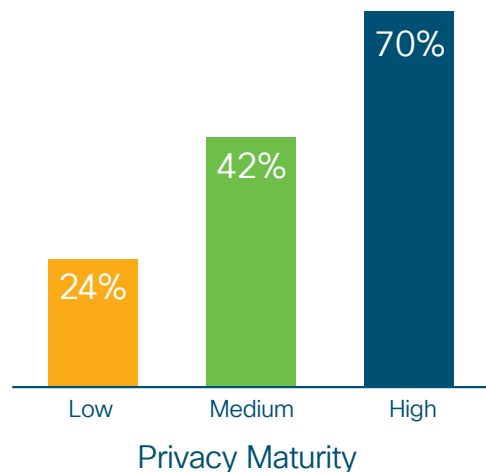
Figure 12. Percentage of Organizations Experiencing Various Business Benefits from Privacy Investments, by Maturity Level (N=4431)



Source: Cisco Data Privacy Benchmark Study - 2021

- (2) Mature privacy organizations are much better equipped to handle changing privacy requirements around the world. Seventy percent of the high-maturity organizations said they can handle these changes without undue stress, compared with 42% of the medium-maturity organizations, and only 24% of those that are low maturity. In a constantly evolving privacy environment with many new laws and regulations each year, this is a significant benefit. (See Figure 13.)

Figure 13. Percent of organizations who feel they can handle changing privacy requirements without undue stress, by maturity level (N=4431)

