


2019

Privacy Gains: Business Benefits of Privacy Investment



This white paper explains the impact and importance of investing in privacy. The paper details the business benefits that enterprises realized from investing in privacy programs and tools, their preparation for and compliance with privacy regulations, and the risks associated with maintaining subpar privacy standards.

Throughout the past decade, Cisco has published a wealth of definitive security and privacy intelligence information to help professionals learn about best practices, manage their environments, and respond to a changing landscape. In January 2019, Cisco published its 2019 Data Privacy Benchmark Study, based on responses from a double-blind survey of over 3200 security and privacy professionals in 18 countries and across all major industries. To support this quantitative study, the Cisco Privacy organization asked The Beacon Group to conduct a qualitative market assessment across target verticals and geographies to capture in-depth insight from privacy professionals. As part of its Privacy Market Assessment, Beacon spoke with 29 privacy leaders across the United States, Latin America, Asia Pacific, and Europe. This white paper is a result of the collaboration between Cisco and Beacon.

Introduction:

Privacy is good for business

Cisco is committed to upholding its customers' privacy and believes that enterprise privacy program investments have tangible business benefits. Together, Cisco and Beacon have studied the ways in which privacy drives value for enterprises worldwide, well beyond complying with regulatory standards. This paper analyzes and details these benefits and contemplates the future state of data privacy. Based on global survey data, as well as qualitative conversations with select data privacy leaders worldwide, Cisco and Beacon identified some top business benefits realized through privacy investment. Those benefits that enterprises are experiencing today have been communicated and confirmed in the market and detailed in this paper. Though today's privacy-related benefits are well defined, continued enterprise privacy investment and experimentation, which are expected, will likely yield additional benefits in the future.

Beacon qualitative assessment



Beacon Privacy Market Assessment: Key Takeaways

- Auxiliary benefits of privacy-related investments include gaining a competitive edge and mitigating data breach loss
- General Data Protection Regulation (GDPR) compliance is challenging for enterprises with limited resources, as time, personnel, and funding needs increase
- Views of privacy as “good for business” seem to be commonly held, especially by EU enterprises or by companies marketing to the EU
- Sales delays are consistent with subpar vendor practices

Cisco 2019 Data Privacy Benchmark Study: Key Findings

- GDPR-ready companies are benefiting from their privacy investments beyond compliance in a number of tangible ways
- They had shorter sales delays due to customer’s data 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 (79,000 vs. 212,000 records) and system downtime was shorter (6.4 hours vs. 9.4 hours)

Cisco quantitative survey



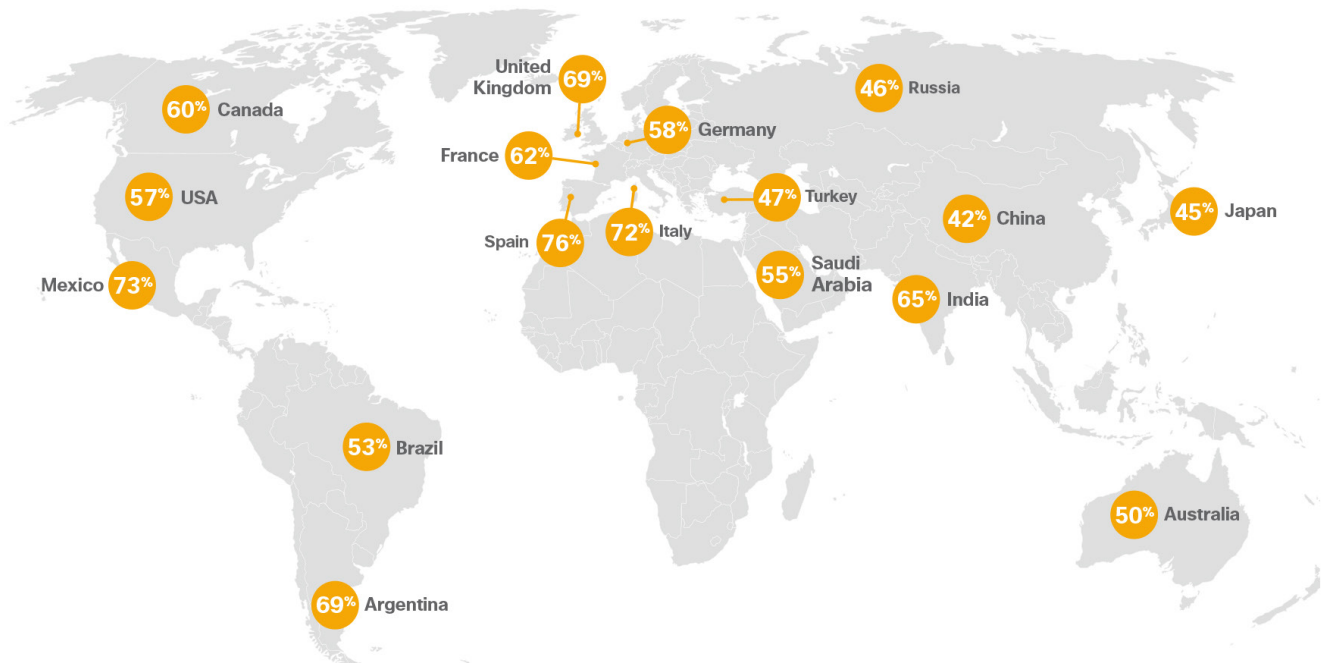
- As a result, the overall costs associated with these breaches were lower; only 37% of GDPR-ready companies had a loss of over \$500,000 last year vs. 64% of the least GDPR ready
- When asked whether privacy investment was yielding benefits (such as greater agility and innovation, gaining a competitive 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

