CISCO CYBERSECURITY SERIES 2019 • DATA PRIVACY
JANUARY 2019

Maximizing the value of your data privacy investments

Data Privacy Benchmark Study

CISCO

Executive Summary

The EU's General Data Protection Regulation (GDPR) became enforceable on May 25, 2018, and privacy laws and regulations around the globe continue to evolve and expand.

Customers are asking more questions during the buying cycle about how their data is captured, used, transferred, shared, stored, and destroyed.

Most organizations have invested, and continue to invest, in people, processes, technology, and policies to meet customer privacy requirements and avoid significant fines and other penalties. In addition, data breaches continue to expose the personal information of millions of people, and organizations are concerned about the products they buy, services they use, people they employ, and with whom they partner and do business with generally. As a result, customers are asking more questions during the buying cycle about how their data is captured, used, transferred, shared, stored, and destroyed. In last year's study (Cisco 2018 Privacy Maturity Benchmark Study), Cisco introduced data and insights regarding how these privacy concerns were negatively impacting the buying cycle and timelines. This year's research updates those findings and explores the benefits associated with privacy investment.

Cisco's Data Privacy Benchmark Study utilizes data from Cisco's Annual Cybersecurity Benchmark Study, a double-blind survey completed by more than 3200 security professionals in 18 countries and across all major industries and geographic regions. Many of the privacy specific questions were addressed to more than 2900 respondents who were familiar with the privacy processes at their organizations. Participants were asked about their readiness for GDPR, any delays in the sales cycle due to customer data privacy concerns, losses from data breaches, and their current practices related to maximizing the value of their data.

The findings from this study provide strong evidence that organizations are benefitting from their privacy investments beyond compliance. Organizations that are ready for GDPR are experiencing shorter delays in their sales cycle related to customers' data privacy concerns than those that are not ready for GDPR. GDPR-ready organizations have also experienced fewer data breaches, and when breaches have occurred, fewer records were impacted, and system downtime was shorter. As a result, the total cost of data breaches was less than what organizations not ready for GDPR experienced. Even though companies have focused their efforts on meeting privacy regulations and requirements, nearly all companies say they are receiving other business benefits from these investments beyond compliance. These privacy-related benefits are providing competitive advantages to organizations, and this study can help guide investment decisions as organizations work to mature their privacy processes.

> **"Privacy is such a vital ingredient to organizational success, both to protect data and foster innovation."**
>
> **John N. Stewart, Senior Vice-President and Chief Security and Trust Officer, Cisco**

“This research provides evidence for something Privacy professionals have long understood – that organizations are benefitting from their privacy investments beyond compliance. The Cisco study demonstrates that strong privacy compliance shortens the sales cycle and increases customer trust.”

Peter Lefkowitz, Chief Digital Risk Officer,
Citrix Systems and 2018 Board Chairman,
International Association of Privacy Professionals (IAPP)

The Results

59% of companies report they are meeting all or most of GDPR's requirements today, with another 29% expecting to get there within a year. The top challenges to getting ready for GDPR were identified as data security, employee training, and keeping up with the evolving regulations.

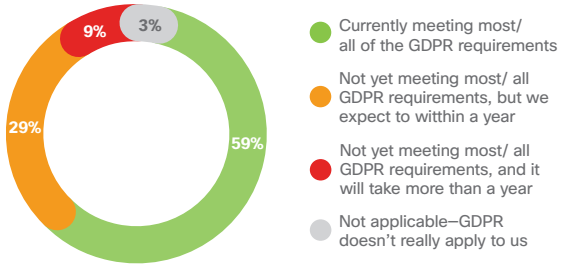
GDPR readiness

Among all respondents in the Data Privacy Benchmark Study, 59% indicated they are meeting all or most of GDPR's requirements today. (See Figure 1) Another 29% said they expect to be GDPR ready within a year, leaving 9% who said it would take more than a year to get ready. While GDPR applies to businesses located in the EU or to the processing of personal data collected about individuals located in the EU, it is interesting that only 3% of the respondents in our global survey indicated that they did not believe GDPR applied to their organization.