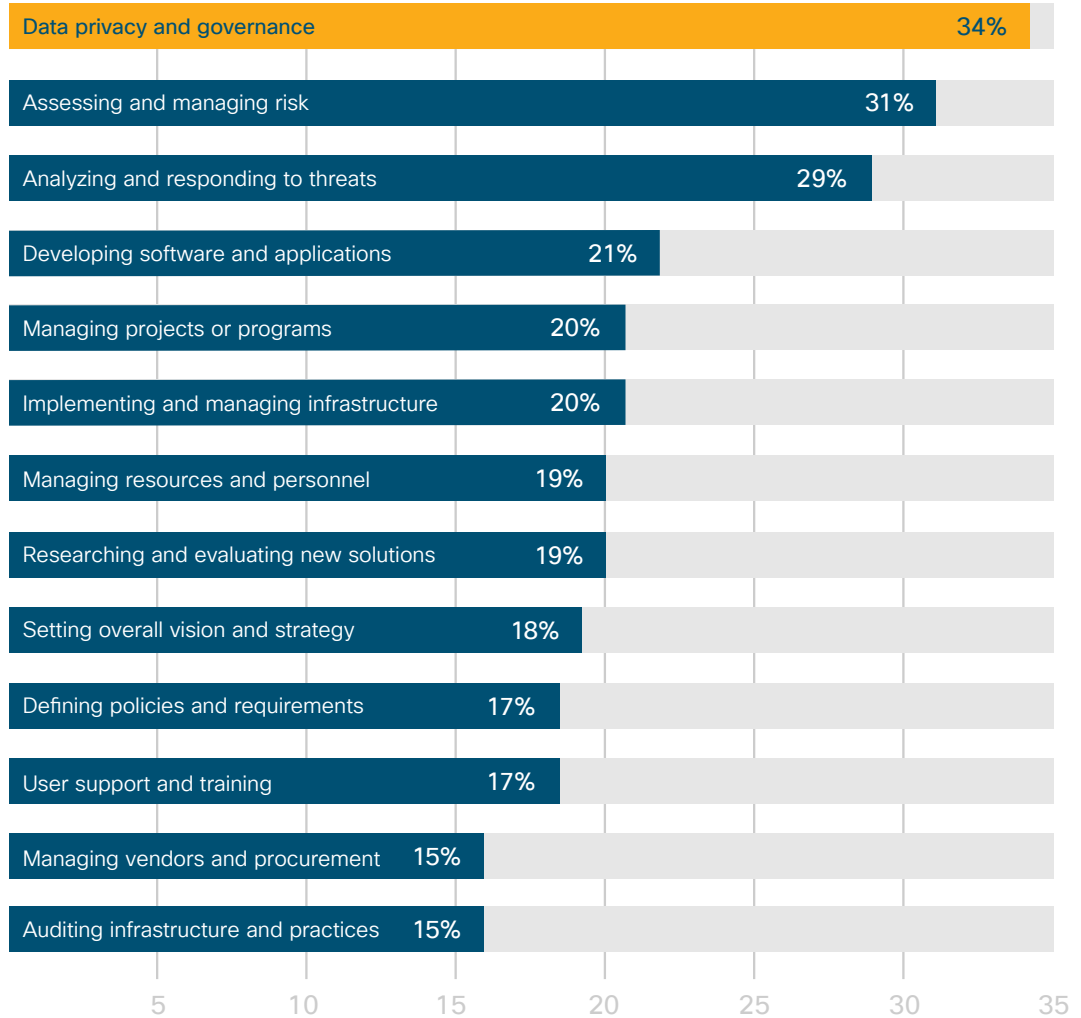


Source: Cisco Data Privacy Benchmark Study - 2021

6. Privacy – a Core Competency for Security Professionals

Organizations are working to ensure more employees are trained and knowledgeable about privacy risks and requirements, especially those who are directly responsible for an organization’s data and keeping it safe. The security professionals who completed the benchmark survey were asked to define their top 3 areas of responsibility. Remarkably, “Data privacy and governance” was selected most often (32%) by these respondents, just ahead of “Assessing and managing risk” and “Analyzing and Responding to Threats.” (See Figure 14.) Along with all the usual security functions, data privacy has become a core competency for these teams. Security teams are responsible not only for keeping unauthorized people out, but they are also increasingly partnering with privacy teams to ensure those who are authorized to have access to data handle it properly.

Figure 14. Primary Areas of Responsibility among Security Professionals
(Could choose up to three) (N=4738)

