Cisco 2018
Privacy Maturity Benchmark Study

Good privacy is good for business

The General Data Protection Regulation (GDPR) will become fully enforceable on May 25, 2018. Many organizations are rightly investing in resources and processes to meet the GDPR standards and avoid significant fines and other penalties. In addition, the many data breaches that exposed the personal information of millions of customers have made organizations increasingly concerned about the products they buy and with whom they partner. Customers are asking more questions during the buying cycle about how data is captured, transferred, stored, and deleted. In this study, Cisco shares insights on how data privacy concerns are impacting the buying cycle.

The Cisco 2018 Privacy Maturity Benchmark Study was created in conjunction with Cisco's Annual Cybersecurity Benchmark Study, a double-blind survey completed by more than 3600 security professional in 25 countries and across all major industries. The privacy specific questions focused on a subset of nearly 3000 respondents who were familiar with the privacy processes at their organizations. Participants were asked about the makeup of their privacy teams, maturity level of their privacy processes, and the impact (if any) they experienced related to delays in the sales cycle due to customer data privacy concerns. We also analyzed responses to other questions regarding cyber events to understand which organizations had been breached in the last year and the size of any losses from these events.

The findings from the Privacy Maturity Benchmark Study have clarified the importance of having good privacy processes well beyond GDPR compliance and have enabled the quantification of some of the financial benefits. In particular, privacy-mature organizations are experiencing shorter delays in their sales cycle due to customer data privacy issues. They are also experiencing lower losses associated with data breaches. This suggests that organizations should assess their own privacy maturity levels and understand potential financial opportunities from additional benefits in privacy processes.

Summary of key findings:

- Sales delays due to data privacy concerns are widespread and significant in length. 65 percent of organizations reported that they have delays in their sales cycle, and among all respondents, the average sales delay was 7.8 weeks.
- The sales delays varied by country and industry. The longest delays by country occurred in Latin America and Mexico, and by industry in the government and healthcare sectors.
- Notably, the average sales delay was highly correlated with the privacy maturity level of the organization. Privacy-immature companies are experiencing an average 16.8 weeks of delay, compared to just 3.4 weeks for privacy-mature companies.
- Sales delays also varied significantly by the organizational model adopted for the privacy resources. A hybrid model, which has a mix of centralized and decentralized privacy resources, had shorter delays (4.6 weeks), compared to models with fully centralized (9.8 weeks) or decentralized resources (7.1 weeks).
- The level of privacy maturity also correlated with the likelihood and costs of data breaches. 74 percent of privacy-immature companies experienced a cyber loss of over $500,000 in the last year, compared to only 39 percent of privacy-mature companies.

Sales delays due to privacy

Among all respondents in the Privacy Maturity Benchmark Study, 65 percent indicated they are experiencing sales delays due to data privacy issues (See Figure 1). When asked about the length of the delay, the estimates varied widely. The average delay was 7.8 weeks, and over 90 percent of organizations reported delays between zero and 20 weeks. Interestingly, there were a significant number of organizations reporting delays of up to 50 to 100 weeks (See Figure 2).