For more information, see the full Cisco [study here](#).

The Cisco 2019 Data Privacy Benchmark Study consisted of a survey completed in late 2018 by over 3200 security professionals who were familiar with privacy processes and their impact at their organizations. The Beacon Group conducted 29 in-depth interviews with privacy leaders around the globe in August 2018. The results of the Cisco survey shed light on the impact of data privacy concerns on sales delays, as well as the correlation between GDPR readiness and the likelihood and costs of a data breach. The study showed that nearly all companies are getting business benefits from their privacy investments, including better agility and innovation, operational efficiencies, and competitive advantage, and they experienced fewer and less costly data breaches.

Beacon’s primary interviews shed light on the challenges that privacy professionals face across disparate geographies, as well as how they see privacy creating value for the enterprise. Beacon discovered that privacy-related sales delays are frequently caused by issues or misalignment during the vendor contracting process. Specifically, when companies have subpar privacy practices or policies, or are unwilling to share their current practices, delays in contract signing or even a product redesign can occur. Furthermore, privacy leaders across the globe clearly articulated the ways in which privacy creates business value for their organizations. The results of these interviews and the Cisco study will be detailed in the following pages, but the message is clear: privacy is good for business.

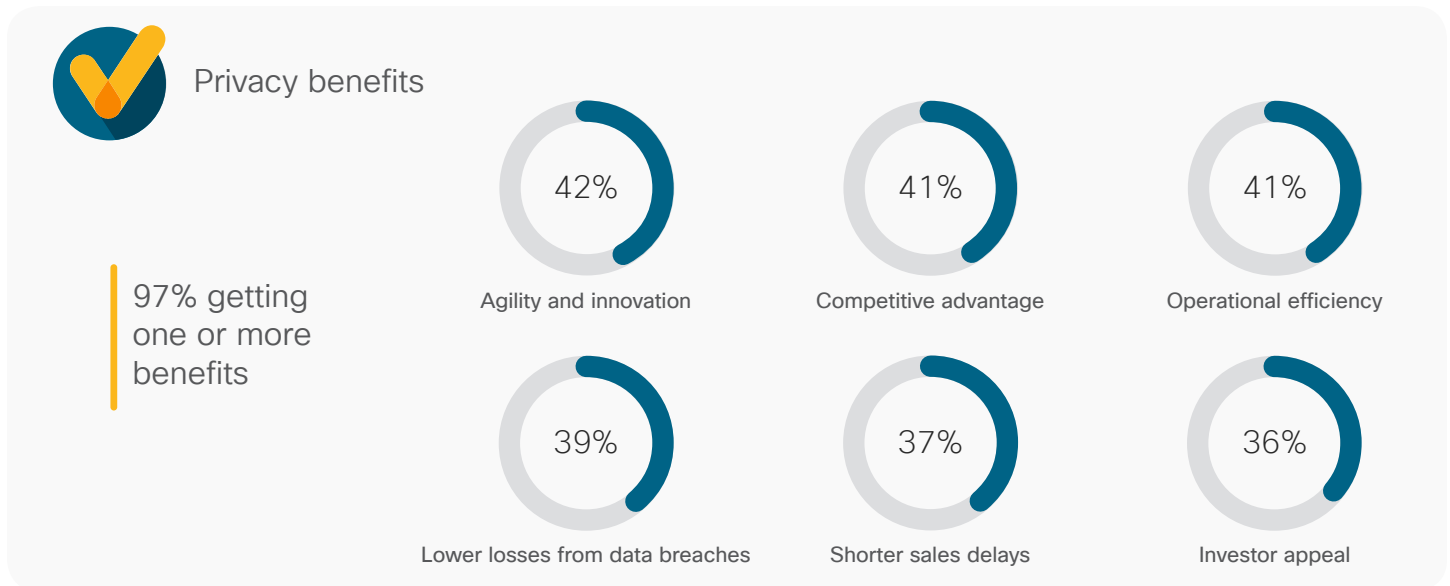
Figure 1. GDPR Readiness by Country



Source: Cisco 2019 Data Privacy Benchmark Study

Business Benefits of Privacy Investment

Figure 2. Privacy-related investment benefits realized by global enterprises



Source: Cisco 2019 Data Privacy Benchmark Study

