In The News

9 CCPA questions every CISD should be prepared to answer

02.03.20

CSO Online

Executive management anxiety over the California Consumer Privacy Act will rise as the enforcement deadline looms. Security managers will need to know the answers to these questions.

The California Consumer Privacy Act (CCPA) went into effect on January 1 and it is affecting companies not just in California but across the United States — and even around the world. Here are nine questions that every CISO must be able to answer about this law.

1. WHAT IS THE CCPA?

"What the heck is this?"

That was the first question Branch Metrics CEO Alex Austin had for Cathleen Hartge, his data protection officer (DPO), when he first heard about the CCPA when it was still being finalized by California's lawmakers.

The CCPA was approved in June 2018 by the California legislature. It was passed in a hurry to avoid a public referendum on the issue. As a result, a lot of the details of the law and how it will be enforced are still being worked out. It allows consumers to ask companies for the details of the personal information that the companies have collected about them or shared with third parties, and to ask for that information to be deleted.

"As you can imagine, there are a lot of users engaging with our customers' companies," says Austin. As a result, Branch had to prepare both for compliance-related requests from its business customers, as well as requests submitted directly to Branch Metrics by end users.

The CCPA also allows for fines against companies that violate the law and allows consumers to sue companies as well. The law went into effect on January 1, but the California attorney general won't start enforcing it until July 1 of this year.

2. DOES THE CCPA APPLY TO OUR COMPANY?

For most CISOs, this should be an easy question to answer. Does their company collect personal data on California residents? If so, does it make over $25 million in revenue per year, handle personal data for 50,000 people, devices, or households from California per year, or make at least half of its revenue from selling the information of California residents?

If any one of those last three apply, then the company falls under the CCPA. According to the International Association of Privacy Professionals, more than 500,000 companies need to comply with CCPA, nearly 400,000 of which are located in states other than California. That's more than 40% of all companies in the U.S.

In California itself, the proportion is higher. According to the regulatory impact assessment prepared by Berkeley Economic Advising and Research for the California Department of Justice, 75% of all California businesses are required to comply with the CCPA.

International companies will need to comply as well, if they collect data on California residents.

3. WHAT IS OUR RISK EXPOSURE?

Many companies already have a good understanding of what data they keep, where it's located, and how it's protected. Those that don't will need to start out with a data mapping project, says Chris May, leader in the forensic practice at Deloitte Risk and Financial Advisory.

This can keep CISOs up at night, he says. "The hardest question is not knowing what they don't know," he says. "Maybe we're not being compliant by accident, because we're not aware of some area in the organization that is collecting and maintaining protected information."

The situation is constantly changing, May adds. "It would be difficult for any company to say that they are 100% compliant," he says. "It's so new that we're not sure how the agencies will determine if someone is compliant or not."

4. ARE WE COMPLIANT WITH THE CCPA?

According to a survey published by Osterman Research in December 2019, 52% of companies surveyed says that they would not be compliant on January 1, 2020.

That might be overly optimistic, says Christophe Bertrand, an analyst at Enterprise Strategy Group. "I don't think people who think they are compliant are actually compliant," he says. "I suspect that the number is 10%, mostly the larger companies who have seen this coming — and that's very generous."

One issue is that the CCPA takes a very broad view of personal data. "It could be almost anything," he says. "An email that says, 'Hey, I'm sick today,' can be construed as personal data or privacy data."

Another mistake that some companies might make is to assume that if they're using a CCPA-compliant vendor to handle their sensitive data, then they are CCPA compliant as well. "There's a tragic misunderstanding of what's happening," he says. "There's a big risk of confusion."

If a vendor is CCPA compliant, that could mean that they have the correct processes in place for the data that they collect on their own customers, or that they have certain security systems in place, or that they offer tools to customers to search and delete data. A cloud storage provider, for example, may allow its customers to see their own private data, but wouldn't be responsible for going into the files those customers are storing that contain the data of their own end users.

"If they enable you to be compliant, that's great," says Bertrand, "but they're not going to be modifying your website. That's your job. And they're not going to be working on processes to give consumers their data within 45 days. You're always responsible for your data, and you're always responsible for the compliance for your data."

The law is still too new, he says, and still evolving.

5. WE ALREADY COMPLY WITH GDPR. IS THAT ENOUGH?

Europe's General Data Protection Regulation (GDPR) went into effect in the spring of 2018. The California law doesn't have some of GDPR's most onerous requirements, such as the narrow 72-hour window in which a company must report a breach. In other respects, however, it goes even farther. For example, it takes a broader view of what constitutes private data and allows consumers to file lawsuits.

Branch Metrics was already in compliance with GDPR when Austin learned that CCPA was on its way. That didn't mean that the company was fully ready for CCPA. "I specifically asked about what we need to do to update our privacy policy, and potentially any contracts with our customers," he says.

"The good news for us was that we already had our GDPR playbook, and we were most of the way there," says Hartge, his DPO. For CCPA, she says, much of the additional work that Branch Metrics had to do involved understanding the incremental changes required by the CCPA.

It helped that Branch didn't just set up a compliance system for its European users but created a compliance platform that applied to everyone everywhere. The platform includes all the compliance requirements of all the jurisdictions that Branch Metrics is subject to — a superset of all the privacy laws. "It's been extremely important to us to allow users, regardless of whether they're in Europe or California, or subject to these types of regulations or not, to have access and control for this type of data."