Only 3% of the respondents in our global survey indicated that they did not believe GDPR applied to their organization.

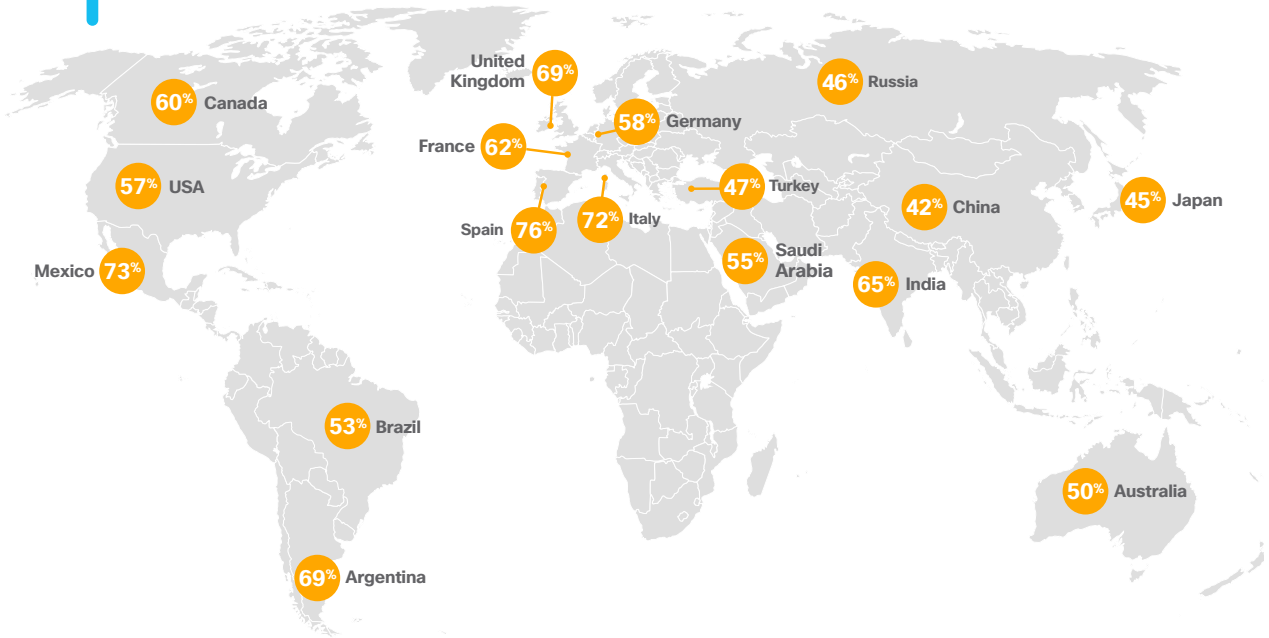
By country, the level of GDPR-readiness ranged from 42% to 76%. (See Figure 2) The European countries in the survey (Spain, Italy, UK, France, Germany) were, not surprisingly, generally on the higher end of the range.

Figure 1 GDPR readiness
Percent of respondents, N=3206



Source: Cisco 2019 Data Privacy Benchmark Study, n=3206

Figure 2 GDPR readiness by country
Percent of respondents, N=3206



Source: Cisco 2019 Data Privacy Benchmark Study

Respondents were asked to identify the most significant challenges their organizations faced in getting ready for GDPR. The top responses were data security, internal training, evolving regulations, and Privacy by Design requirements. (See Figure 3)

Figure 3 Most significant challenges in getting ready for GDPR
Percent of respondents, N=3098

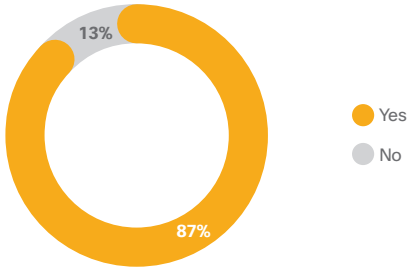
42%	Meeting data security requirements
39%	Internal training
35%	Staying on top of the ever-evolving developments as the regulation matures
34%	Complying with Privacy By Design Requirements
34%	Meeting data subject access requests
31%	Cataloging and inventorying our data
30%	Enabling data deletion requests
29%	Hiring/identifying Data Protection Officers for each relevant geography
28%	Vendor management