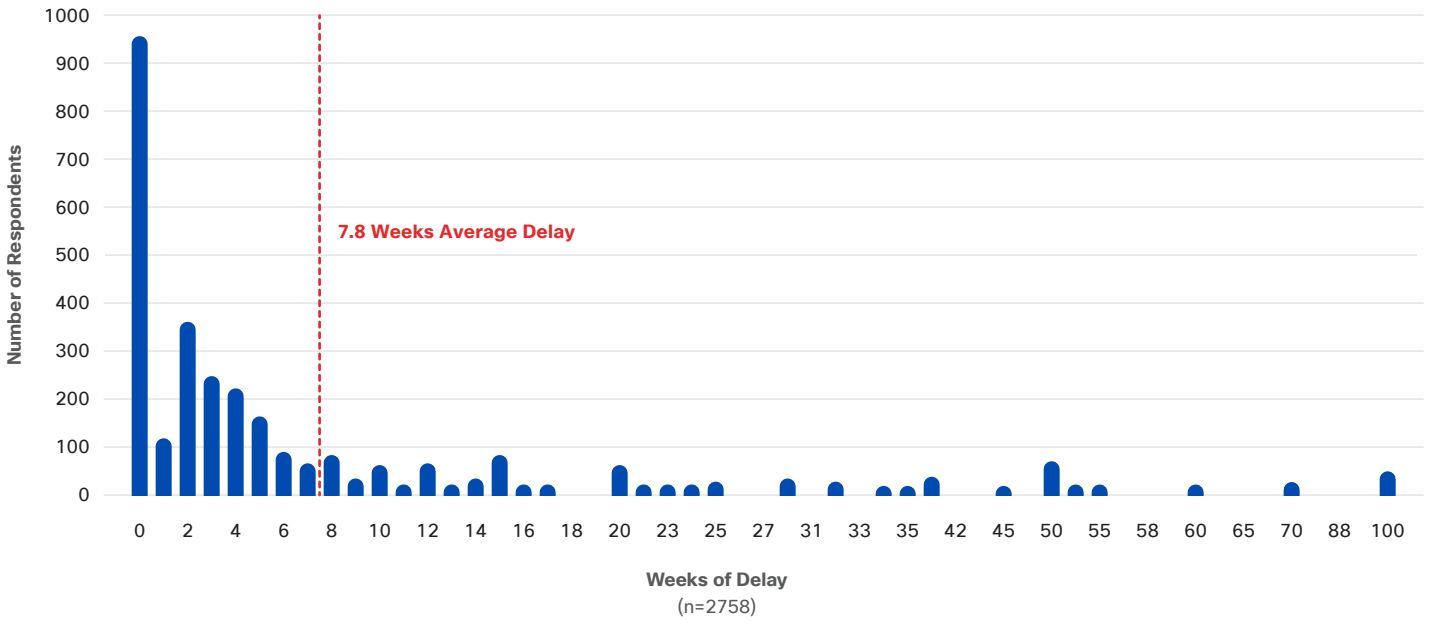
Sales delays, at a minimum, cause revenue to be deferred for some period of time. However, sales delays can often lead to lost revenue as well. As a product or service approaches the end of its lifecycle, a delayed sale may become a lost sale. Delays may also cause customers to select a competitor's product or even to move on to other priorities and not buy the product or service at all.

Figure 1 Sales delays due to data privacy issues

65% have delays in sales due to data privacy issues

Source: Cisco 2018 Privacy Maturity Benchmark Study

Figure 2 Length of sales delays due to data privacy issues



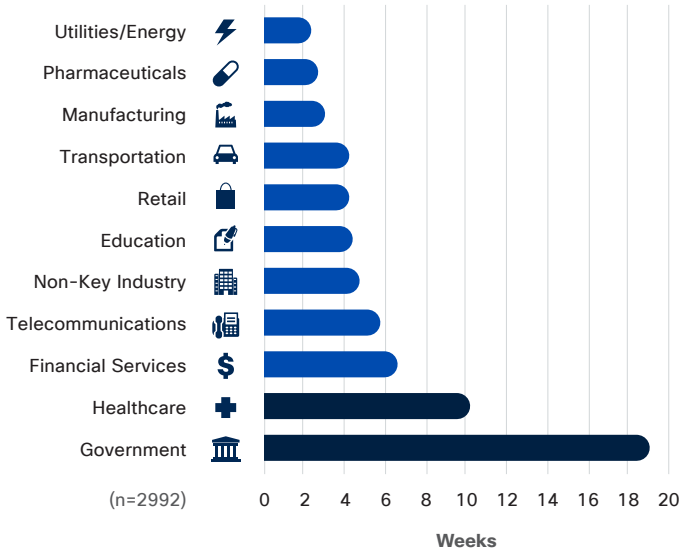
Source: Cisco 2018 Privacy Maturity Benchmark Study

Sales delays by geography and industry

There was significant variation in average sales delays reported by geography and industry. Longer delays are likely associated with countries or industries where privacy regulations and customer privacy expectations are high, as well as where existing regulations or expectations may have increased recently. The study shows the longest sales delays were seen in Latin America (15.4 weeks), Mexico (13.0 weeks), and Japan (12.1 weeks), and the shortest delays were reported in China (2.8 weeks) and Russia (3.3 weeks). See Figure 3 below.

