New York tests the limits of cybersecurity rulemaking, experts say

(September 14, 2016) - Cybersecurity regulations proposed by New York for banks, insurers and other financial firms licensed in the state would go far beyond what other states and even the federal government have required, experts say.

"New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises," said Gov. Andrew Cuomo in a prepared statement. "This regulation helps guarantee the financial services industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible."

The rulemaking would essentially codify existing best practices at large banks and insurance companies.

"This is regulations for public relations," said Jacob Frenkel, a member of Dickinson Wright PLLC. "Every financial institution understands the legal and reputational risks already and acutely. Financial institutions and major corporations are dedicating substantial resources — human capital and dollars — to cyber."

Yet compliance will be difficult for small and medium-sized firms, with elements such as much broader use of encryption, a 72-hour data breach reporting requirement and detailed specifications for testing, risk assessment, multi-factor authentication and the hiring of a chief information security officer.

"Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances," according to the proposed rule's preamble.

However, the specific requirements in New York's proposed regulation do not align with the risk-based approach generally found in existing federal and state cybersecurity regulations and guidance.

"This raises the bar and goes beyond everything that exists today, in my view," said Nathan Taylor, a partner at Morrison & Foerster LLP and co-author of "The Law and Financial Privacy." If adopted, the proposal "would in fact create the most detailed, onerous and prescriptive data security regime in this country," he added.

Small firms would be exempt from some parts of the regulation, such as testing, multi-factor authentication and the hiring of a chief information security officer, if they have fewer than 1,000 customers, less than $5 million in gross annual revenue and less than $10 million in assets.

However, even the smallest firms would still have to develop a comprehensive cybersecurity policy, covering at least 14 points listed in the regulation "at a minimum." In addition, all firms would have to notify the New York Department of Financial Services within 72 hours of learning about "actual or potential unauthorized" tampering with nonpublic information.

Most of the 47 states with data breach notification laws require notice within 30 to 60 days, according to Mark Schrieber, a partner at McDermott Will & Emery and leader of its cybersecurity and data privacy practice.

"This really is extraordinary, and I don't use that word lightly," he said. "This is about as broad as anything I've seen."

Experts say the definition of "nonpublic information" is very extensive, including the mention of an individual's name. The rub is financial firms would be required to encrypt nonpublic information in transit and at rest.

"You would have to encrypt every email you send a customer, even though it may not be sensitive," Taylor said.

"New York is using too much stick here, they need to offer more guidance on what will satisfy this regulation," said Brian **Finch**, a partner at Pillsbury Winthrop Shaw Pittman LLP. He said the regulation should be modified to include risk-based performance standards, a safe harbor for compliance and an explicit appeals process "with the burden on the state to show that the covered entity has failed to meet its obligations."

Taylor added that "what it creates is a ton of regulation out there that may not be well thought out, which creates a rapidly evolving compliance nightmare. On the whole these efforts will revitalize calls to Congress, which has spent more than a decade considering data security and data breach notification bills."

By Paul Merrion, CQ Roll Call

End of Document