Source: Cisco 2019 Data Privacy Benchmark Study

Sales delays due to privacy

Respondents were asked whether they are experiencing delays in their sales cycles due to customers' data privacy concerns. 87% of respondents said they do have sales delays, whether from existing customers or prospects. (See Figure 4) This is significantly higher than the 66% of respondents who reported sales delays in last year's survey and is likely due to the increased awareness of the importance of data privacy, GDPR becoming enforceable, and the emergence of other privacy laws and requirements. Data privacy has become a board-level issue for many organizations, and customers are making sure their vendors and business partners have adequate answers to their privacy concerns before doing business together.

Figure 4 Respondents experiencing delays in their sales cycles due to customers' data privacy concerns
Percent of respondents, N=2064



Source: Cisco 2019 Data Privacy Benchmark Study

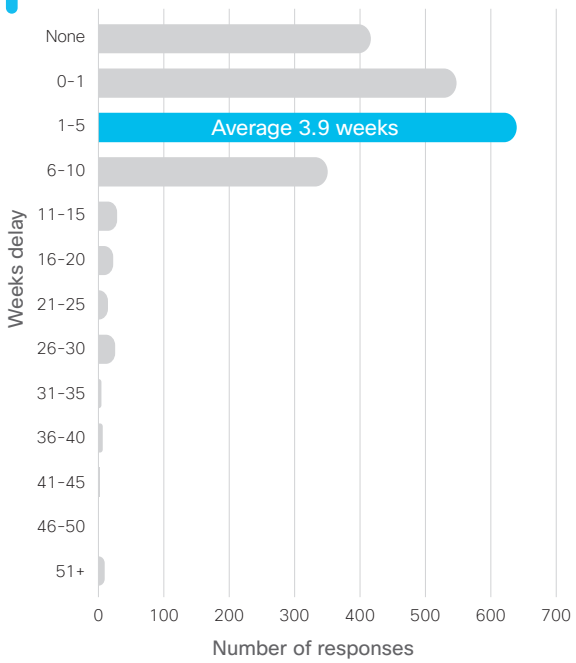
When asked about the length of the delay, the estimates varied widely. The average delay for sales to existing customers was 3.9 weeks, and over 94% of organizations reported delays between 0 and 10 weeks. Nonetheless, there were some organizations reporting delays up to 25 to 50 weeks or more. (See Figure 5) Note that the average delay for sales to prospects was 4.7 weeks, perhaps reflecting the longer timeframes needed to adequately address privacy concerns in a new potential customer relationship. These average delays

Sales delays due to customer data privacy concerns continue to be an issue for most organizations.

87% reported they have delays in selling to existing customers or prospects, which is up significantly from last year.

for both existing customers and prospects are significantly shorter than the average of 7.8 weeks reported in last year's survey, perhaps reflecting the fact that firms have become better equipped over the last year to answer customer's privacy concerns.

Figure 5 Delays in answering customers' data privacy concerns
Percent of respondents, N=2081



Source: Cisco 2019 Data Privacy Benchmark Study

By country, the distribution of sales delays for existing customers ranged from 2.2 weeks to 5.5 weeks. Longer delays can usually be found where privacy requirements are high or in a state of transition, as organizations work to adapt to the concerns raised by their customers. (See Figure 6)

The top reasons for privacy-related sales delays:

- *investigating specific customer requests*
- *translating privacy information into the customer's language*
- *educating the customer about the company's privacy practices or processes*
- *having to redesign the product to meet the customer's privacy requirements*

Figure 6 Country break-down of distribution of sales delays
Percent of respondents, N=2081

Country	Avg delay (weeks)
Argentina	3.9
Australia	3.9
Brazil	5.2
Canada	5.1
China	3.5
France	4.2
Germany	3.1
India	4.9
Italy	2.6
Japan	4.1
Mexico	2.9
Russia	2.5
Saudi Arabia	4.8
Spain	5.5
Turkey	2.2
United Kingdom	4.9
United States	3.7
Overall	3.9

Source: Cisco 2019 Data Privacy Benchmark Study

Sales delays, at a minimum, cause revenue to be deferred for some period of time. This can lead to missed revenue targets, impacting compensation, funding decisions, and investor relations. In addition, delayed sales can often turn into lost sales, for instance when delays cause a potential customer to buy a competitor's product or not buy the product or service at all.

