CISCO CYBERSECURITY SERIES 2020 • DATA PRIVACY
JANUARY 2020

From Privacy to Profit: Achieving Positive Returns on Privacy Investments

Cisco Data Privacy Benchmark Study 2020

cisco

Contents

Introduction 3

Key Findings 3

Survey Methodology 3

Results: Achieving Positive Returns on Privacy Investments 4

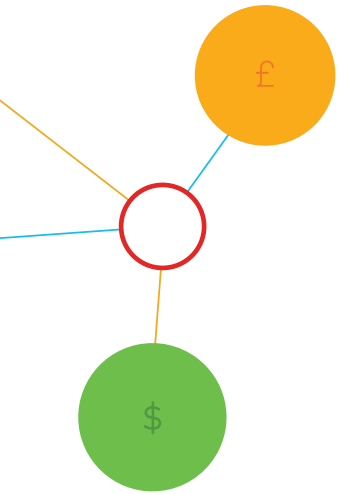
1. Privacy Spending, Benefits, and Returns 4
2. Measuring and Valuing Privacy Accountability 8
3. Multiyear Results on Privacy's Business Benefits, Sales Delays, and GDPR Readiness 11
4. Value of Privacy Certifications in the Buying Process 12

Conclusion: The Business Case for Privacy 13

About the Cisco Cybersecurity Series 14

Introduction

Over the past few years, data privacy has evolved from "nice to have" to a business imperative and critical boardroom issue. Today, people are asking more questions about how their personal data is used, and they now view privacy as an important component of a company's brand (see the Cisco 2019 Consumer Privacy Survey). Privacy regulations like the EU's General Data Protection Regulation (GDPR) have raised awareness and enforcement of privacy, and this is compelling organizations to better manage and protect personal data to avoid significant fines and penalties.



More than 40% of organizations are seeing benefits at least twice that of their privacy spend.

Meanwhile, data breaches continue to expose the personal information of millions, and consumers struggle to understand how to protect themselves. Over the last three years, Cisco has conducted privacy research by surveying thousands of organizations worldwide. Our research has demonstrated that – beyond meeting compliance requirements – good privacy is indeed good for business and individuals.

Key Findings

In this year's survey we further explore and quantify privacy spending and benefits to determine the ROI for privacy, assess the impact of organizations' privacy accountability, and consider the importance of privacy certifications in the vendor selection process. Here are some of the key findings:

- Most organizations are seeing very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend.
- Using the "Accountability Wheel" created by the Centre for Information Policy Leadership (CIPL), we found strong correlations between organizations' privacy accountability and lower breach costs, shorter sales delays, and higher financial returns.
- The percentage of organizations saying they receive significant business benefits from privacy (e.g., operational efficiency, agility, and innovation) has grown to over 70%.
- The vast majority (82%) of organizations view privacy certifications such as ISO 27701 and Privacy Shield as a buying factor when selecting a product or vendor in their supply chain.

The findings in this report provide strong evidence that privacy has become an attractive investment even beyond any compliance requirements. Organizations that get privacy right improve their customer relationships, operational efficiency, and bottom-line results.

Survey Methodology

The data in this report is derived from the Cisco Annual Cybersecurity Benchmark Study, a double-blind survey of 2800 security professionals in 13 countries.[1] Survey respondents represent all major industries and a mix of company sizes. We directed privacy-specific questions to the more than 2500 respondents who stated they are familiar with the privacy processes at their organizations.

[1] Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Mexico, Spain, the UK, and the U.S.

Results: Achieving Positive Returns on Privacy Investments

1. Privacy Spending, Benefits, and Returns

To develop a baseline understanding of companies' privacy investments, we asked respondents about the size of their total annual spending on privacy. For all respondents, the average annual privacy spend was US$1.2 million, and it varies significantly by size of company.

Among large enterprises (10,000 or more employees), average spend was $1.9 million, and 2% of these enterprises spent more than $5 million. On the other end of the spectrum, the average privacy spend of small businesses (250–499 employees) was $800,000, and 41% of them spent less than $500,000. (See Figure 1.)