Maintaining adequate privacy practices across organizations allows enterprises to realize unexpected benefits. Although many top decision-makers across global enterprises continue to see privacy program and tool investments as a way to avoid risk, experts increasingly recognize the value that privacy programs and tools provide to their organizations. Leaders of privacy-mature organizations are most likely to understand the business value of their programs, but many privacy professionals still struggle to demonstrate positive ROI within their organizations. Nevertheless, clear business benefits are being derived from investments in privacy programs and tools. Some of the key benefits, detailed in this white paper, include gaining a competitive advantage, mitigating data breach loss, optimizing data usage, improving operational efficiency, and increasing investor appeal.

Competitive Advantage

Figure 3. Privacy competitive advantage



Source: Beacon Privacy Market Assessment

Strong data privacy practices create a competitive advantage for an enterprise. Even in Europe, where GDPR is now in full force, many business leaders view exceeding privacy regulations as a differentiator.

The degree of competitive advantage hinges on regulatory context and market leader share. In the retail sector, customers can be fickle and are often happy to switch vendors based on data protection concerns. In the healthcare sector, however, enterprise decision-makers are less likely to see a privacy-centric approach as a differentiator given the inherent expectation that manufacturers and providers already protect sensitive data.

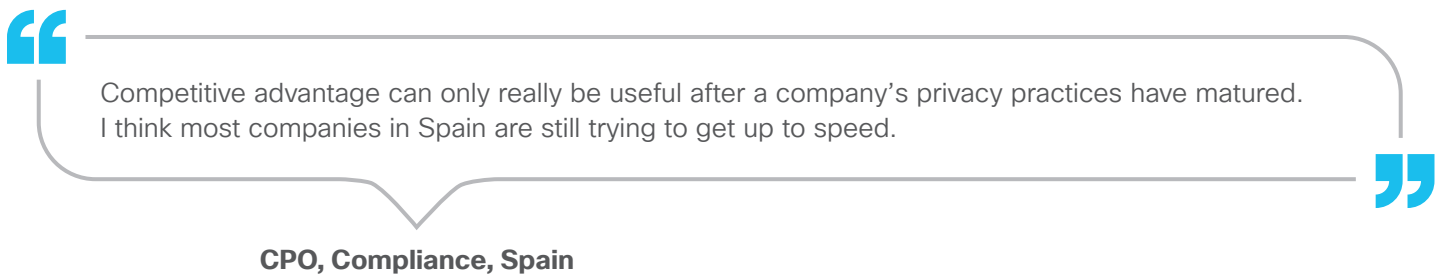
Figure 4. Privacy as a Competitive Advantage for Indian Enterprises



Source: Beacon Privacy Market Assessment

Interestingly, but perhaps not surprisingly, a strong privacy program and specifically GDPR readiness have become a competitive advantage for companies worldwide marketing to the European market. In India, for instance, where there are numerous business connections to Europe (particularly in IT and business process management), many privacy leaders view their work as directly creating competitive advantage for the organization.