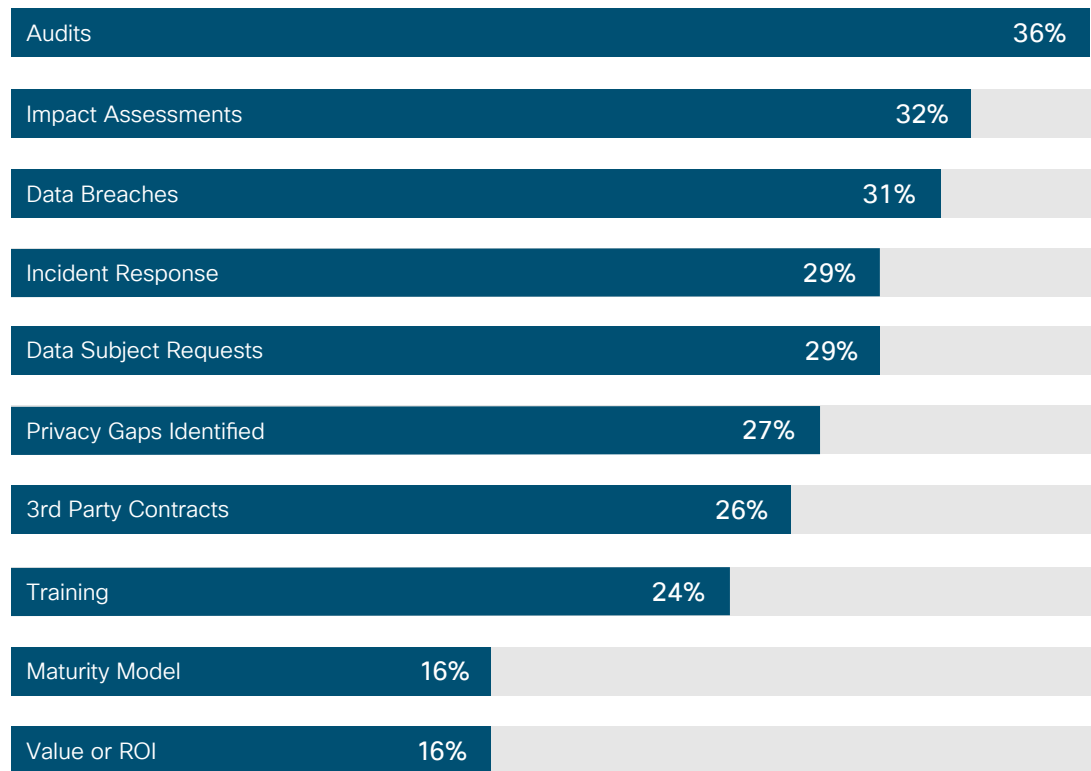


Source: Cisco Data Privacy Benchmark Study - 2021

7. Reporting Privacy Metrics to the Board

Finally, a new area in our research this year is exploring privacy metrics, especially whether privacy metrics are being reported to companies' executive management and Board of Directors, and if so, which ones. Establishing a regular cadence of metrics reporting is another indication of the importance organizations are placing on privacy and the costs, benefits, and risk it entails. Among this year's respondents, 93% of organizations are now reporting at least one privacy metric to the Board, with 14% reporting five or more privacy metrics. Among the most reported metrics are Privacy Program Audit findings (36%), Privacy Impact Assessments (32%), and Data Breaches (31%). (See Figure 15.)

Figure 15. Privacy Metrics Reported to Board of Directors (N=4446)



Source: Cisco Data Privacy Benchmark Study - 2021



Conclusion

The pandemic brought with it a compelling societal need for sensitive personal information – health, contacts, and location. This need put the individual’s fundamental right to privacy at risk and forced a balancing between individual rights and public safety. Instead of pushing privacy aside, organizations and individuals turned to privacy teams to help them navigate their pandemic response and ensure privacy’s principles continue to be respected while using sensitive data to serve the public good.

Privacy budgets are higher, privacy certifications have become more critical, and privacy laws around the world have been very well-received. Privacy skills and expertise have become a core competency, and privacy is now a Board-level issue. Investing in privacy is not only enhancing customer trust in an uncertain world, but it is also delivering significant business value. Privacy is much more than just a compliance obligation, it’s a fundamental human right and business imperative.

In future research, Cisco will continue to monitor these trends and issues for the benefit of our customers, privacy leaders, and other stakeholders. For additional information about Cisco’s privacy research, please contact **Robert Waitman, Director of Privacy Research and Economics at Cisco**, at rwaitman@cisco.com.

A person's legs and feet are visible at the top of the page, walking on a floor with a world map pattern. The person is wearing dark trousers and black shoes. The floor is light-colored with dark outlines of continents. The background is a blurred, high-angle shot of the person walking.

About the Cybersecurity Report Series

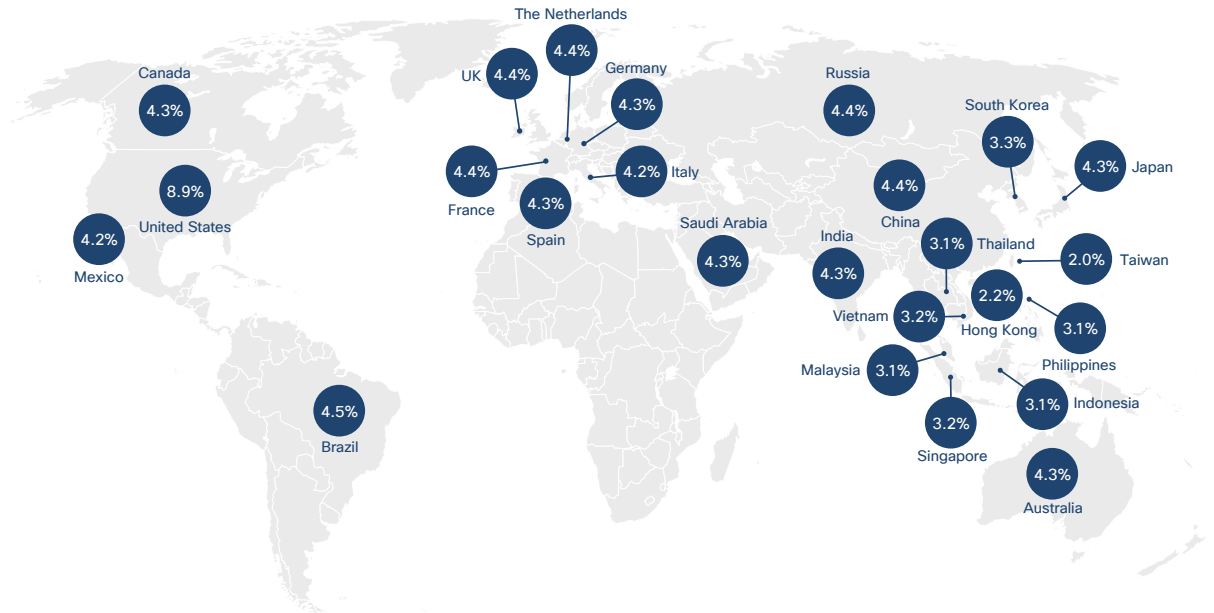
Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as 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 publications under the banner Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security and privacy 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 2020 series included the Security Outcomes Study, Future of Secure Remote Work Report, Simplify to Secure Cybersecurity Report, and CISO Benchmark Report. For more information, and to access all the reports and archived copies, visit www.cisco.com/go/securityreports.