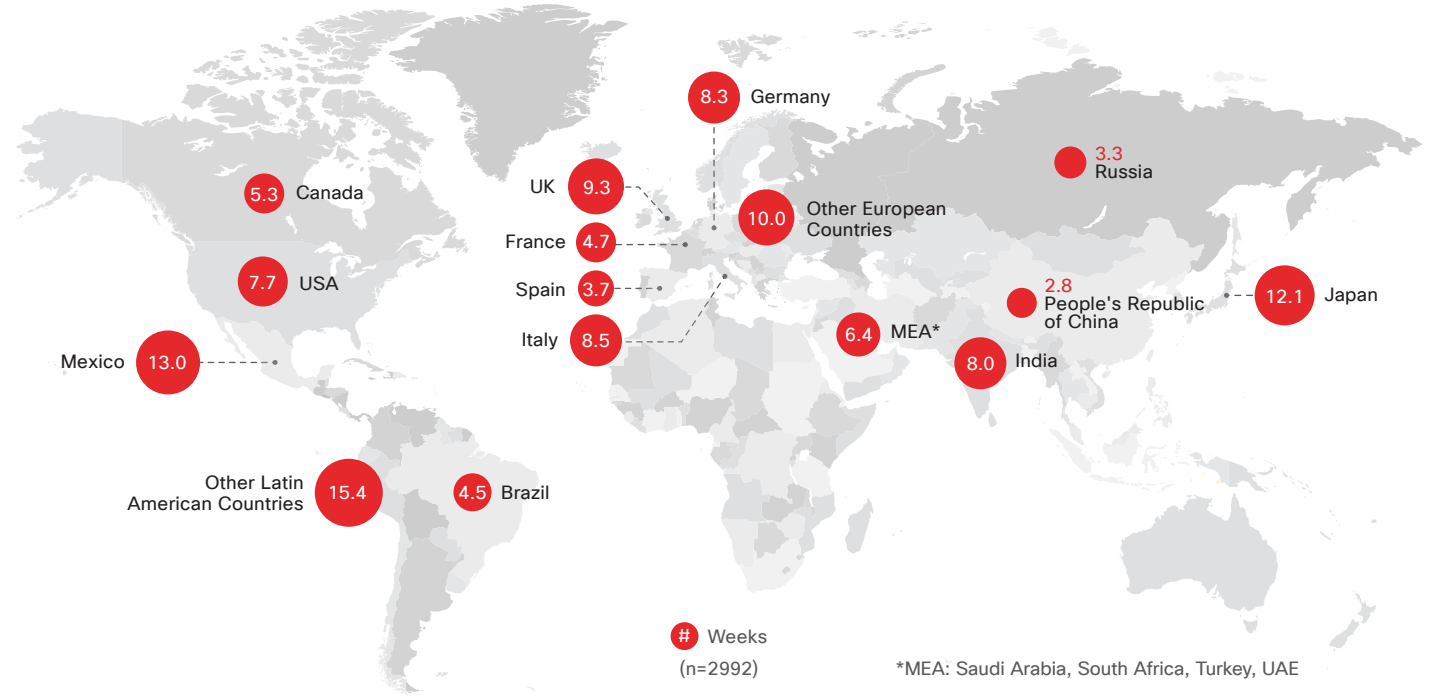
By industry, companies in the government and healthcare sectors had the highest delays, given the stricter standards and the highly confidential nature of the data. Conversely, industries with relatively less Personally Identifiable Information (PII), such as utilities and pharmaceuticals, had the shortest average delays (See Figure 4).

Figure 4 Average sales delay by industry



Source: Cisco Security Research

Figure 3 Average sales delay by country



Source: Cisco 2018 Privacy Maturity Benchmark Study

Privacy maturity and sales delays

Respondents were asked to assess the current maturity level of their privacy processes, according to the standard model developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) . This model defines five maturity states: (1) Ad hoc, (2) Repeatable, (3) Defined, (4) Managed, and (5) Optimized (See sidebar). Respondents selected the maturity level that most closely matched the current situation at their organization. Overall, roughly one fifth of the organizations identified themselves in each of the five maturity levels.