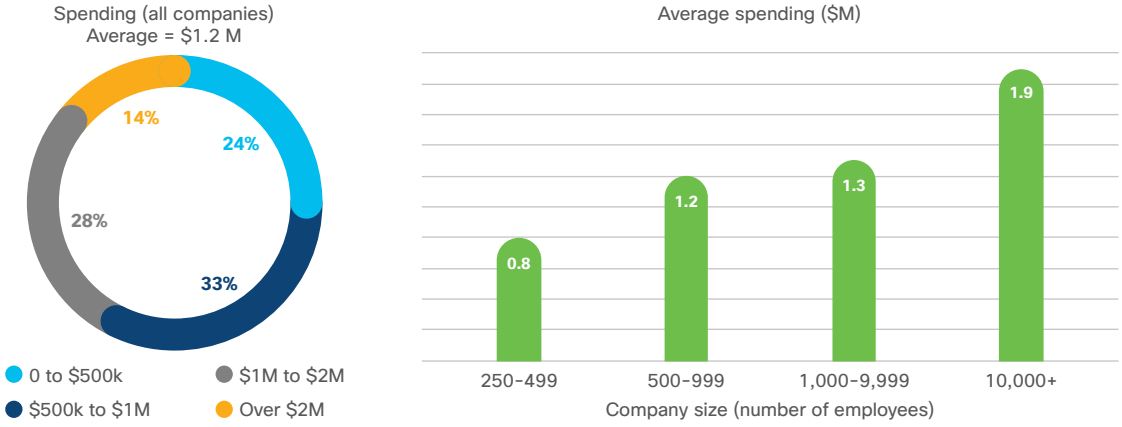
For some time, privacy regulation has been an important driver of companies' efforts to protect their personal data, and avoiding fines and penalties is certainly one motivator. However, based on conversations with customers and our privacy research over the past three years, we believe that **even greater value comes from business benefits beyond compliance.**

To assess this value, we asked respondents what types of benefits (if any) they are seeing in areas such as operational efficiency, fewer and less costly data breaches, reduced sales delays, improved customer loyalty and trust, and so on. **A large majority (generally more than 70%) indicated they are seeing "significant" or "very significant" benefits in each of these areas.** (See Figure 2.)

Figure 2 Business impact of privacy
Percentage of companies getting significant benefits in each area, N=2549

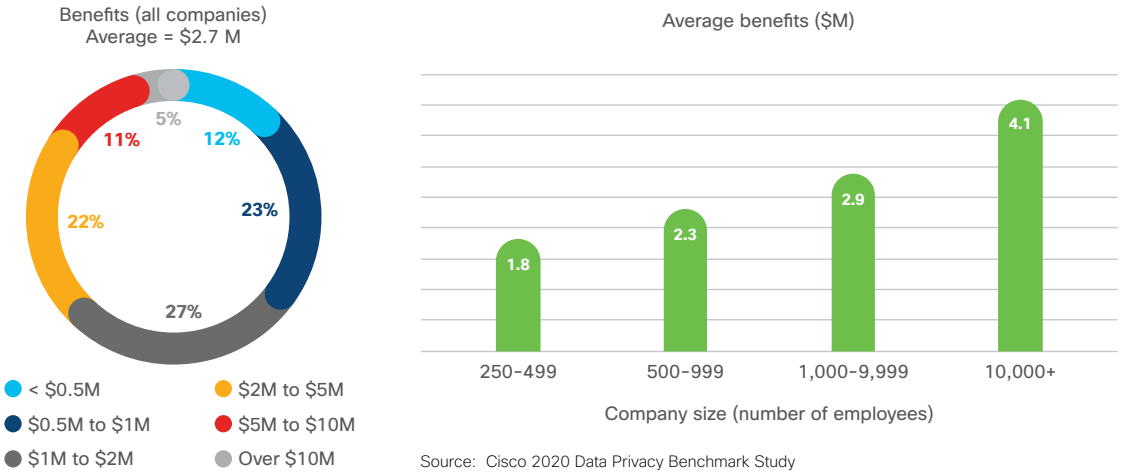
Source: Cisco 2020 Data Privacy Benchmark Study

Figure 1 Annual privacy spending overall and by company size
N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

Figure 3 Estimated privacy benefits overall and by company size
N=2549



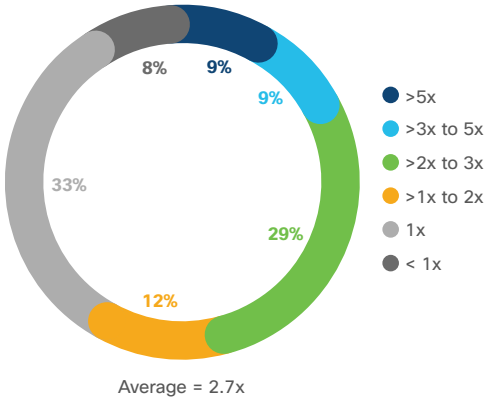
Source: Cisco 2020 Data Privacy Benchmark Study

For every $1 of investment, the average company received $2.70 of benefit.

