Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data Security Gets New Look With Insurance Tax Credit Bill

By **Allison Grande**

Law360, New York (September 20, 2016, 10:52 PM EDT) -- A House lawmaker's proposal to give a tax credit to companies who purchase data breach insurance and implement a widely respected cybersecurity framework is likely to win backing for its approach of encouraging rather than requiring robust protections, but questions about how strong safeguards will actually need to be is likely to raise roadblocks.

Building on the wealth of legislative and regulatory proposals floated in recent years to combat the growing spate of cyberattacks that have hit businesses in a range of sectors, Rep. Kevin Perlmutter, D-Colo., on Thursday floated H.R. 6032, the Data Breach Insurance Act.

However, unlike the vast majority of its predecessors — including tough cybersecurity rules for financial institutions proposed by the New York Department of Financial Services last week — Perlmutter's bill doesn't mandate compliance, but instead proposes to give a 15 percent tax credit to companies who purchase data breach insurance coverage and adopt the National Institute of Standard and Technology's voluntary cybersecurity framework.

"There's a lot for businesses to like about the bill," Debevoise & Plimpton LLP partner Jim Pastore said. "Among other things, it's a sharp departure from other government guidance — including, most recently, the NY DFS proposed cybersecurity regulations — that seek to rule with the stick, and not the carrot."

Given that both lawmakers and regulators have tended to take more of a "stick" rather than a "carrot" approach to cybersecurity to date, this shift is likely to not only win favor among businesses, but could also help to improve their cybersecurity posture in general, attorneys say.

"The basic concept [is] that it is much better to be encouraging investment in cybersecurity rather than demanding it," Pillsbury Winthrop Shaw Pittman LLP's privacy practice co-chair Brian Finch said. "Incentives will only encourage reasonable, flexible and innovative measures to improve cybersecurity."

But despite the potential upshot to adjusting the traditional focus when it comes to cybersecurity, the change also brings with it an array of issues, including who will pay to incentivize companies and if the security improvements will be worth the cost.

"If taxpayers are indirectly subsidizing these security measures, then one certainly hopes the insurance product is going to deliver and it's not going to be business as usual with either policyholders not

protecting their systems as well as they should, or having insurance companies take kind of an unduly narrow interpretation of cyber insurance and start fighting claims," Anderson Kill PC shareholder Joshua Gold said.

How compliance will be determined with the second of Perlmutter's "two-prong approach" to encouraging better cybersecurity hygiene — namely, that companies adopt the NIST framework or a similar standard approved by the Secretary of the Treasury — will also be vital to determining whether the plan will deliver any real security improvements, attorneys added.

"The bill is so bare that it leaves a number of important questions unanswered, [including] how will compliance with NIST or any other standard be determined and enforced," Shook Hardy & Bacon LLP data security and privacy group co-chair Al Saikali said. "Compliance with NIST or any other standard is going to be based on a snapshot in time, so a company could go out of compliance one month or one day after an audit is completed, yet they would still have the benefit of the tax credit."

The move to link adherence to the NIST framework with cybersecurity insurance makes sense, attorneys say, given that both elements are increasingly being recognized as vital to having a robust data security plan.

The voluntary NIST framework since its release in February 2014 has been increasingly gaining praise as an effective tool to help evaluate cybersecurity risks and implement tailored security programs, while demand for cyber insurance coverage has been steadily growing, especially as finding coverage under traditional policies for novel cybersecurity claims becomes more difficult.

"When you look at the NIST framework, there are two parts of being prepared: one is identifying your risks, and the other is what to do about risks,"Ballard Spahr LLP of counsel Kim Phan said. "The NIST framework helps to address the first part, while cyber insurance falls into what do you do about the risk."

K&L Gates LLP partner Roberta Anderson noted that the drive to link these two elements began even before the NIST framework took effect. In August 2013, the White House released a list of possible incentives that could be offered to critical infrastructure operators that agreed to adopt the NIST framework, with lower rates for cybersecurity insurance being at the top of the list of proposed incentives.

"The Data Breach Insurance Act is the most recent concrete example of the way in which the government is seeking to utilize the insurance market in conjunction with the NIST framework for the evaluation, elevation and advancement of enterprise-wide cybersecurity risk management," Anderson said, adding that the two elements are increasingly being viewed as a catalyst for helping to evaluate and curtail cyber risks and that the tools "appear to be working effectively and in harmony."

As with any legislative proposal that involves a tax credit, the main question plaguing the representative's bill is whether it will actually incentivize more widespread adoption of the desired behavior, or if it's just going to reward companies that are already undertaking the tasks that the bill is hoping to promote, Akin Gump Strauss Hauer & Feld LLP senior policy counsel Francine Friedman said.

"It could provide some level of incentive for the insurance marketplace to develop or to increase adoption of the NIST framework, but as is often the case with these types of bills, it's hard to know at the outset what impact it will have," Friedman said, although she pointed out that the bill as currently

drafted does have a five-year sunset provision that could help in making sure this issue is adequately addressed.

When it comes to purchasing cyber insurance, a myriad of factors including the complexity, inconsistent pricing and relative youth of the marketplace could impact whether more companies decide to sign up for policies and, if they do, if the coverage will provide any actual benefits to themselves or consumers, attorneys say.

"There are many kinds of data breach insurance though, and it takes diligence to make sure that the particular policy purchased is correct for your type of business," Pepper Hamilton LLP partner Sharon Klein said. "A one-size-fits-all is not very effective."

On the one hand, getting a 15 percent tax credit could encourage companies interested in cyber insurance but wary of the mounting price tag to take the plunge and reap the benefits of coverage, which include not just getting protection from the onslaught of litigation and other steps companies need to take in response to a breach, but also getting access to learning materials and forensic experts that insurers often provide to their insureds.

Or on the other hand, with the average cost of a cyber insurance policy currently clocking in at around $1 million, while the average cost of a data breach is closer to $4 million, the tax credit could just prompt those who already have insurance to up their coverage limits, attorneys noted.

"Conceptually, the bill provides businesses with another tool for them to be able to seek out additional cyber insurance coverage," Phan said. "Whether or not that ultimately results in additional protections for consumers remains to be seen."

Perlmutter's proposal also sparks hope that the NIST framework, which according to the lawmaker has so far been adopted by 30 percent of businesses to manage their cyber risk, will rise to the level of a somewhat de facto cybersecurity standard.

"It's not an insignificant task to comply with the NIST framework, so if a company can do that and achieve some tax savings, that could be very helpful and make it a good investment," Mintz Levin Cohn Ferris Glovsky & Popeo PC attorney Brian Lam said.

However, achieving broad buy-in may not prove to be that easy, since the NIST framework was designed specifically for critical infrastructure operators and was drafted as a blueprint that could be implemented rather than a true standard that can be adopted, attorneys noted.

While the bill ultimately may not end up gaining any traction, given the lack of success Congress has had in recent years pushing through cybersecurity bills in general and the recent push to simplify the tax code, Perlmutter's proposal shouldn't be ignored, attorneys say.

"The ability to offer the carrot instead of the stick is important, and if a comprehensive bill on this topic were ever to be passed in Congress, this type of incentive could come up and be part of that discussion now that it's been put out there," Friedman said.

--Editing by Philip Shea and Catherine Sum.