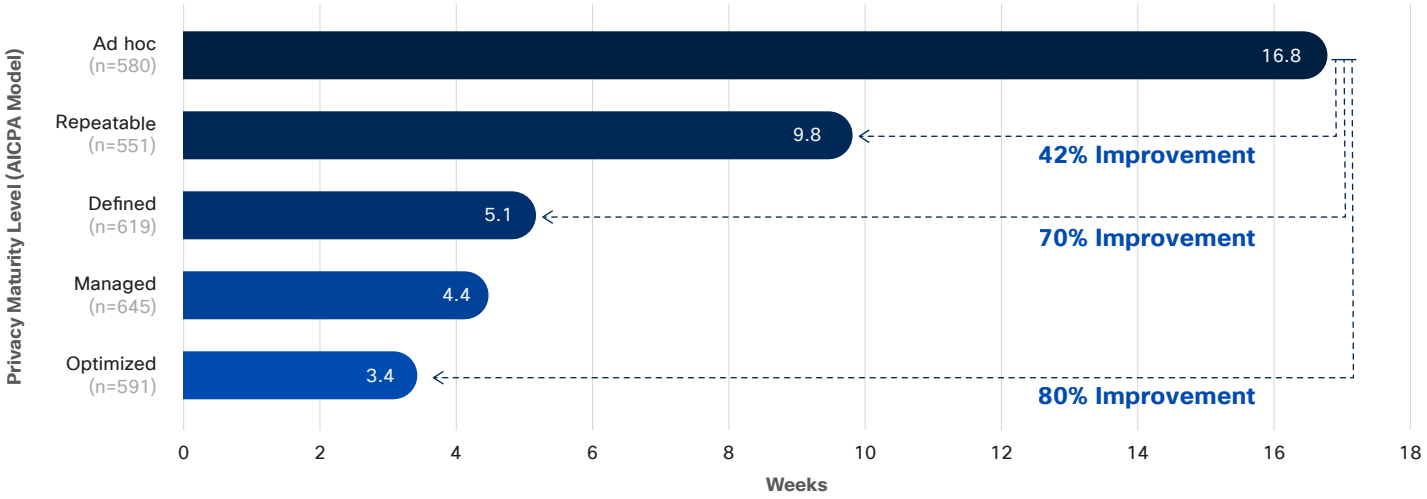
When these self-assessed privacy maturity levels were compared to the sales delay estimates, an interesting finding emerged: while the overall average sales delay was 7.8 weeks, privacy-immature organizations had much longer delays than those that were privacy-mature. "Ad hoc" organizations experienced the longest delays (16.8 weeks) and the delays declined with higher privacy maturity levels. The most privacy-mature organizations ("Optimized") had average delays of only 3.4 weeks, which is 80 percent shorter than those that were "Ad hoc" (See Figure 5).

It is also worth noting that the most significant differences were between "Ad hoc" (16.8 weeks), "Repeatable" (9.8 weeks), and "Defined" (5.1 weeks) organizations. This suggests that for relatively privacy-immature organizations, moving just one level higher could be quite beneficial. For example, going from "Ad hoc" to "Repeatable" would represent a 42 percent improvement in the average sales delay, and from "Ad hoc" to "Defined" would represent a 70 percent improvement.

AICPA/CICA Privacy Maturity Model

1. **Ad hoc** – Privacy procedures or processes are generally informal, incomplete, and inconsistently applied.
2. **Repeatable** – Privacy procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
3. **Defined** – Privacy procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. **Managed** – Reviews are conducted to assess the effectiveness of the privacy controls in place.
5. **Optimized** – Regular review and feedback are used to ensure continuous improvement towards optimization of privacy processes.