We also asked respondents to provide their best estimate of the financial impact of these benefits (in ranges such as $500,000 to $1 million). Across all companies in the survey, the **average estimated benefit was $2.7 million.** Large enterprises (10,000 or more employees) estimated their benefits at $4.1 million, and 17% placed the value at more than $10 million. Small businesses (250–499 employees) estimated their benefits at $1.8 million. (See Figure 3.)

Combining data on privacy investment and benefits, we have developed initial estimates for companies' return on their privacy spending. Across all respondents, the average ratio of benefits to spend was 2.7, meaning that **for every dollar of investment, the company received $2.70 worth of benefit.** Nearly half (47%) of the companies are seeing greater than a twofold return, 33% are breaking even, and only 8% appear to be spending more than they receive back in benefits. (See Figure 4.)

Figure 4 Distributions of privacy returns, percent of respondents
N=2543



Source: Cisco 2020 Data Privacy Benchmark Study

"It is a business imperative and competitive advantage for companies, their boards, and senior leaders to embrace accountability and transparency in how they manage personal data."

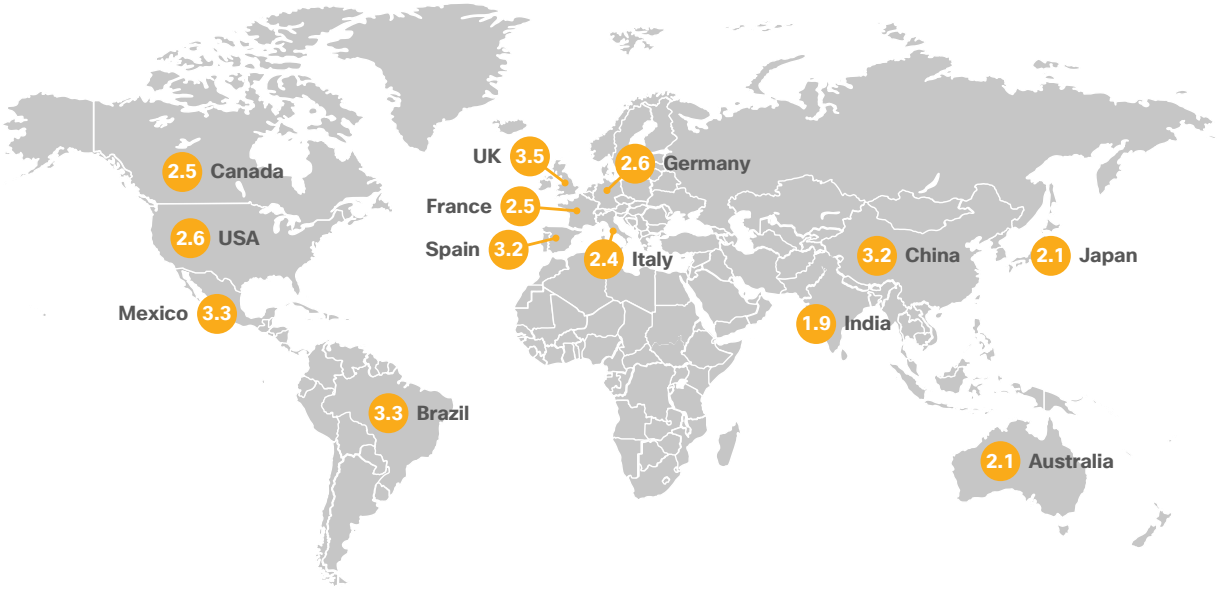
Bojana Bellamy
President, Centre for Information Policy Leadership (CIPL)

Interestingly, the average return on privacy investment varies significantly by country, with the highest average returns located in the UK (3.5x), Brazil (3.3x), and Mexico (3.3x). (See Figure 5.)

Note that returns did not vary significantly by size of company. Larger companies are spending more and receiving more benefits, but the ratio of benefits to spending is similar for large, midsize, and small companies.