Respondents were also asked to identify the reasons for any privacy-related sales delays at their organizations. The top responses included the need to investigate specific customer requests, translating privacy information into the customer's language, educating the customer about the company's privacy practices or processes, or having to redesign the product to meet the customer's privacy requirements. (See Figure 7)

Figure 7 Reasons for sales delays
Percent of respondents, N=1812

49%	We need to investigate specific/unusual requirements for the customer/prospect before they felt comfortable with our privacy practices.
42%	We need to translate information about our privacy policies/processes into the customer's / prospect's language.
39%	The customer/prospect needs to lean more about our privacy policies or processes.
38%	Our product or service needs to be redesigned to meet the customer's/prospect's privacy requirements.
33%	We are unable or unwilling to meet the customer's/prospect's privacy requirements (e.g., data breach policies, data deletion requirements).
28%	It takes time to find the right person or team to respond to the customer's/prospect's questions.
17%	We have to resolve questions as to which party is ultimately accountable or liable for the data.
5%	We have to involve our lawyers to clarify uncertainty regarding the law.

Source: Cisco 2019 Data Privacy Benchmark Study

Business benefits of privacy investments

Organizations that have invested in getting ready for GDPR have done so primarily to avoid the significant fines and other penalties associated with not meeting the regulation. However, as the research indicates, there are other significant business benefits associated w ith these privacy investments.

In looking at the sales delays due to privacy issues, the average delay for selling to existing customers was 3.9 weeks. However, those organizations which reported they are meeting all or most of GDPR's requirements had an average sales delay of 3.4 weeks, compared to 4.5 weeks for organizations which aren't yet ready but expect to be within a year, and 5.4 weeks for those organizations that are over a year away from being GDPR ready. Thus, the least prepared organizations have average delays that are nearly 60% longer than those who are most prepared. (See Figure 8)

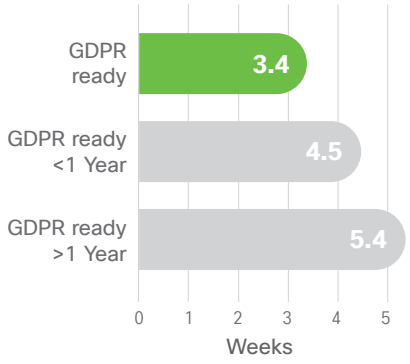
While a majority of companies reported having a data breach in the last year, a lower percentage (74%) of the GDPR-ready companies were impacted, compared to 80% of the organizations less than a year from GDPR readiness and 89% of those that are farthest from being GDPR ready.

Summary of key findings

GDPR-ready companies are benefitting from their privacy investments beyond compliance in a number of tangible ways. They had **shorter sales delays** due to customer's privacy concerns (3.4 weeks vs. 5.4 weeks). They were **less likely to have experienced a breach in the last year** (74% vs. 89%), and when a breach occurred, **fewer data records were impacted** (79k vs. 212k records) and **system downtime was shorter** (6.4 hours vs. 9.4 hours). As a result, the **overall costs associated with these breaches were lower**; only 37% of GDPR-ready companies had a loss of over $500,000 last year vs. 64% of the least GDPR ready.

These results highlight that privacy maturity has become an important **competitive advantage for many companies**. Organizations should work to maximize the business benefits of their privacy investments, which may go beyond the requirements of any particular privacy regulation.

