BUSINESS INSURANCE.

Cyber breaches could prompt cooperation in Congress

Breaches expected to prompt Congress into action

By Judy Greenwald
November 23, 2014

Congress Could Cooperate on Cyber Security

With Republicans gaining control of the U.S. Senate in January, long-stalled cyber security legislation finally stands a strong chance of gaining approval by Congress and being signed into law.

Despite a Democratic president, there should be enough areas of agreement —such as the desire for voluntary cyber security standards for businesses — between a Republican-led Congress and President Barack Obama to enable the parties to forge a bipartisan compromise on the legislation, expert say. Even ongoing, thorny concerns over people's privacy are not expected to ultimately scuttle the measure.

“It's safe to assume it will be a No. 1 priority” with the next Congress, Norma M. Krayem, a principal with law firm Patton Boggs L.L.P. in Washington, said of working on finalizing cyber security legislation.

“Having both houses in the hands of one party is going to be very, very helpful. It will be easier for the two houses of Congress to come to a greater agreement with regard to what ought to be in the legislation,” said Larry Clinton, president and CEO of the Arlington, Virginia-based Internet Security Alliance, a multi-industry trade association.

“This was much harder with a divided Congress,” he said.

Another factor, Mr. Clinton said, is that “this issue has matured.” Historically, major pieces of legislation “rarely pass when they first come up. It takes a little while for the members of Congress to be comfortable with the issue ... I think we're in the same situation now with cyber security.”

Indeed, the issue of cyber security burst into the national forefront this year with the series of high-profile and costly data breaches affecting the public and private sectors.

“There have been enough committees who have done some research on it” and have paid attention to the numbers to the point where they are “more comfortable with the issue than they have been, so that helps,” Mr. Clinton said.

In addition, “there's a great deal more coherence to the president's approach and that of the Republicans, so I think ... we can potentially see some substantive legislation in this area,” Mr. Clinton said.

The only mitigating factor will be the time it takes for incoming Senate committee chairmen, including those for homeland security, government affairs, intelligence and commerce, to assess their take on cyber security, “not whether they plan to do anything about it,” Ms. Krayem said.

Mauricio Paez, a partner with law firm Jones Day in Washington, said there are still divergent views within the political parties on issues including the requirements that should be imposed on companies for data breach notification, “and a host of other hot-button issues for data breach response.”

However, “The change in Congress shows that there's likely to be more debate around the issue and potentially a bit more consensus building,” Mr. Paez said. “There is an opportunity, I think, for getting some areas addressed,” including information sharing.

If the new Senate chairman wanted to go off in a “substantially different direction, that would have to play itself out,” between the administration, the private sector and Congress, Ms. Krayem said.

“You have an outgoing president who is interested in the issue,” and there is “much less distance between Republicans and Democrats on cyber security” than there had been before, Mr. Clinton said.

A GOP task force has issued recommendations on cyber security that “doesn't look terribly different than what is essentially proposed in President Obama's executive order on cyber security,” which was issued in May 2013, he said.

Mr. Clinton said both the GOP task force and the president propose a voluntary program, and standards for best practice, and call for the development of market incentives to promote their voluntary adoption by companies.

Mr. Clinton said he does not expect anything regulatory in nature to be approved, “but there will be incentives for the private sector to engage in a variety of pro-security actions,” such as liability protection for sharing more information.

NIST framework

There also may be incentives put in place to “promote the wider use” of the National Institute of Standards and Technology's proposed voluntary cyber security framework, Mr. Clinton said.

In addition, he said, “I wouldn't be surprised if there is probably some streamlining of current regulatory bodies, perhaps something done to promote insurance use, various market incentives” and perhaps some benefits provided to firms that “demonstrate higher degrees of security.”

For instance, many businesses are seeking some uniformity of rules regarding data breach notification.

In the incoming Congress, "we could see them actually coalescing around" uniform data breach notification standards, said Francine E. Friedman, Washington-based senior policy counsel with law firm Akin, Gump, Strauss, Hauer & Feld L.L.P.

Privacy is likely to continue to be a sticking point to a certain degree, though, some experts say.

Harley Geiger, advocacy director and senior counsel at the Washington-based Center for Democracy and Technology, said that although he would expect continued pressure on Congress to pass cyber security legislation, the issue is whether it will "allow information about civilians to go directly to the National Security Agency, or some other federal agency such as Homeland Security, before going to the NSA" and then used for law enforcement purposes.

"The administration under President Obama has done enough to create privacy and civil liberties concerns, that I think the bulk of Republicans will adopt those concerns, and not want to hand the Administration any more powers," said Jim Harper, a senior fellow with the Washington-based Cato Institute.

However, David LeDuc, senior director of public policy for the Washington-based Software & Information Industry Association said that while it is still a consideration, he thinks the privacy issue is an impediment that "can certainly be overcome."