To our knowledge, this study is one of the first to estimate privacy returns for companies on a global scale. While survey responses are inherently imprecise, we believe these findings – drawing on data from thousands of companies – provide very useful information for organizations working to understand their own returns and prioritize their privacy investments.

Figure 5 Average privacy returns by country
Global average: Benefits = 2.7 times investment
N=2543



Source: Cisco 2020 Data Privacy Benchmark Study

"This study provides empirical evidence that investment in privacy creates business value."

Harvey Jang
Vice President, Chief Privacy Officer, Cisco

33% of organizations scored above 4.0 on accountability.

2. Measuring and Valuing Privacy Accountability

Over the past two decades, the principle of "accountability" has emerged as a critical theme in global privacy law, policies, and practices. According to this principle, organizations must be accountable for implementing applicable privacy and data protection requirements, and they must be able to demonstrate their compliance capabilities. The Centre for Information Policy Leadership (CIPL) has worked with regulators and business leaders to develop the CIPL "Accountability Wheel", a framework for helping organizations build, manage, assess, and adapt their privacy program.[2] To better understand where organizations stand today, we asked survey respondents to evaluate their progress on each of the seven elements of the "Accountability Wheel" on a scale of 1 (very little in place) to 5 (all or most in place). (See Figure 6.)

While the variation in scores across the seven accountability elements was small, the variation across companies was quite significant. The overall average score was 3.65 for all organizations, but 25% of them scored 3.0 or less, 41% scored between 3.0 and 4.0, and 33% scored over 4.0. (See Figure 7.)

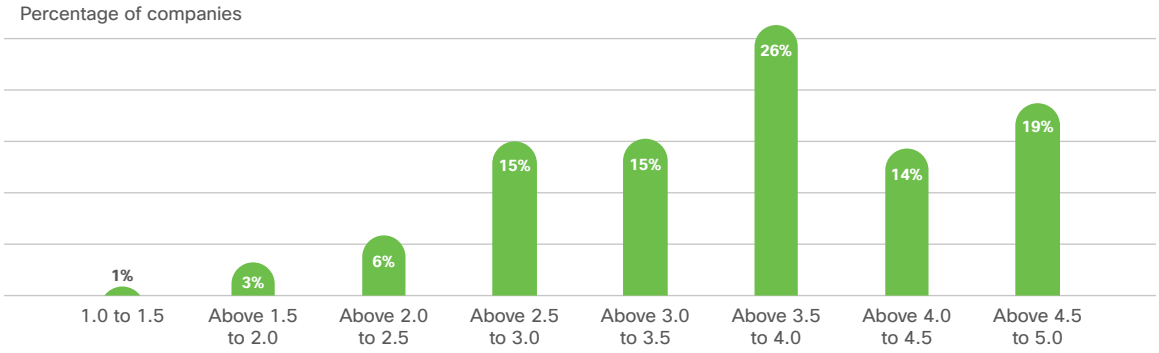
Figure 6 CIPL Accountability Wheel

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 2020 Data Privacy Benchmark Study; Centre for Information Policy Leadership (CIPL)

Figure 7 Distribution of Accountability Wheel scores
N=2549



Note: The bars do not add to 100% due to rounding.

Source: Cisco 2020 Data Privacy Benchmark Study

[2] The Centre for Information Policy Leadership is a global privacy and security policy think-tank based in Brussels, Washington, and London. It works with industry leaders, regulatory authorities, and policy makers to help frame and advance privacy and cybersecurity policy, law, and practice. (www.informationpolicycentre.com)