Figure 5. Privacy Program Maturity and Competitive Advantage



Source: Beacon 2018 Privacy Market Assessment

Breach Mitigation

Figure 6. Privacy Processes Guard Against a Breach

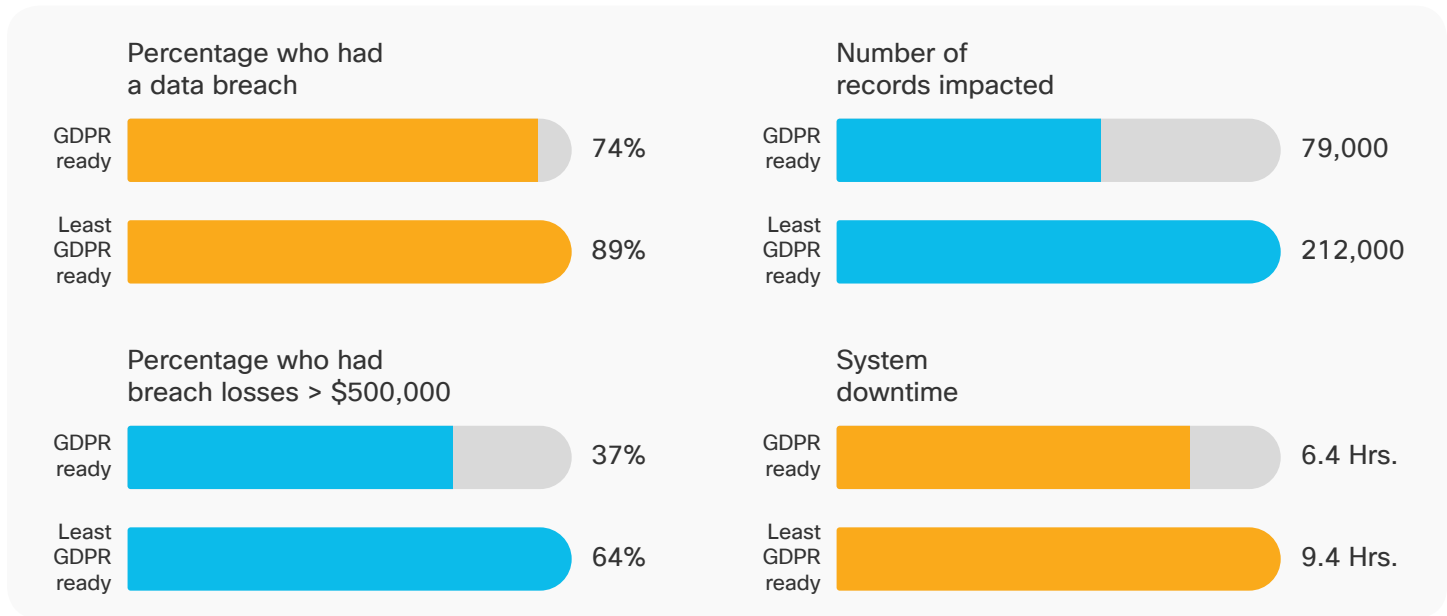


Source: Beacon Privacy Market Assessment

Aside from avoiding regulatory fines, the most immediate business impact that privacy leaders cite is mitigating financial losses incurred by a data breach. How does privacy protect against a data breach? While information security technologies provide the actual protection to guard against a cyber attack, privacy policies establish boundaries for who can and should access what data, when, and why. Aside from the immediate loss of business that occurs post breach, they also tend to carry long-term impacts on company brand and reputation.

Not only does a privacy program help protect a company from a breach, but the more mature that program is, the smaller the financial loss if a breach occurs. In the Cisco 2019 Data Privacy Benchmark Study, the companies that invested to get ready for GDPR experienced fewer and less costly breaches. Seventy-four percent of GDPR-ready companies experienced a data breach in the last year (versus 89% of the least GDPR-ready companies). And when a breach occurred, the GDPR-ready companies experienced fewer records impacted (79,000 vs. 212,000) and shorter system downtime (6.4 hours versus 9.4 hours), and only 37% of them experienced a loss of over \$500,000 in the last year from data breaches, compared to 64% percent of the least GDPR-ready companies. (See Figure 7.)

