The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2016
PHILADELPHIA, OCTOBER 11, 2016 VOL 254 • NO. 71 An ALM Publication

NY Cybersecurity Regs Could Spur Legal Work Nationwide

BY ZACK NEEDLES
Of the Legal Staff

Attorneys around the country are already fielding calls from clients about New York's recently proposed cybersecurity regulations for financial institutions and insurers, which, if enacted, could have both immediate and long-term implications far beyond the state's borders.

Scott T. Lyon, a technology, cybersecurity and data privacy attorney in Sedgwick's Irvine, California, office, said the proposed regulations are of keen interest to financial services and insurance-related companies throughout the United States, whether or not they do business in New York.

"Even if they don't, they're thinking: OK, what's my state going to be doing? Is this going to be the model? How long is it going to take another state to clone this program and roll it out? What are federal regulators going to do?" Lyon said.

And the likelihood of New York's regulations serving as a national model is high, according to Richard M. Borden, a former cybersecurity lawyer with Bank of America who is now counsel at Robinson & Cole in Hartford, Connecticut.


LEVY


LANDON

"It would not surprise me if this or something very close to it were adopted [elsewhere] at the state and even federal level and for different industries," Borden said, calling the proposed regulations, released by the New York Department of Financial Services on Sept. 13, "very comprehensive, tightly written and extremely thoughtful" and comparing them in scope to the Sarbanes-Oxley Act of 2002.

Kevin M. Levy, chair of the technology transactions group at GrayRobinson in Miami, said the DFS proposals represent a step toward the future of cybersecurity regulation in the United States, focusing more on protecting data on the front end as opposed to simply requiring companies to have adequate data breach response plans.

"This is pushing us a little bit toward the European laws, which are all about what you have to do with the data and how you collect it," Levy said.

But cybersecurity lawyers across the country may not have to wait for other states to adopt

New York's approach before they see an increase in business.

If enacted as written, the proposed rules would require all state-regulated banks and insurers to annually assess their cyber vulnerabilities; develop comprehensive data and system protection policies as well as immediate response plans for security breaches; and designate a chief information security officer (CISO).

A 45-day public comment period began Sept. 28 and the regulations are scheduled to go into effect Jan. 1, 2017, after which covered entities would have 180 days to comply.

The would-be mandates are not necessarily ground-breaking—they incorporate ideas from federal regulations like the Securities and Exchange Commission's Regulation Systems Compliance and Integrity and most of the major financial institutions and insurers already have similar measures in place. But what is special about the DFS regulations, attorneys said, is the level of accountability they demand.

For example, the regulations would require companies to have detailed written cybersecurity policies that a board of directors must review and a senior officer must sign off on. The company's designated CISO would also be required to submit a report, at least biannually, to the board detailing the effectiveness of the policy.

Covered entities would also be required to submit to the DFS an annual certification of compliance and would have 72 hours to notify the agency of "any material risk of imminent harm relating to its cybersecurity program."

"This is the first time we really have a regulation that is directly covering these risks in a comprehensive manner," Borden said. "You have a lot of very good people at all of these places who are trying really hard—they're all worried about [cybersecurity]. What this does is provide consistency and accountability."

And that accountability doesn't end with the state-regulated businesses.

REGULATION BY ASSOCIATION

Section 500.11 of the DFS proposal would require state-regulated financial institutions and insurers to demand that any third-party vendors with access to the covered entities' information systems or nonpublic information agree to adopt similarly stringent cybersecurity policies.

If that section is enacted, data protection would necessarily become a key aspect of contract negotiations between state-regulated institutions in New York and their service providers—and cybersecurity lawyers said they see opportunity.

Shawn Tuma, a cybersecurity lawyer at Scheef & Stone in Dallas, said he's recommended for years that his clients require their outside vendors to contractually agree to adopt data protection measures.

"[The vendors] tell us to go pound sand," he said. "They say, 'We're not doing this, it's just your policy.' Now we would be able to say, 'No, this is a legal obligation.' That gives us a lot of negotiating leverage."

New York financial and insurance businesses "contract with hundreds of vendors and reviewing those contracts is going to be another burden for institutions" on top of the internal infrastructure changes they'll need to make, said Jana M. Landon, who chairs Stradley Ronon Stevens & Young's e-discovery team in Philadelphia and advises clients on data security.

Landon likened the potential effect of the DFS regulations' third-party provisions to the process health care providers went through in the wake of the Health Insurance Portability and Accountability Act of 1996, which similarly required covered entities to obtain assurances from their business associates that health information would be safeguarded.

"They sometimes had to have entire divisions just dealing with contract negotiations," Landon said.

Landon also noted that for vendors who don't already have comprehensive cybersecurity plans in place, the New York regulations would require a "significant investment" that could prove cost-prohibitive for some companies.

"Will this actually push any vendors out of the market? If they

can't comply with regulations, they can't do business [with a covered entity]. If all of New York is doing that, the vendor market is going to become a lot smaller," Landon said.

But to the extent that vendors are willing and able to comply with the terms, the third-party provisions proposed by the DFS could also have the effect of strengthening cybersecurity across a number of industries.

"Through [covered entities'] contractual relationships, it's going to regulate the field," Tuma said. "That's a slow process. That takes year one for the regulated institutions to comply, then it takes time for their legal teams to realize, 'Oh, we have to pass this along to the service providers,' and then the service providers say 'No' … but the impact is going to be substantial."

COST AND EFFECT

In terms of compliance, a more immediate concern for lawyers may be the requirements the DFS regulations would place on the covered institutions themselves.

Some banking and insurance industry attorneys have decried the proposals as "onerous" and "inflexible."

Cybersecurity lawyers acknowledged that compliance could be challenging for midsized and smaller companies, particularly if precautions like annual penetration testing—in which companies assess the integrity of their security by trying to infiltrate their own systems—are not already part of their routine.

"If a company or an institution has not done this yet or hasn't done much of this, it's going to require significant amounts of work," Borden said. "It may end up leading to companies outsourcing certain types of activities because they aren't going to be able to hire."

Even for the major companies that are already ahead of the curve on cybersecurity, there are concerns. What happens if something does go wrong?

"There is no such thing as perfect cybersecurity," said David W. Opderbeck, a cybersecurity lawyer at Gibbons in Newark, New Jersey. "You can do testing and penetration and still get breached. So what does that mean? How will this be enforced?"

But the consensus among cybersecurity lawyers appears to be that regulations like those drafted by the DFS are necessary in an era in which multimillion-dollar cyberheists and hacker-induced bank shutdowns are no longer merely the stuff of 1980s action movies.

Not to mention the myriad problems that can occur because of something as simple and innocent as a bank employee accidentally downloading ransomware.

"This to me is about trust—trust in the financial system—and having regulation that helps to sustain trust in the financial system," Borden said, analogizing the DFS cybersecurity regulations for banks and insurers to fire codes for commercial buildings. "In many ways it's like that. If there's a fire, you know that certain things are going to happen and you can trust that they will. Bad things can happen. We don't want that financial fire."

And, as with any new regulations, companies will likely need to turn to their outside counsel for compliance advice. That need may be particularly acute when the subject is cybersecurity, lawyers said.

"Legal departments haven't built up expertise [in cybersecurity] except at large corporations where they deal with these issues regularly," Borden said.

Tuma agreed that the demand for lawyers who understand cybersecurity is not likely to wane any time soon.

"As much as I love the theory and philosophy, at the end of the day I'm following this because I see business," he said.

Zack Needles can be contacted at 215-557-2373 or zneedles@alm.com. Follow him on Twitter @ZackNeedlesTLI. •