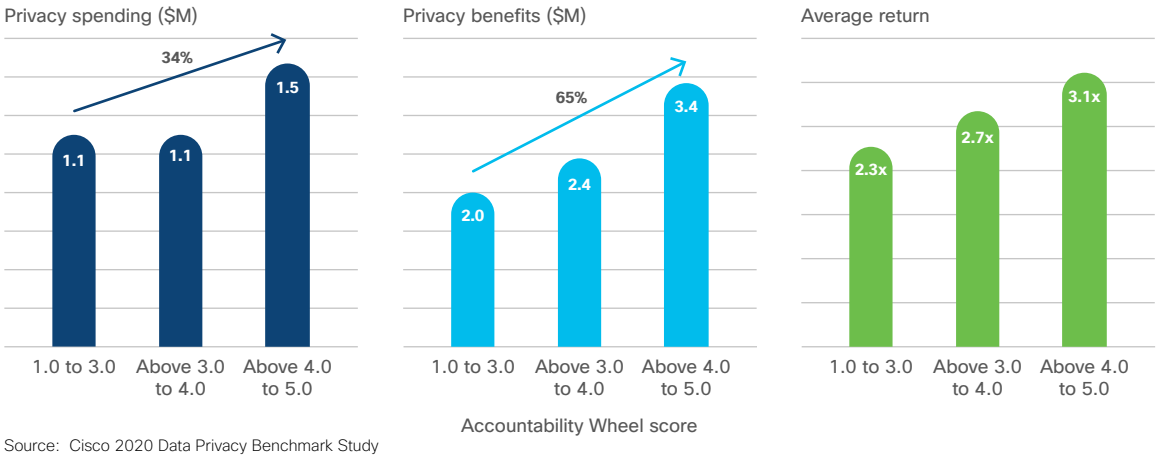
Higher levels of privacy accountability provide very large returns.

Our analysis reveals that companies having higher Accountability Wheel scores also have greater privacy-related benefits such as higher investment returns, fewer and less costly breaches, and shorter sales delays.

Returns on privacy investment

We analyzed correlations between accountability scores and the returns on privacy investment. High accountability organizations spend somewhat more annually on their privacy programs ($1.5 million) compared to the low accountability group ($1.1 million). But these organizations also saw much greater average benefits ($3.4 million vs. $2.0 million). This translates to an overall privacy return of 3.1x for high accountability organizations, 2.7x for the middle group, and 2.3x for the low accountability organizations. **The implication is that achieving higher levels of privacy accountability requires additional investment, but this investment provides very large returns.** (See Figure 8.)

Figure 8 Spending, benefits, and returns by Accountability Wheel score
N=2543



Source: Cisco 2020 Data Privacy Benchmark Study

> **"Privacy and accountability are central to our data-driven innovation, and have become key differentiators for our brand. This research reinforces the fact that privacy is a critical investment for forward-looking companies."**
>
> Caroline Louveaux
> Chief Privacy Officer, Mastercard

High accountability organizations had less downtime from breaches, fewer records impacted, and lower breach costs.