Figure 7. GDPR-ready companies have fewer and less costly breaches



Source: Cisco 2019 Data Privacy Benchmark Study

Optimized Data

Figure 8. Privacy Drives Success and Innovation Through Optimized Data

“ [Privacy] gives you more confidence in being able to market to people and ensure that we’re compliant and not liable. ”

CPO, Insurance, UK

“ We have a lot of data on consumer behavior, which is private data—where people buy, what they like, all of that. For us, that generates value. ... If we want to start a marketing campaign, we want to make sure we can use that data legally first. ”

CPO, Financial Services, Chile

Source: Beacon Privacy Market Assessment

Having a strong privacy program allows organizations to extract more value from the data that they already have. In the preliminary stages of establishing a privacy program or addressing local regulations, businesses typically undergo a “data mapping” or “data discovery” phase to identify what data they actually have. In the process, they drive insights into customer behavior or from other organizational data they already have access to, delivering more actionable, real-time insights from existing data assets. Not only can data privacy drive valuable insights from existing data, it can lead to more efficient and effective use of that data. A privacy program also reduces the risk of using customer data by ensuring that employees are using it within appropriate bounds (for example, marketing campaigns).

Throughout conversations with privacy leaders, these professionals reiterated the idea that their privacy programs created value for the organization, specifically around data insights and data usage. As seen in Figure 8, a privacy leader at a UK insurance company brought up the idea that privacy has enabled the company to function more effectively and also to feel more confident while doing so. In Latin America, the privacy head of a multinational bank concurred, suggesting that data privacy has allowed the bank to do its job more effectively and with complete confidence. Having a strong privacy program in place allows enterprises to derive greater insights, innovation, and ultimately business success.

Operational Efficiency

Figure 9. Privacy Creates Operational Efficiency

“ We want to know where the consumer is spending and how they’re spending it so we know how to offer something more relevant, instead of blasting 10,000 customers and wasting market dollars. Data privacy has helped us use fewer resources and do it better. ”

CPO, Pharmaceuticals, Singapore

“ We have huge filing cabinets where things have been kept for years, and so we’ve finally started getting rid of what we don’t need, which is a functional benefit in terms of efficiency and space. Do we really need 10 reams of filing cabinets full of data? If we haven’t got it, it helps minimize the risk. ”

CPO, Hospital, UK

“ Part of the challenge for an organization like ours is to have an inventory of all the data processing activities that take place. That’s an area that can create business value. Mapping our data can help us find inefficiencies in our process. ”

CPO, Insurance, UK

Source: Beacon Privacy Market Assessment

Data privacy programs have the ability to increase operational efficiency, which is of tangible value to a business. Privacy professionals have suggested that during the initial “data mapping” or “data discovery” phase of establishing a privacy program, companies often discover inefficiencies in their current workflows when they attempt to track where data is moving within an organization.

Additionally, having clear privacy policies and established processes for handling complex privacy issues allows organizations to minimize the types of delays that a less privacy-mature company might otherwise experience.

Investor Appeal

Figure 10. Privacy Programs Positively Affect the Attractiveness of a Company as an Investment



