libn.com
powered by Long Island Business News

John Cooney / Photo by Bob Giglione

Cybersecurity bill nudges data sharing between biz, feds

By: Joseph Kellard November 23, 2015 0

Recently approved cybersecurity legislation that gives companies legal immunity to share data with the federal government is being touted as a necessary first step to prevent hacker attacks such as the recent high-profile data breaches to Sony, Ashley Madison, Target, Home Depot and the Office of Personnel Management.

But critics decry the information-sharing bill, which President Barack Obama is expected to sign, as yet another door for the National Security Agency and other governmental entities to open to illegal surveillance of its citizens. Those activities were brought to light by leaks from private activist and NSA contractor Edward Snowden.

By a vote of 74-21, the Cybersecurity Information Sharing Act passed the U.S. Senate in October. Co-sponsored by North Carolina Republican Richard Burr and California Democrat Dianne Feinstein, the legislation was crafted to encourage private companies to voluntarily share information about cyber threats, data breaches and the like with other private entities and the federal government in an effort to build cyber defenses in the United States and assist companies to protect their data and privacy from cyber thieves, proponents said. The Department of Homeland Security would receive and manage the data information and share it with other federal agencies, including the NSA and FBI, as well as participating companies.

The anti-hacking bill includes penalties for governmental misuse of information and limits government's activities to disclose, retain or use information about cyber threats, and purports to provide protection for companies that monitor and share information from privacy lawsuits and antitrust laws that pertain to collusion.

Clifford Tsan, a partner at Bond, Schoeneck & King in Garden City and co-chair of the firm's cybersecurity and data privacy group, called CISA a welcomed but limited first step in trying to address heightened cyber attacks on businesses and government agencies, the bedrock of which encourages information sharing.

"Without an encouragement, the natural instinct of business is to not share because they don't want to risk, among other things, losing trade secrecy protection that might apply to information that is either a threat or has been breached," Tsan said. "They might not want to expose themselves to liability for sharing information, which could be to a third party or a vendor that is maybe working with the business, or whether it's storing the information or using it in some other way and somehow a breach has occurred."

John Cooney, of counsel at Ruskin Moscou Faltischek in Uniondale and chair of the firm's cybersecurity and data privacy practice, said that while the legislation provides companies protection from liability for sharing information – which otherwise could technically count as a breach of state and federal regulations, and subject them to a number of

different lawsuits – CISA requires that businesses redact irrelevant personally identifiable information before sharing cyber threat information with the government.

"If a company just does a data dump and says 'We were attacked, here's the information and our files,' they could still be subject to lawsuits for that personal information that they disclosed, and this law will not protect them," Cooney said.

Before CISA heads to Obama's desk, the bill must first be reconciled with similar legislation the House of Representatives passed in April. Tsan and Cooney said the bill is in its preliminary stages and is too vague on matters such as the types of information that is deemed sharable and what procedures and regulations will emerge from the legislation.

Within the Senate bill there are a number of procedures that are due within 60 to 100 days after CISA is enacted, Cooney said, and the Department of Homeland Security, as well as the attorney general, are required to promulgate procedures that are expected to clear up some of the vague definitions about cyber threats and cyber sharing.

"We don't want a business to act in good faith with the government and share the information and then find out that there's a technicality that they didn't comply with and thus they shared that information but are still subject to a suit over that sharing," Cooney said. "Otherwise they could end up in a worse situation with sharing than they were by not, and expose themselves to a lot of reputational harm."

Cooney noted that New York businesses must already comply with a labyrinth of 47 state standards and laws pertaining to breach notification and data security. If a business has a single customer from Massachusetts, he explained, then that business is also subject to data security laws from that state.

"So it's almost impossible for businesses to figure out all of the different laws that they are subject to, and that's just at the state level," said Cooney, who along with Tsan calls for a federal data security standard. "Then you have the Federal Trade Commission, the Securities and Exchange Commission, the Office of Civil Rights, and they all have data security standards."

Meanwhile, the Senate rejected proposals to amend CISA, including a measure calling for more stringent reviews by companies to remove personal data before sharing it with the government.

Opponents have argued that CISA permits the sharing and monitoring of customer data without adequate restrictions and oversight, and will do little to nothing to keep the cyber barbarians at the gate and stop illegal government surveillance. Technology companies such as Apple, Google, Twitter and Dropbox, as well as privacy advocates and civil liberties groups, oppose the bill.

"We don't support the current CISA proposal," Apple said in a statement last month. "The trust of our customers means everything to us and we don't believe security should come at the expense of their privacy."

Tsan said that, given the current atmosphere in the wake of Snowden's revelations of the NSA's massive surveillance of Americans' personal information, and when people's information is everywhere and easily obtainable by hackers, there is "extraordinarily heightened sensitivity" to the issue of privacy. Moreover, it was disclosed that a number of tech companies were cooperating with government and disclosing personal information whenever it was requested, for which the companies came under heavy criticism and have since been adamant about the need for court orders.

"I think the critics largely see this as a wolf in sheep's clothing, that it's just going to be yet another way for the government to continue its warrantless surveillance, even though the bill requires companies to remove irrelevant PII from information that is disclosed by the government," Tsan said.

Other critics of the bill note that it encourages disclosing information to a government that has been subject to a number of hacks and cyber attacks itself, including the federal Office of Personnel Management.

"So they don't necessarily trust that it's going to be safeguarded and they don't trust that it's going to be necessary to actually figure out the cyber threats," Cooney said. "The criticism from the groups is that the government is using this as another way to spy, data-mine, to obtain personal information and to surveil our population."

Tagged with: CYBERSECURITY BILL | FEDERAL GOVERNMENT | LAW | LONG ISLAND | SURVEILLANCE