BIRD | MARELLA P.C.

BIRD • MARELLA • BOXER • WOLPERT • NESSIM • DROOKS • LINCENBERG • RHOW

California Is Named the U.S. Capital of Cyberattacks

Published by *Corporate Counsel*

California suffers more cybercrime attacks than any other state, and general counsel there need to help lead the charge in fighting it, according to attorney Jeremy Matz.

“When it comes to cybercrime, California has the dubious distinction of being one of the top targets in the world,” Matz told CorpCounsel.com. The former federal prosecutor is a principal with Los Angeles-based litigation firm Bird Marella, where he counsels businesses and individuals affected by cybercrime.

Because the state and its Silicon Valley are at the center of the digital revolution, California Attorney General Kamala Harris in February issued a guide for businesses, “Cybersecurity in the Golden State.” But its advice could be useful for companies anywhere.

Matz explained that the increasing cybercrime in California is also occurring nationally and internationally. He said one trend is that hackers are spreading out around the world. “Asia, particularly China, are still the hotbeds,” he said, “but we’re seeing more hacking originating in African countries like Nigeria, along with eastern Europe, the Ukraine and Russia."

Another trend, he noted, is the increasing interconnection between cybercrime and virtual currencies like bitcoin. “These kind of digital currencies are tailor-made for hackers,” he explained. “There’s no government control, no way to track it. So the best way to translate a stolen thing into money is digital coin.”

Matz said that general counsel can play an important role in making a company proactive in the cyberbattle against hackers. “The general attitude of companies should not be ‘if’ but ‘when.’ They need to assume that they are a prime target.”

And once attacked, a key decision for companies, especially publicly traded ones, is how and when to disclose to regulators and victims. California was the first state to pass a law requiring data breach notification in 2003.

But Matz notes that “there can be valuable and legitimate reasons to hold off a little bit on making [a public] disclosure, as long as you notify law enforcement and your regulators. Law enforcement can often have greater success tracking perpetrators as long as they don’t know that the company is on to them yet.”

He highly recommended that businesses hire a specialized cyberfirm to assist in security precautions as well as in damage control after a breach occurs. “Law firms can help,” he said, “but cyberfirms are invaluable.”

California’s cybersecurity guide for business echoes Matz’s advice on being proactive. Among its suggestions:

- Assume you are a target;
- Lead by example: “executive management has to get involved”;
- Map and encrypt your data;
- Defend yourself by seeking out comprehensive security solutions from firewalls to antivirus programs to multilayers of defensive technology;
- As the first level of defense, train employees to understand cyberrisks;
- Plan for the worst and have a trained response team ready when a breach occurs.

Read more: http://www.corpcounsel.com/id=1202661907920/California-Is-Named-the-US-Capital-of-Cyberattacks#ixzz376Vs3x3k