Figure 5 Average sales delay, by privacy maturity level



Source: Cisco 2018 Privacy Maturity Benchmark Study

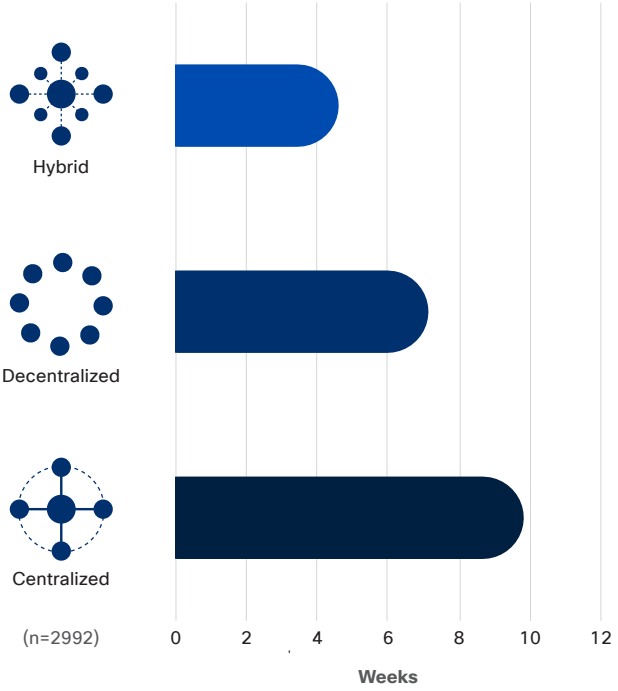
Organizational model and sales delays

Privacy resources can be centralized, decentralized, or follow a hybrid model with a mix of centralized and decentralized resources. Of the organizations participating in the study, 47 percent reported using a centralized model for their privacy resources, 29 percent use a decentralized model, and 24 percent use a hybrid model. In terms of sales delays, the hybrid model appears to be the best performing, with average delays of only 4.6 weeks compared to 7.1 for decentralized and 9.8 for centralized organizations (See Figure 6).

Privacy maturity and cyber events

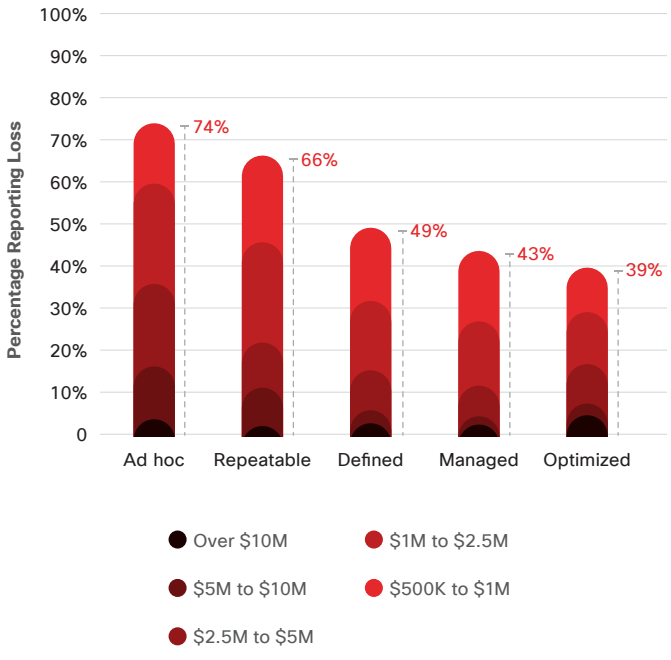
Finally, an organization's privacy maturity appears also to be correlated with lower losses from data breaches. 74 percent of privacy-immature organizations experienced losses of over $500,000 during the last year due to data breaches, compared to only 39 percent of privacy-mature organizations. This may result from privacy-mature organizations having processes that minimize the amount of data the organization stores and protects, but more research is needed to confirm this relationship (See Figure 7).

Figure 6 Average sales delay, by privacy organizational model



Source: Cisco 2018 Privacy Maturity Benchmark Study

Figure 7 Organizations with data breach losses of $500K+ in the last year, by privacy maturity level



Source: Cisco 2018 Privacy Maturity Benchmark Study

Implications

Given these results, every organization should better understand the impact of data privacy on their sales cycle. Businesses should assess what percentage of their product or service portfolio may be impacted by customer privacy concerns and quantify the potential size of any delays. Work should be done to minimize the delays, which could include:

1. **Ensuring that salespeople have timely access to information that addresses common customer privacy concerns**
2. **Establishing teams to quickly investigate customer issues as they arise**
3. **Working with engineering and product development to make any needed changes, ideally ensuring that privacy is built in from the beginning**

Conclusion

The Cisco Privacy Maturity Benchmark Study quantifies some of the business benefits of good privacy, specifically shorter sales delays and lower losses from cyber events. More research is needed to examine how these benefits may change over time, especially in response to shifting regulations and customer expectations 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 decision-making and improved trust with our customers.

More information:

Visit Cisco Data Privacy at
https://www.cisco.com/c/en/us/about/trust-center/data-privacy-day.html

Privacy Sigma Riders Podcast “Good Privacy is Good for Business"
https://www.cisco.com/c/en/us/about/trust-center/privacy-podcast.html

Follow us **@CiscoTrust**

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 2018