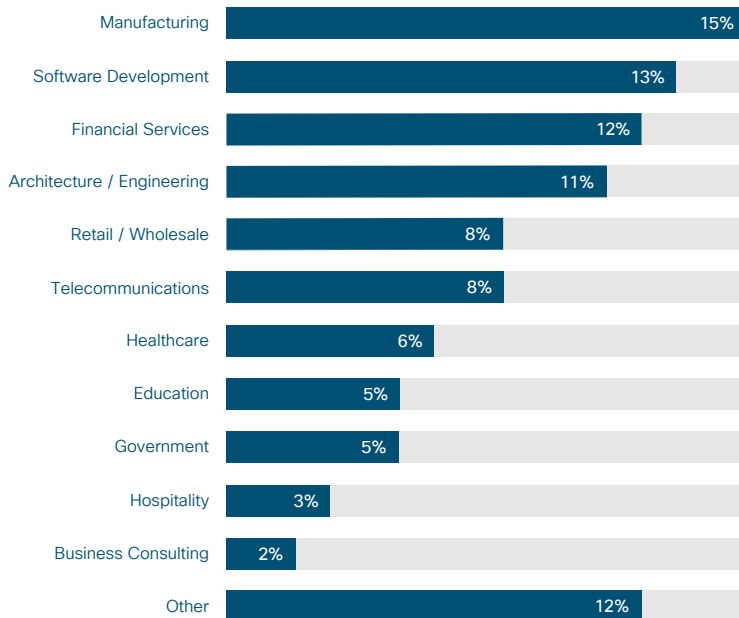
Appendix 1: Demographic information on survey respondents

By Country / Geography



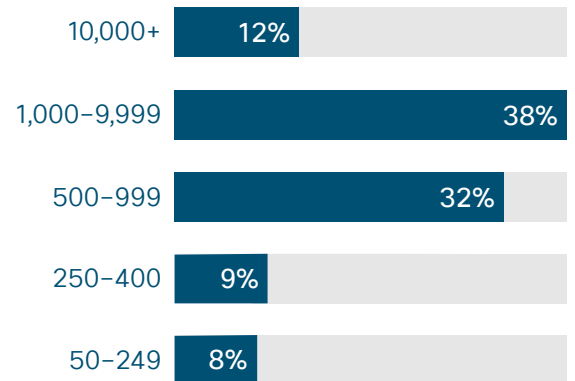
Source: Cisco Data Privacy Benchmark Study - 2021

By Industry



Source: Cisco Data Privacy Benchmark Study - 2021

By Company Size (# Employees)



Source: Cisco Data Privacy Benchmark Study - 2021

Appendix 2: CIPL Accountability Wheel and Scoring Scale



Scoring scale:

- 1 We have little in place
- 2 We are working on it and have made some progress
- 3 We have made significant progress, but we still have a substantial way to go
- 4 We have a majority of this in place
- 5 We have all or nearly all in place

Source: Cisco Data Privacy Benchmark Study - 2021
Centre for Information Policy Leadership (CIPL)

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 2021

RPT_01_2021

© 2021 Cisco and/or its affiliates. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (2062922)





CISCO SECURE