Figure 8 Average weeks delay (existing)
Percent of respondents, N=2081



Source: Cisco 2019 Data Privacy Benchmark Study

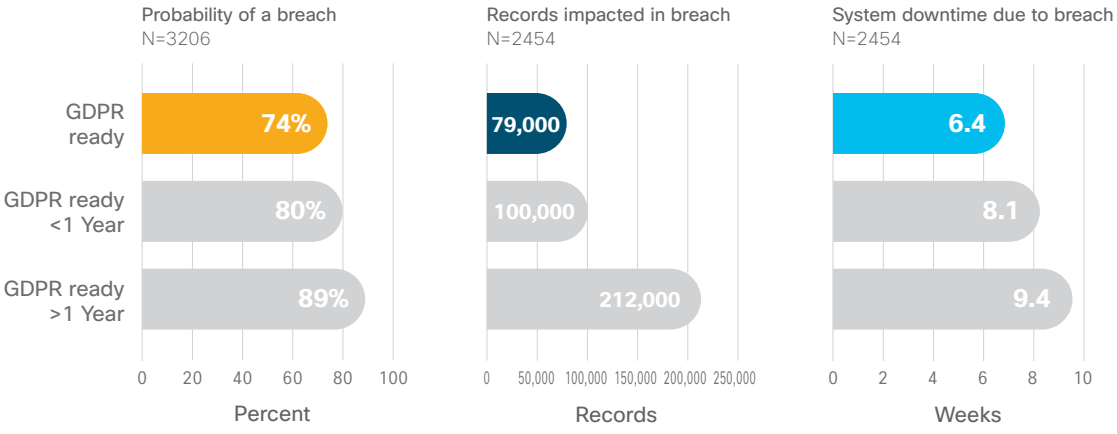
"Organizations have a long way to go to maximize the value of their privacy investments. Our research shows that the market is set and ready for those willing to invest in data assets and privacy may be the path forward to get there."

Michelle Dennedy, Chief Privacy Officer, Cisco

Another tangible benefit from GDPR-readiness is that it appears to lower the frequency and impact of data breaches. GDPR requires organizations to know where there personally identifiable information (PII) is located and provide appropriate protections for this data. These efforts may have helped organizations better understand their data, the risks associated with their data, and to establish or strengthen protections for that data.

While most companies reported having a data breach in the last year, a lower percentage (74%) of the GDPR-ready companies were impacted, compared to 80% of the organizations less than a year from GDPR readiness and 89% of those that are farthest from being GDPR ready. (See Figure 9)

Figure 9 Business benefits of privacy investments



Source: Cisco 2019 Data Privacy Benchmark Study

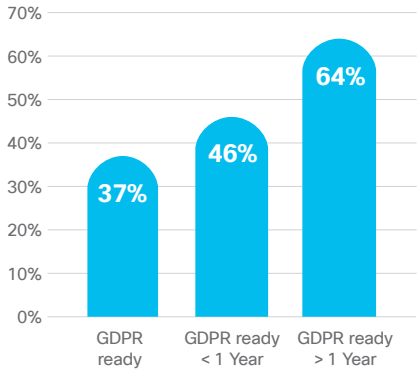
Nearly all companies (97%) report they are receiving auxiliary benefits today from their privacy investments – including agility / innovation, competitive advantage, operational efficiency, mitigating losses from breaches, reducing sales delays, and gaining appeal with investors.

Furthermore, once a breach occurred, the GDPR-ready companies experienced a smaller impact. The average number of records impacted was 79,000 for these companies versus 212,000 for those that are least ready for GDPR (see Figure 9)

GDPR-ready companies also experienced shorter system downtimes associated with the breach, perhaps connected again to better management of their data assets. GDPR-ready companies had an average system downtime of 6.4 hours versus 9.4 hours for organizations least ready for GDPR. (See Figure 9)

With fewer records impacted and shorter downtimes, it is not surprising that the GDPR-ready companies experienced lower overall costs associated with data breaches. Only 37% of these companies had losses from data breaches totaling at least $500,000, compared to 64% of those companies least prepared for GDPR (See Figure 10)

Figure 10 Probability of data breach loss of $500k
Percent of respondents, N=3206



Source: Cisco 2019 Data Privacy Benchmark Study

With fewer records impacted and shorter downtimes, it is not surprising that the GDPR-ready companies experienced lower overall costs associated with data breaches.