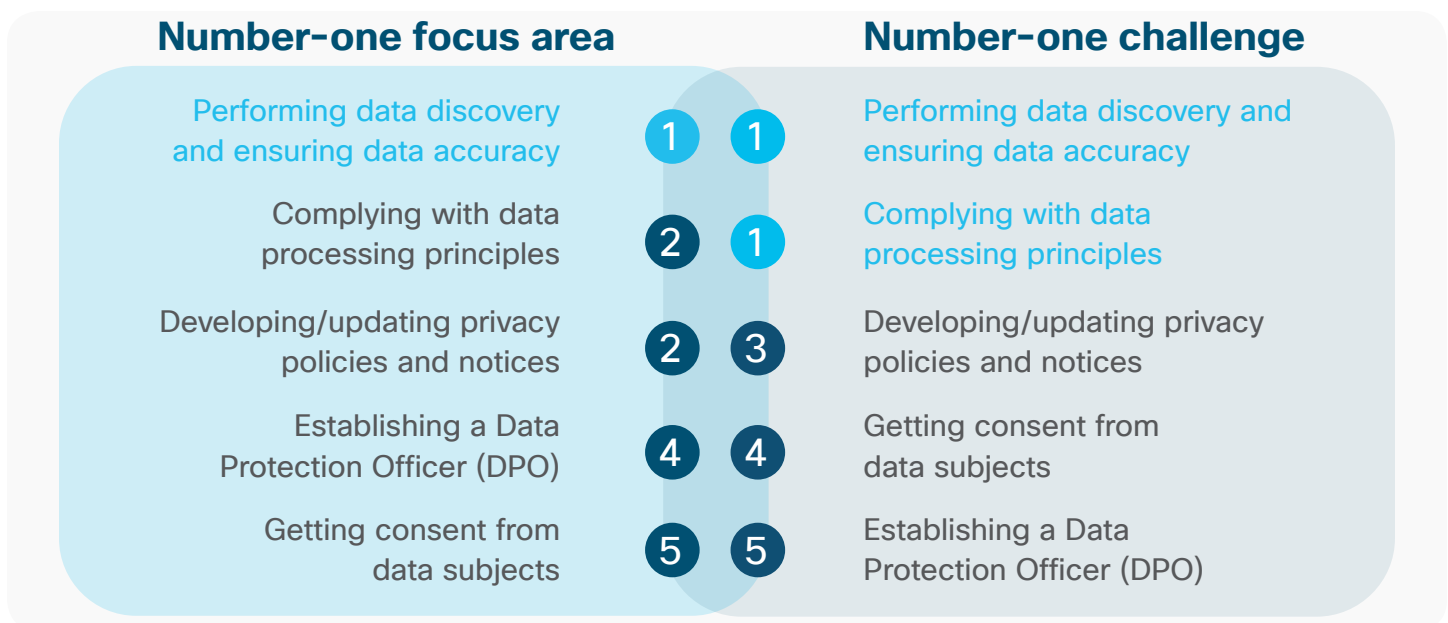
Source: Beacon Privacy Market Assessment

Though not mentioned as frequently as mitigating data breaches or gaining competitive advantage, privacy leaders worldwide point out that having established privacy programs can help attract investment dollars. Given the number of high-profile data breaches that have occurred in recent years, investors appear to be more skittish than ever and want to know exactly what companies are doing to protect themselves against this looming concern. This holds true across industries and geographies. There is less enthusiasm to invest in a company that is likely to experience a data breach of material proportions.

Challenges of Adopting a Privacy-Centric Approach

Growing Complexity

Figure 11. GDPR challenges



Source: IBM Institute for Business Value 2018

While the regulatory environment varies significantly across countries, the privacy and data protection landscape is generally becoming more complex worldwide. Europe received increased attention recently when GDPR came into effect in May 2018. But in addition, privacy and data protection frameworks in other geographies also continue to evolve and require companies to act with transparency, fairness, and accountability. Privacy and/or cybersecurity laws have been recently adopted or revised, or are in the process of being updated, in numerous jurisdictions across Asia Pacific and the Americas, including China, Japan, Singapore, Thailand, India, Brazil, and California, among many others. While the challenges and opportunities for enterprises vary based on the regulatory environment and customer demands of each country, many businesses today are struggling with a lack of sufficient resources and the need to shift an organizational mindset to prioritize privacy and data protection.

Organizational Culture Shift

Figure 12. The Need for an Organizational Culture Shift

“ People within the organization tend to see it from a compliance perspective, but from my point of view, compliance is a way to leverage trust. The awareness you need to implement a company-wide privacy policy is very important. It’s really important for people to understand that privacy is not a separate topic, but needs to be embedded throughout business processes, whether with employees or clients or contractors or suppliers. You don’t get revenue from privacy per se, but you will generate revenue from investing in it. A lot of people just see it as an additional cost, and it’s very difficult to make them understand. ”

CPO, Financial Services, Hong Kong

“ My current role is very much about making people understand the importance of privacy. ... What is most challenging is changing people’s mindsets. We work with different people from different cultures, and making people understand that I’m here to help you and not to make you stop doing things is definitely hard. We have to do it, but how do we do it without hurting our business prospects? That’s another key challenge. ”

CPO, Pharmaceuticals, Singapore

“ We went from a checklist to a cultural shift within the whole organization. The biggest challenge in complying with GDPR was making people understand that privacy is not a compliance thing. People just thought it was a boring standard, but we had to promote the view that data is important so they can understand how important privacy is. The change in mindset was the biggest initial challenge, for sure. We started with the third- and fourth-level employees too, instead of top management. ”

CPO, Technology, India

Source: Beacon Privacy Market Assessment

Privacy leaders worldwide repeatedly say that shifting their organizational culture is the most difficult aspect of their job. To become truly privacy-centric, employees must be trained both in what they can and cannot do and what they must do to take privacy seriously at all levels. An effective training program will also be able to successfully communicate the business value and data insights that privacy can unlock. Communicating the value of privacy within an organization includes training at all levels, from individual contributors to the most senior leaders and the board of directors.

