Secure Channels' SCIFCOM Platform Preps Companies for CCPA

Encryption-as-a-Service Portal Provides Solutions in Time for New Regulations

IRVINE, CA, UNITED STATES, October 22, 2019 /EINPresswire.com/ -- The Jan. 1, 2020, deadline approaches quickly, and many companies remain unprepared to meet key requirements of the California Consumer Privacy Act (CCPA). Around half of U.S businesses, service providers and third parties have yet to put "reasonable" data security measures in place to satisfy the act's sometimes-vague regulations. The experts at Secure Channels Inc. shed light on what covered companies can expect after the deadline, and provide solutions that will help protect them from the act's heavy penalties.

The CCPA, dubbed "America's GDPR" by PricewaterhouseCoopers (PwC), was modeled after the EU's General Data Protection Regulation. The GDPR strictly regulates and sets penalties for organizations anywhere in the world handling and failing to protect EU citizens' data. The CCPA likewise holds accountable companies anywhere handling the personal data of the most populous state's residents.

"One need only look at the penalties the GDPR has set out so far to see where CCPA is headed," notes Secure Channels CEO Richard Blech. "This past July they hit two companies with a combined $350 million in proposed fines for data breaches. This happened within a two-day period."

Blech refers to the penalties the GDPR intends to levy against British Airways (£183 million) and Marriott (£99.2 million) announced July 8 and 9 respectively. Marriott's violations stemmed from IT failings of a hotel chain they subsequently purchased, inheriting its liability, while a hack against British Airways redirected customer data from the company's website to an unauthorized party. "In BA's case, there was no financial loss to any customers exposed by the breach, but the failure to protect the data alone may result in the largest GDPR fine to date — second largest breach fine in history," Blech points out. "The CCPA is the same kind of beast. Affected consumers will be able to sue companies under the regulations without having to prove financial harm."

Thus far, the CCPA is ambiguous in what meets its "reasonable security" requirements, making compliance tricky. "The CCPA doesn't explicitly mandate that covered companies encrypt consumer data, but it does give consumer's the right to sue when their unencrypted data is compromised due to failures implementing reasonable security measures," Blech explains. "There's little hard guidance for what their definition of 'reasonable' is, but the California Attorney

General's 2016 Data Breach Report does specifically recommend strong encryption. Bottom line is encrypting consumer data may be the one step that can spare a company from the severe financial fallout that comes with a breach."

The CCPA states that violations of the act can result in fines between $100 and $750 per consumer per incident, or actual damages if greater. A company that mishandles 50,000 Californians' unencrypted personal data can net fines between $5 million and $37.5 million from the base fines alone, not counting reimbursement of any financial damages and business lost through operational and/or reputational harm.

The CCPA complements California's extant data breach notification law that limits breach reportage to consumers to events involving unencrypted data. A properly-deployed encryption system can therefore shield a company from both fines and a damaged reputation. However, even with so much to lose, PwC and others report that approximately half the businesses they surveyed believe they will not have measures in place to achieve compliance by the 2020 deadline. Blech attributes this to the complexity and cost typical to implementing or overhauling a security system.

"Encryption is one of the ways a company can mitigate the damages of a breach, but IT customers are saying the same things today they were saying 20 years ago: it's too difficult to deploy, it's expensive, it's too user-unfriendly, it's cumbersome, it's incompatible with their systems. Even the accepted top-shelf encryption, AES-256, is a 20-year-old cipher that will have questionable efficacy against the unpredictable, rapid advancements in quantum computing. They've needed a solution that fits their budget, system architecture, operational needs and, most of all, is simple to use."

Blech is confident Secure Channels' encryption-as-a-service portal answers these concerns. "We've released SCIFCOM with our assembled encryption solutions that make it easy and extremely cost-effective for companies to temper the CCPA's presumed heavy-handedness."

Blech elaborates, "What we've put together with SCIFCOM are encryption apps and plugins that can provide standalone protection or work within any existing systems companies have in place. It's strong, user-friendly encryption for any data-protection situation.

"Visitors to the portal can download our free XFA Mail plugin to send and receive encrypted email. It's weightless and works with most email clients, like Gmail and Outlook, and uses our post-quantum XOTIC cryptosystem to keep communicated data out of the hands of unauthorized parties. Or, they can sign up for a free SCIFCOM account and send encrypted mail and files directly through the portal."

Blech continues, "We've also released ZIPcrypt through SCIFCOM. Anyone who downloads it can encrypt files right on their desktop with XOTIC and AES ciphers. It's a very simple solution for users who want to archive data or send encrypted files from their computers.

"Our SUBROSA solution phases out old PIN and password technology for a more secure, intuitive picture-based authentication system where users create easy-to-remember passcodes. That's available to developers as a toolkit and sandbox environment."
SCIFCOM is also the destination for companies seeking encryption they can integrate into their systems. "XOTIC is the main encryption component of many our SCIFCOM products, and we've made it available to companies and tech integrators across all industries as a free trial demo. We want companies to see that XOTIC can be deployed anywhere, easily, and for a mere fraction of the cost they could face if they get breached."

Blech hopes vulnerable companies protect themselves and, more urgently, their consumers before a breach puts them on the wrong side of privacy regulations. "If we've learned anything from GDPR's handling of breaches, it's clear that the attitude is there's no excuse anymore not to

have strong data security in place. That may be true, but we also know there have been obstacles for a lot of companies that want to deploy cybersecurity solutions. That's why SCIFCOM is there. We made it easy. Everyone should have access to no-friction encryption." Learn more about SCIFCOM at https://securechannels.com/scifcom/.

About Secure Channels
Secure Channels is a cybersecurity solutions development company based in Irvine, Calif. Our experts engineer and develop high-performance, cost-effective cybersecurity technologies as platform-agnostic software and hardware-ready solutions to protect organizations from present and emerging threats. Our award-winning, cryptanalyst-celebrated solutions include post-quantum encryption, authentication and identity management systems. We provide advanced data protection, no-friction encryption, authentication, enterprise confidentiality solutions and proximity-based monitoring and intelligence capabilities. Learn more at https://securechannels.com/.

Contact
Secure Channels Inc.
+1 949-679-5777
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
