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

Cybersecurity Bill Enjoys Better Prospects After Exec Order

By **Allison Grande**

Law360, New York (April 22, 2013, 9:28 PM ET) -- The U.S. House of Representatives passed a controversial cybersecurity bill last week that would boost information sharing between the public and private sectors, and while the measure may still falter over the same privacy concerns that doomed it last year, attorneys believe that momentum built by a recent executive order should ultimately push it to passage.

The House approved H.R. 624, the Cyber Intelligence Sharing and Protection Act, in a 288-127 vote Thursday. The largely Republican-backed measure, which would encourage the government and private companies to voluntarily share information on cyberthreats, passed with the support of 92 Democrats and the opposition of 29 Republicans.

The legislation garnered more support from Democrats than similar cybersecurity legislation that failed to be considered in the Senate after receiving the support of only 42 House Democrats last April, with many opponents citing concerns that the bill did not adequately protect individuals' personal information. Attorneys say the increased backing this year reflects a heightened urgency to address cybersecurity threats that is likely to result in a better outcome for the revamped bill this legislative session.

“Information sharing is the one big cybersecurity topic about which there is consensus in business and government — which makes it all the more likely that something like CISPA will emerge,” Hogan Lovells partner Harriet Pearson told Law360 on Monday.

President Barack Obama endorsed the approach proposed in the House bill when he signed an executive order in February that pushed the government to work with banks, electric grid operators, communications providers and other critical infrastructure companies to establish voluntary cybersecurity standards and share information about cyberthreats.

But the White House has been less than supportive of CISPA, saying last week that the president would veto the legislation unless it's amended to require that private companies remove irrelevant personal information when sending data to the government. But attorneys say the president's strong push for enhanced cybersecurity protections make it more likely that his administration would be willing to work out a compromise that will allow the private and public sector to better share data.

“The game changer is the executive order,” BakerHostetler privacy, security and social media team co-leader Gerald Ferguson said. “By saying that there's a real need for legislation to promote and protect information sharing, the administration has put itself in a position where it is going to want to sign CISPA as long as there can be some steps take to address privacy concerns.”

The executive order also squarely addressed a central criticism of CISPA that greatly contributed to its demise last year: that it failed to establish standards that critical infrastructure operators would either be required or incentivized to implement in order to protect their networks.

While attorneys agree that the establishment of at least best practices is still necessary, the executive order's creation of a process, led by the National Institute of Standards and Technology, to develop a framework of voluntary cybersecurity best practices within the next year removes the pressure to make the component a feature of legislation immediately.

“With the executive order in the process of being implemented, I think that makes it even less necessary to try to enact critical infrastructure requirements,” Mayer Brown LLP partner Howard Waltzman said. “Even though the administration has been continuing to call for it … many companies think that the process should be permitted to unfold before Congress contemplates statutory requirements.”

The chance for passage this legislative term is also enhanced by another year of companies and the government experiencing cyberintrusions, which has brought with it the mounting realization that no industry sector is safe from attack, according to attorneys.

“There is no question that this issue cries out for congressional action, and few members of Congress will want to be seen as the ones who stymied a much-needed security measure,” Hunton & Williams LLP global privacy and data security practice head Lisa Sotto said. “The atmosphere with respect to cyberthreats is highly charged and therefore highly susceptible to bipartisan action.”

The facilitation of voluntary information sharing would be an important first step toward addressing the growing threats by pairing the intelligence-gathering capabilities of the government with the technical analyses done by companies that experience intrusions, experts say.

“The groups carrying out these attacks are not robots; they're human,” said Neal Pollard, a director with PricewaterhouseCoopers LLP who focuses on cybersecurity consulting. “It's important to get knowledge of not only what they are doing with the information, but [also] what they are after, because that will help companies place their resources much more effectively.”

While CISPA secured enough votes in the House to override the president's threatened veto, it still faces an uncertain future in the Senate, which refused to take up the bill last year and has yet to say if it will take a similar step this year.

Like in the House, support in the Senate for legislation that would facilitate information sharing for cybersecurity purposes is high, making it likely that the upper chamber will try to come to an agreement on an amended version of CISPA that addresses some of the privacy concerns that fueled opposition to the House bill, according to attorneys.

“The main concern is that a provision needs to be put in the bill that prevents personal information from being transmitted from businesses to the government, and that protection for personal information is not in CISPA,” Weil Gotshal & Manges LLP partner Michael Epstein said. “If the Senate is gong to pass it, they'll probably pass a version that addresses the privacy concerns, and then the question is going to be whether the House and Senate can agree on a common version, which is likely to be challenging because the House knew what the concerns were and didn't address them in the version it passed.”

But attorneys say it is promising that House lawmakers were willing to add several amendments to the bill to limit the sharing and use of sensitive personal data, including provisions that would stipulate that shared information can only be used for cybersecurity purposes and that would require the data to go through a civilian agency before being handed to the military.

"[A] big takeaway is the House leadership's willingness now to compromise on the privacy issues," Pearson said. "It remains to be seen whether the privacy amendments offered and enacted last week are sufficient to ease advocates' concerns about corporate information being shared with the intelligence community, but at least they were sufficient to get new votes."

--Editing by Elizabeth Bowen and Chris Yates.