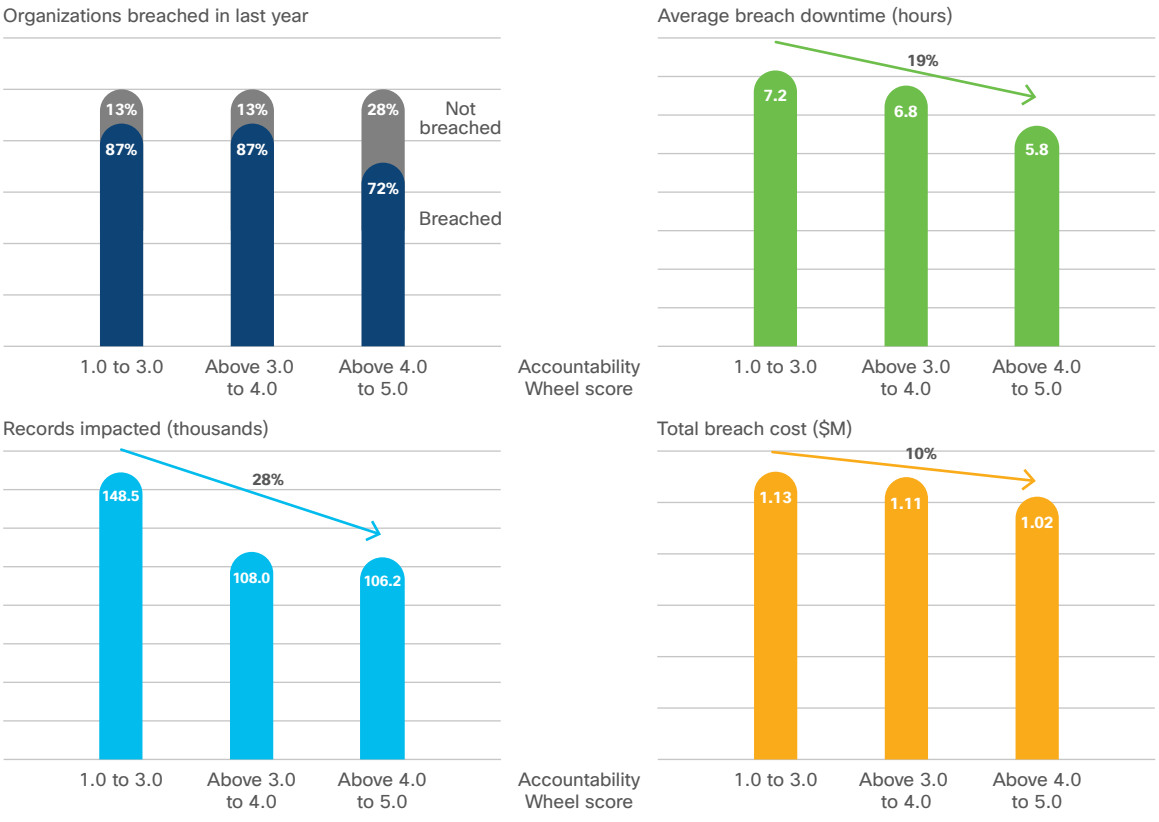
Breaches and costs of breach

Among organizations with accountability scores of 4.0 or less, 13% experienced no data breaches last year. Organizations with scores above 4.0, however, were over twice as likely to be breach-free (28%). In addition, the impact and costs of a breach were significantly lower for these high accountability organizations. They had 19% less downtime from breaches, 28% fewer records impacted by a breach, and 10% lower breach costs. **Having mature and accountable processes to manage, control, and curate data seems to help organizations avoid and/or limit the impact of data breaches.** (See Figure 9.)

Privacy-related sales delays

In terms of sales delays, the story is similar. Organizations scoring high (above 4.0) in accountability averaged only 3.6 weeks of delay, compared with 3.9 weeks for the middle accountability group and 5.5 weeks for the low accountability group. This translates to a 35% reduction in average sales delays, enabling organizations to better protect themselves and ensure a more reliable revenue stream.

Figure 9 Breach and breach implications by Accountability Wheel score
N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

3. Multiyear Results on Privacy's Business Benefits, Sales Delays, and GDPR Readiness

This study marks the third year that Cisco has researched the progress and impact of privacy on organizations worldwide. It is therefore interesting to track year-over-year changes in key privacy metrics.

70% of respondents are getting business benefits as a result of privacy efforts – including competitive advantage, agility, and improved company attractiveness.

Privacy business benefits

One of the primary themes of past annual privacy benchmark surveys has been the growing number of organizations that recognize the business benefits of privacy beyond compliance requirements. In last year's survey, we found that approximately 40% of respondents recognized various benefits from privacy investment including competitive advantage, organizational agility, and improved company attractiveness to investors. In this year's survey, **the percentage has increased dramatically, and 70% of respondents are getting business benefits in each of these areas.**

Sales delays

Sales delays related to customer privacy concerns have fluctuated over the last three years, both in the number of companies experiencing delays and in their length. These delays are typically caused when customers want to know what data is captured in a company's product or service, how the data is stored and transferred, who has access to it, and so on. Two years ago, we reported that 65% of organizations had sales delays related to privacy. This increased to 87% last year and dropped to 62% this year. We believe the increase last year was primarily due to GDPR becoming enforceable, which caused vendors to grapple with customer expectations and requirements related to the new regulation. The average delay was 4.2 weeks in this year's survey, which is similar to the 3.9 weeks we reported last year. Over time, we would expect both the percentages and average delays to drop as companies develop more mature processes to handle customers' questions and integrate privacy processes into their sales cycles.

GDPR readiness

Since GDPR became enforceable in May 2018, we have monitored organizations' progress with GDPR readiness. Among respondents in this year's survey, 55% said they are now ready for GDPR, 29% said they will be ready within a year, 12% expect to be ready in more than a year, and 3% said GDPR does not apply to them.

These results are nearly identical to the results in last year's study, perhaps implying that organizations have not made significant progress with GDPR readiness since last year. However, we believe the more likely explanation is that organizations view GDPR requirements as an ongoing business and operational process. Those that thought they still had work to do last year probably feel the same way this year.

Interestingly, the percentage of firms saying GDPR does not apply to them remained low at 3%, so most survey respondents around the world recognize the importance of complying with this EU-based regulation.

Privacy certifications represent a buying factor for 82% of organizations worldwide.

