Pandemic, Compliance Driving Increased Privacy Spending

Immigration advocates say US needs legislation to effectively respond to arrivals at border, but divisions run deep.

John P. Mello Jr.

November 9th, 2021

The global pandemic and the need to comply with laws governing consumer data are fueling increases in privacy budgets, according to a report by an association for privacy professionals and a multinational professional services firm.

The Privacy Governance Report for 2021 produced by the International Association of Privacy Professionals, EY and EY Law discovered through a survey of privacy professionals around the world that privacy spending has increased significantly over 2020, with the average privacy spend amounting to $873,000 and the median budget $330,000.

It also noted that 60 percent of the privacy pros surveyed expect their budgets to increase in 2022, and almost none anticipate budget cuts.

As with many workers since the pandemic began, privacy pros are working from home in greater numbers.

More than eight in 10 privacy pros (81 percent) are working exclusively or mostly from home, surveyors found. That's expected to continue for the rest of 2021, with 78 percent of the privacy pros expecting to remain remote or hybrid workers.

There appears to be no change in sight. For next year, 82 percent of the privacy pros are still expecting to be working mostly remotely or in some form of hybrid arrangement, dividing their working hours between home and office,

Compliance Is Top Priority

The report noted that compliance with the European General Data Protection Regulation, California Consumer Privacy Act, California Privacy Rights Act and other U.S. state privacy laws, as well as other global laws, has been a top priority for most privacy teams over the past year.

It revealed that 26 percent of the companies subject to the CCPA were in full compliance and 41 percent were "very compliant." GDPR compliance was lower, with 20 percent in full compliance and 43 percent very complaint.

"Privacy laws have had a significant impact on how companies are approaching privacy, but it has been mainly internal to the companies' operations," observed Rob Shavell, CEO and co-founder of Boston-based Abine, maker of Blur, a combination password manager, email masker and ad tracker blocker.

"It's not something that consumers have felt much of a difference," he told TechNewsWorld.

"It's a big change for companies because they have to hire a bunch of people and pay attention to where data is stored and who it's shared with, more so than they did before these laws were passed," he added.

Customizing Privacy

Liz Miller, vice president and a principal analyst with Constellation Research, a technology research and advisory firm in Cupertino, Calif. explained that lots of organizations have fundamentally changed how they operate because of privacy laws.

"The challenge is they haven't redefined what privacy means to them," she told TechNewsWorld.

"They're complying with the laws without asking what does privacy mean to us and how is protecting our customers' data and privacy fundamental to the way we operate?" she said.

"They're checking off the boxes, but the more interesting organizations are redefining what privacy means to them and making it something the customer is driving and not something to be exploited," Miller observed.

"They're asking their customers what they want from the company that has value to them," she added.

"That's a residual benefit to consumers from this wave of regulation," she continued. "More people are becoming aware that privacy is an opportunity to create a conversation about what everyone wants — a durable, lasting relationship with the customer."

Help Wanted

The report also noted that nearly half the pros (45 percent) revealed their organizations are planning to hire at least one or two new privacy professionals over the next six months.

Those extra bodies will be needed when the California Privacy Rights Act takes effect on January 1.

“The CPRA is going to have a considerable effect on privacy,” observed Timothy Toohey, an attorney with the Greenberg Glusker law firm in Los Angeles.

He explained that the law will be giving consumers new rights, including the right to see information that a company has collected about them.

“That can be quite burdensome on companies,” he told TechNewsWorld.

In addition, the law imposes data and privacy requirements on vendors of companies.

“In this next year, there’s going to be a lot of scrambling by companies putting new agreements into effect with their vendors,” Toohey said.

“Some companies can have hundreds of vendors,” he added.

Legal Jungle

An increasing number of privacy laws — both at the state level in the U.S., as well as at the national level around the world — make privacy operations increasingly central to what an organization does, the report noted.

The proliferation of those laws, especially in the United States, can also complicate the compliance task for companies.

“It’s created a problem,” Toohey acknowledged.

“We have three states with comprehensive laws — California, Virginia and Colorado — and a lot states are considering them, particularly in light of the pandemic and work-from-home, because of the proliferation of information online,” he said.

“Whenever you have laws worded slightly differently, as all these laws are,” he explained, “it creates potential compliance headaches.”

“You have to reframe your agreements,” he continued. “You have to look at your privacy policies, and you have to comply with consumer requests from various jurisdictions, since there is no standard federal law — nor is there likely to be one in the immediate future,” Toohey added.

Pandemic Affects Privacy

However, Shavell maintained businesses may be complaining too much about the plethora of privacy laws in the United States.

“Companies say it’s difficult to comply with the growing number of privacy laws. That’s hyperbole,” he said.

“Companies say it because they want to act like everything is hard, so they don’t have to do it,” he continued. “In reality, these laws are very similar. Most of them are just subsets of one another. The CCPA, for example, is just a subset of the GDPR.”

While companies are beefing up their privacy teams, they’re also beefing up their surveillance tools, largely due to the pandemic. “One pattern we see in the shift to remote work is that companies are hunting for ways to monitor output and productivity without a manager physically observing employees,” observed Julian Sanchez, a senior fellow at the Cato Institute, a public policy think tank in Washington, D.C.

“For many, the answer is tools like InterGuard, ActivTrak, Hubstaff and TimeCamp, which are essentially spyware that can track what workers are doing on their computers in incredibly granular ways,” he told TechNewsWorld.

“The pandemic didn’t invent these tools, of course, and plenty of businesses had them installed on in-office computers before Covid, but the shift to more remote work led to a significant spike in adoption,” he said.

Vaccine mandates can also pose a risk to privacy.

“Vaccine mandates are creating all these little databases at places requiring proof of vaccination for service,” Shavell explained. “There’s no real control over those databases.”

“What we advocate is a low-tech approach,” he said. “Check for a vaccine card, but don’t create a database. There’s no need to enter that information where hackers, scammers or marketers can get it.”

The complete IAPP-EY Annual Privacy Governance Report 2021 is available here.