Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Obama Cybersecurity Blitz May Lessen Liability For Breaches

By **Allison Grande**

Law360, New York (January 13, 2015, 9:40 PM ET) -- The White House began a push this week for federal legislation that would create a national breach reporting standard and encourage cyberthreat information sharing, measures that attorneys say would reduce companies' liability for cyberattacks by replacing the dozens of reporting standards that currently exist and providing a shield to companies that divulge threats.

On Tuesday, the White House proposed a legislative framework that would provide "targeted liability protection" to companies that share cyberattack data with the government. The move came a day after President Barack Obama unveiled several additional proposals, including the establishment of a national breach reporting standard that would require companies to alert consumers of a data breach within 30 days of the discovery of the incident.

The flurry of activity is meant to turn up the heat on the newly instated Congress to move on privacy reform in the wake of high-profile breaches at entities such as Sony Pictures Entertainment Inc. and U.S. Central Command. But the proposals appear to be similar in substance to legislative proposals that have been floated by lawmakers during previous congressional sessions, leading attorneys to wonder if the increased pressure would be enough to overcome hurdles that have held up the proposals in the past.

"What's new is that there is definitely momentum in light of the Sony cyberattack, and I'm sure the administration sees this as an opportunity to forge a national data breach notification statute and to push information sharing legislation," Fox Rothschild LLP privacy and data security practice leader Scott Vernick said. "But what's old is whether or not that will get done or if it will be politics as usual."

Of the half-dozen legislative proposals the administration has advanced in recent days, attorneys say the ones with the strongest chance of passage are the data breach notification and cybersecurity information-sharing proposals, which have made it the furthest in previous sessions.

If adopted in the way proposed by the administration, the pair of measures — widely perceived as the most business friendly of the lot — would likely reduce the exposure companies face under the existing cybersecurity regime, according to attorneys.

Under the data breach proposal, which the administration has named the Personal Data Notification and Protection Act, a company would be required to alert consumers of a data breach within 30 days of discovering it. While the measure would bind companies to a strict reporting deadline, it would

ultimately ease their liability by replacing the current patchwork of 47 state breach notification laws with a single nationwide standard.

“The way it works now, if a company is a victim of a cyberattack, it's that company’s obligation to comply with the notification laws of every affected state, which is extremely burdensome and time consuming,” Kramer Levin Naftalis & Frankel LLP partner Erica Klein said. “With uniform federal guidelines, a company’s liability would likely decrease, because its reporting obligations would be more clear, and compliance would be easier for a company to determine and achieve.”

Under a single federal law, companies would not have to worry as much about complying with 46 state laws but "tripping up" and being exposed to liability under the 47th, according to Skadden Arps Slate Meagher & Flom LLP privacy group head Stuart Levi.

“It would make it far easier and cheaper to manage data breach notifications,” Levi said.

The information-sharing proposal floated Tuesday would also clamp down on the threat of lawsuits or investigations by federal and state agencies for missteps in disclosing information about cyberattacks. It would create what the White House described as “targeted liability protection” for companies that share “appropriate cyberthreat information” with the U.S. Department of Homeland Security’s National Cybersecurity and Communications Integration Center.

“Certainly, companies want to ensure that they're not going to incur liability for sharing information with the government and that the information will be protected from disclosure without their consent,” WilmerHale partner Benjamin Powell said.

Still, if companies are uncertain about what exposure they may face for turning over information about their systems and cybersecurity defenses to the government, the initiative is likely to fall apart, attorneys noted.

“Liability protection is a critical component of a voluntary cyber information-sharing program,” Mayer Brown LLP partner Howard Waltzman said. “Without meaningful liability protection, companies will be hesitant to participate because any act or omission made by a participant based upon cyberthreat information received by that entity could subject it to liability.”

Companies were quick to note that nuances that are yet unknown to the public or that might be introduced by lawmakers later in the process could easily dismantle the liability shield.

“These are all good ideas, but the devil will be in the details, and for now, these announcements have only created more questions than answers,” said Shook Hardy & Bacon LLP data security and data privacy practice co-chair Al Saikali.

On the data breach side, questions remain over a number of issues, including what type of incident that would trigger notification, how long the time period for that notification would be, who would be responsible for enforcing the statute and if the federal law would preempt more restrictive state laws.

The proposal outlined by the president on Monday did not mention preemption, but if lawmakers allow states to continue to set more stringent standards, the liability benefits of having a federal rule will likely evaporate, attorneys said.

“Having a unified national standard that preempts state laws is in everyone's interest because it improves efficiency for companies and clarity for consumers,” Haynes and Boone LLP associate Emily Westridge Black said. “The goal of a notification law is to get people the information they need to protect themselves in the most timely and efficient manner possible, and having a unified standard accomplishes that goal.”

Confusion over when the clock for data breach notification begins and whether there are any safe harbors that would allow companies to delay or escape their obligations could also chip away at the potential liability benefits of the administration's proposal, attorneys say.

“In many ways, a bright line can trigger more uncertainty rather than less,” Jones Day of counsel Jay Johnson said.

On the information-sharing front, companies will need to pay careful attention to how broadly “liability protections” are defined, as the administration's proposal Tuesday offered few details on the subject. The White House, however, did note that to qualify for liability protection, companies would have to comply with certain privacy restrictions, such as removing unnecessary personal information and taking measures to protect any personal information that must be shared.

If the privacy requirements end up being too unwieldy, companies that participate may end up running the risk of being hit with liability for failing to adequately protect the data they share, attorneys noted.

"Companies generally support the idea of information-sharing, but if they find they aren't getting the liability protections they need, they will push back,” Levi said.

--Editing by Kat Laskowski and Chris Yates.