4. Value of Privacy Certifications in the Buying Process

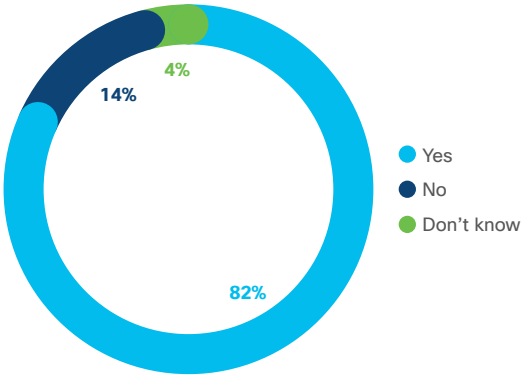
Many organizations have explored obtaining certifications that provide external validation for their privacy programs and practices. Among these are ISO 27701 (a privacy extension for ISO 27001), EU/Swiss-U.S. Privacy Shield (a legal mechanism for transferring data to the U.S.), APEC Cross-Border Privacy 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 intracompany data transfers).

According to our survey respondents, external validation has become very important in today's business environment. When asked whether **these certifications represented a buying factor when selecting a vendor or product, the vast majority (82%) responded affirmatively.** (See Figure 10.)

By country, the highest percentages were in Brazil (95%), India (95%), and China (94%). But even in the countries with the lowest percentages (e.g., Canada), roughly two-thirds of organizations still agreed.

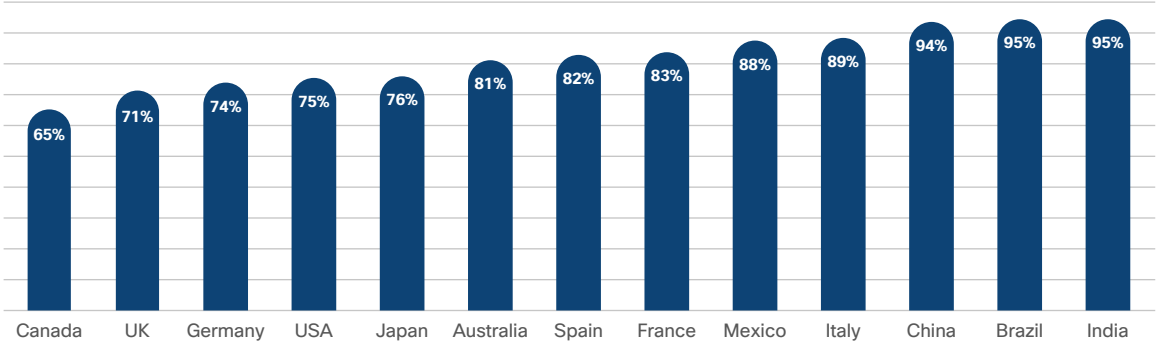
Given this environment, it appears that achieving one or more of these certifications is a very positive investment for firms to consider. (See Figure 11.)

Figure 10 Importance of privacy certifications as buying factor
N= 2549



Source: Cisco 2020 Data Privacy Benchmark Study

Figure 11 Importance of privacy certifications
Percentage agreeing that certifications are a buying factor, by country, N = 2549



Source: Cisco 2020 Data Privacy Benchmark Study

Conclusion: The Business Case for Privacy

This research quantifies the business value associated with organizations' privacy investments. Going beyond the benefits initially identified in our 2018 and 2019 Data Privacy Benchmark Studies, **we have now calculated an ROI for privacy, and we have shown that most organizations are getting a very positive return on their privacy investments.** We have also measured their progress using the CIPL Accountability Wheel and found a strong connection between higher accountability and higher business benefits. Finally, we found external validation and privacy certifications to be an important factor in vendor selection and buying decisions.

Future research will explore how these investments, benefits, and returns might change over time in response to evolving privacy regulations and customer expectations worldwide. Cisco will continue to work with our customers and other privacy leaders to enable better protection for customers' personal data, enhanced decision-making on privacy investments, and improved customer trust.

For additional information about Cisco's privacy research, please contact Robert Waitman, Director of Privacy Insights & Innovation at Cisco, at rwaitman@cisco.com.

About the Cisco Cybersecurity 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.

Cisco Security is now 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 each year's series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others published throughout each year.

For more information, and to access all the reports and archived copies, visit: 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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published January 2020 PRIV_09_0120