Time, Personnel, and Financial Resources

Figure 13. Resource Constraints Pose a Serious Challenge

“ We have about 4000 clients across all of our business lines, and I am the only data privacy lawyer for the company. I am in charge of internal training on personal data protection, confidentiality, IP rights like patents and authorship for any apps we develop, and all our privacy notices, as well as onboarding. I’m in charge of the company email address for privacy issues. I am the privacy department, effectively. The work is of titanic proportions. I also have to deal with contract clauses and data transfers and for doing due diligence with our third-party providers. Sometimes they don’t have as robust of a privacy policy in place as [us]. My biggest challenge is having enough time to do everything. There’s not enough time in the day to get everything done. ”

CPO, Financial Services, Mexico

Source: [Beacon Privacy Market Assessment](#)

While it is becoming increasingly important to invest in privacy, there is clearly still a lag when it comes to resources. Devoting sufficient resources to privacy programs remains a big challenge for organizations both large and small. Even in the EU, many organizations have small privacy teams and budgets—especially in contrast to information security teams and budgets— or have privacy leaders who wear multiple hats. Enterprises in Latin America are particularly resource constrained.

In the initial stages of GDPR compliance, many companies had to start from scratch simply to identify what data they were managing. Privacy professionals frequently cite this initial step and the right to deletion as very difficult and time-consuming challenges. What’s more, the privacy landscape is becoming increasingly challenging, so the complexity and requirements of privacy teams will only increase.

Risks Associated with Lack of Privacy Investment

With the advent of GDPR, the stakes for poor data privacy practices have increased dramatically. With fines of up to 4% of global annual turnover, or 20 million euros (the greater of the two), the risk of noncompliance can be material regulatory fines.

Regulatory Fines

Avoiding potentially massive fines is the most obvious risk of not complying with local regulations. Having an established privacy policy and ensuring internal alignment on the importance of privacy is an absolute necessity when it comes to avoiding those fines. As data protection regulators around the globe have frequently expressed^{viii}, they are not looking to punish companies that are earnestly trying to protect customer data, but to do so, enterprises need to create a privacy program if one doesn’t already exist in their organization.

Data Breach

As previously discussed, the risk of not complying with privacy regulations is more than just incurring fines. Poor privacy practices can lead to massive data breaches that affect a company for long after the breach. Aside from the role of information security, having a strong privacy program is critical to protecting companies from a breach.

Future Outlook

While it is difficult to know definitively what the future holds, the market will likely imagine and realize new, innovative ways to process personal information. Many of these new approaches will be done well with privacy in mind. Clearly, approaches that include privacy considerations will provide more value and market differentiation.

Figure 14. The Future of Data Privacy

“What happens in the next 5 to 10 years? Probably for the retail world it’s realistically the next 5 years. We might move from permission-based marketing to an actual value for each consumer’s profile. That data store of your preferences will have value. Maybe we’ll even move to a phase where you can monetize your own data as a consumer. There may be companies that will be like a bitcoin digital wallet but that store all your personal data, and you can make it as accurate and authentic as possible to make it more valuable.”

CEO, Marketing, US

Source: Beacon Privacy Market Assessment



Conclusion

As the Cisco and Beacon research demonstrates, the benefits of sound privacy practices and systems extend well beyond meeting compliance requirements. Good privacy is good for business, and many privacy leaders and their organizations recognize that fact and benefit from it daily. Although enterprises still face significant challenges when it comes to shifting their organizational culture and ensuring adequate allotment of resources to privacy, increasing awareness of the value of privacy will help organizations make better decisions on their privacy investments.

Contacts

Cisco Privacy Office: trust.cisco.com

The Beacon Group: www.beaongroupconsulting.com