Organizations recognizing the benefits of privacy investment

The previous two sections of this study highlighted the correlations between privacy investments and business benefits, such as shorter sales delays and fewer and less costly data breaches. It is interesting to note that most respondents are now recognizing many of these benefits. When asked whether privacy investment was yielding benefits (such as greater agility and innovation, gaining a competitive advantage, achieving operational efficiency, etc.), 75% of all respondents identified two or more of these benefits and nearly all companies (97%) identified at least one benefit. (See Figure 11)

Figure 11 Benefits of privacy investments
Percent of respondents, N=3259

42%	Enabling agility and innovation from having appropriate data controls.
41%	Gaining competitive advantage versus other organizations.
41%	Achieving operational efficiency from having data organized and catalogued.
39%	Mitigating losses from data breaches.
37%	Reducing any sales delays due to privacy concerns from customers/prospects.
36%	Gaining appeal with investors.
3%	None of the above.

Source: Cisco 2019 Data Privacy Benchmark Study

Organizations reporting they are meeting all or most of GDPR's requirements had an average sales delay of 3.4 weeks.

Maximizing the value of data

Data privacy is one critical aspect of an organization's overall effort to maximize the value of its data assets over the data's lifecycle. Like any other asset, data should be efficiently acquired, stored, protected, utilized, and archived/deleted. Organizations that maximize the value of their data in appropriate ways can benefit greatly by building trust with customers and using well-protected and curated data to enhance the customer experience and drive greater value for all stakeholders.

Respondents in this survey were asked about a range of behaviors typically found in mature data environments, such as having a complete data catalog, connecting data to other assets, hiring a chief data officer, and monetizing the data externally. (See Figure 12) Fewer than one-half of the survey respondents exhibited each of these characteristics, and this will be an area for further research to better understand how organizations are maximizing the value of their data assets.

Implications

These results highlight that privacy investment has created business value far beyond compliance and has become an important competitive advantage for many companies. Organizations should therefore work to understand the implications of their privacy investments, including reducing delays in their sales cycle and lowering the risk and costs associated with data breaches as well as other potential benefits like agility/innovation, competitive advantage, and operational efficiency. The analysis and insights from this survey can serve as a framework and starting point for each organization to maximize the value from its privacy investments.

Figure 12 Behaviors typically found in mature data environments.
Percent of respondents, N=3259

42%	We understand the value of most/all of our data assets.
42%	We know where most/all of the Personally Identifiable Information (PII) is located and how it is used.
40%	We are effective in connecting different data assets together to create more value for our customers and ourselves.
37%	We have a relatively complete catalog of our data assets.
32%	We have a chief data officer.
32%	We consider ourselves an information-centric company.
30%	We are able to monetize selected data assets by selling (or bartering) them externally.
2%	None of the above.

Source: Cisco 2019 Data Privacy Benchmark Study

Organizations that maximize the value of their data in appropriate ways can benefit greatly by building trust with customers and using well-protected and curated data to enhance the customer experience and drive greater value for all stakeholders.

“A good corporate privacy policy can shield firms from the financial harm posed by a data breach – by offering customers transparency and control over their personal information – while a flawed policy can exacerbate the problems caused by a breach.”

Harvard Business Review, “A Strong Privacy Policy Can Save Your Company Millions”, Feb. 15, 2018

Conclusion

Privacy investment has created business value far beyond compliance and has become an important competitive advantage for many companies.

This research has quantified a number of business benefits connected to privacy maturity. Many of the benefits initially identified in last year's report have been confirmed and explored more fully, including reducing privacy-related sales delays and reducing the frequency and impact of data breaches. In future research, we'll explore how these benefits are changing over time, especially as privacy regulations and customer expectations continue to evolve in different industries and different geographies. Cisco will continue to work with our customers and other leaders in the privacy field to provide information for better investment decision-making and improved trust with our customers.

For more information, see:
https://cisco.com/go/dataprivacy

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 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 our 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 in threat researchers and innovators in the security industry, the collection of reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report and the CISO Benchmark Study, with others to come throughout the year.

For more information, 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,

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 2019 PRIV_01_0119_r1