6. WHAT DO WE HAVE TO DO TO BE COMPLIANT WITH THE CCPA?

TeleSign, a Los Angeles-based identity company, provides two-factor authentication services to companies like Evernote, Salesforce and Intermedia. That requires it to have access to individuals' phone numbers. Not complying with CCPA wouldn't just mean fines and lawsuits but could also results in significant lost business.

As a result, complying with CCPA on day one was a top priority for the company. "The first question that my management asked me was, 'What is CCPA? Why is it important to us?' And then, 'What does TeleSign have to do to comply?'" says Kiat Hui, TeleSign's global information security director.

Fortunately, the company had already started doing much of the groundwork in 2017, as part of its GDPR preparations. "Because we already had a privacy team in place, it was easy for us to reach out to them and get them to analyze the CCPA," Hui says.

Like Branch Media, TeleSign decided to go with a "superset" approach to compliance. "For example, for the data mapping, we just have one centralized system that tracks for both GDPR and CCPA privacy laws," Hui says. "We take the highest common denominator — GDPR gives 30 days to respond, CCPA gives 45 days, so we respond to all requests within 30 days."

In addition to updating its data management system to include the CCPA requirements, TeleSign has also published details about its CCPA processes on its website and created a data processing addendum for both existing and potential customers to sign. "It explains our obligations under CCPA and how we will protect your data," Hui says.

7. HOW MUCH WILL THE CCPA COST?

According to the impact assessment estimates, small firms with fewer than 20 employees will incur $50,000 in initial costs, medium-sized firms of 20 to 100 employees will spend $100,000, firms with up to 500 employees will spend $450,000, and those with more than 500 employees will spend $2 million.

"This is not the time for FUD [fear, uncertainty, doubt] or an attempt to pad your budget," says Roger Hale, CISO-in-residence at YL Ventures, a San Francisco-based venture capital firm. Instead, this is an opportunity to improve a company's culture of awareness, he says.

"Privacy awareness and good data governance is the new norm," Hale says. "Take the opportunity to educate your leaders that this is a program, and as such, is not a single year budget item but a new operational program for the company and, just like security, will need to be baked into the company's business processes rather than bolted on after the fact."

Companies will need to update their websites, reconsider their data collection strategies, implement systems to track and delete data on request, and review contracts with vendors and business partners.

There's also a cybersecurity component to compliance — specifically, the need for a very high level of authentication.

"An identity thief could send a message to a company demanding a copy of information about the true data subject," says Benjamin Wright, U.S. attorney and SANS instructor for the law of data security and investigations. Or a troll could demand that a company delete all the information about a particular person.

In the past, Wright says, if a customer canceled their account, the company would still keep backups of their data and just reinstate it if it turned out that the cancellation request was fraudulent. "Now, the new California privacy law is calling for data to actually be deleted," he says.

8. CAN'T WE JUST PAY THE CCPA FINE?

For some companies, taking a wait-and-see attitude can seem appealing. Enforcement isn't going to start until July, and even then, regulators are probably going to go after the biggest offenders first. "I still hear some CISOs talking about fines being less burdensome than the preparations needed to become CCPA compliant," says Hank Thomas, partner and COO at Strategic Cyber Ventures, a Washington D.C.-based venture capital firm.

He says that's a mistake, since individual California citizens can file lawsuits of their own if there's been a breach. Plus, he says, the CCPA draws a "tougher line in the sand" when it comes to defining reasonable security. The CCPA allows for fines of up to $7,500 per privacy violation. So, say, if 1,000 California residents visited your website, and you didn't have the right notifications and opt-out buttons, that alone could add up to $7.5 million.

If there's a breach, there's a $750 fine per lost record. Plus, of course, individual California consumers are allowed to sue as well.

The fines can rack up very quickly. "Compliance is very costly," says Steve Williams, a partner with the law firm Munsch Hardt, "but we've also begun to see from GDPR that not complying is also very costly."

According to research from DLA Piper, there have been 160,000 breaches reported since the GDPR went into effect, resulting in 443 million euros (USD $488 million) in fines in the UK and Europe. "With CCPA, since there's the potential for private litigation, that makes the cost of non-compliance even higher," adds Williams. "California has a reputation for being a state where more consumer-oriented lawsuits are filed than in other states."

That doesn't necessarily mean that there's a cottage industry waiting to erupt in the wake of CCPA, he says. "But there are a number of lawyers and law firms that are focused on consumer protection and will be watching it very closely."

Plus, there are businesses — especially in the B2B space — where compliance is going to be a mandatory requirement for future contracts. "This depends on the type of business you have," says Williams, "but there are going to be some customers that are very sensitive about user data and will make choices about a particular vendor or supplier based on what they're doing to protect and secure their data."

If you're in the business of processing sensitive data, then compliance failures could cause problems for customers. "So those customers are going to be very concerned that you are complying with the law," Williams says. Some clients have already switched vendors, or are rethinking their vendor agreements, because of CCPA compliance.

9. IS THIS THE END OF IT, OR ARE MORE PRIVACY LAWS ON THEIR WAY?

Yes, other laws are already on the way. "I would expect many other states to take action after a period of wait and see to determine the impact of CCPA," says Steve Durbin, managing director at Information Security Forum, a London-based industry group. Companies need to prepare for a hodge-podge of laws — similar to the way that there are different data breach notification laws in every state.

"There is a very real need for a federal law to avoid states introducing their own variations and interpretation," Durbin says. "However, we are still nowhere near a consistent approach to privacy and personal information usage in the United States and I do not anticipate this changing with a federal regulation any time soon."

Primary Contacts

Steven Williams
Dallas
214.855.7544
swilliams@munsch.com

Related Industries

Technology & Telecommunications