NY’s Cybersecurity Rules for Banks, Insurers, Financial Services

Christopher M. Brubaker, The Legal Intelligencer

March 7, 2017

The New York Department of Financial Services' new cybersecurity rules applicable to banks, insurance companies and other financial services companies, 23 NYCRR 500, went into effect on March 1. While most states have some form of data breach notification standards, and some states have security standards generally applicable to personal data, these are the first state-mandated cybersecurity regulations applicable to specific industries. The federal government has had industry specific requirements in place for some time, most notably in health care under HIPAA and HITECH, and for banks and other financial services companies under Gramm-Leach-Bliley. The N.Y. cyber rules while similar in many respects to existing federal regulations are more specific in certain key aspects and include mandates for companies to have a chief information security officer (CISO) and for top level executives to review and certify compliance with the new rules on an annual basis. These requirements have already fueled speculation that one of the biggest impacts of the rules will be heightened litigation in the wake of a cyberincident based on the certifications of executives regarding a company's cybersecurity practices.

The rules apply to "covered entities," which are defined to include any person operating under or required to operate under a license, registration, charter or similar authorization under New York's Banking, Insurance or Financial Services Laws. (As used herein terms are specifically defined in section 500.01.) The N.Y. cyber rules impose a number of requirements on covered entities including: maintaining a cybersecurity program (500.02); maintenance of a written policy or policies detailing the steps to be taken to protect information systems (500.03); designation of a CISO who is to provide at least annual reports to the board of directors or equivalent governing body (500.04); to conduct periodic penetration testing and vulnerability assessments (500.05); the ability to reconstruct material financial transactions and maintenance of audit trails designed to detect and respond to cybersecurity events (500.06); limitation of access to nonpublic information (500.07); specific guidelines for the creation of in-house developed applications and evaluation of externally created applications (500.08); conduct periodic risk assessments sufficient to enable the creation of a cybersecurity program required under the NY Cyber Rules (500.09); utilize qualified cybersecurity personnel to perform or oversee the performance of core cybersecurity functions (500.10); implement written policies and procedures for interaction with third party service providers (500.11); utilization of multi-factor and risk based authentication (500.12); limitations on data retention (500.13); monitoring activity by authorized users to develop risk-based controls to prevent unauthorized use or access by such users and regular cybersecurity awareness training for all personnel that is updated to reflect risks identified in the risk assessment (500.14); encryption of nonpublic information in transit over external networks and at rest (500.15); establish written incident response plan (500.16); and, notice to the superintendent within 72 hours of determining that a cybersecurity event occurred and annual certification of compliance to the superintendent (500.17). Other key aspects of the rules include the ability of affiliates to utilize a single

cybersecurity program. There are also certain exceptions including for covered entities with less than 10 employees including independent contractors, less than $5 million in gross annual revenue for each of the last three years, or less than $10 million in year-end total assets from the requirements of Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16. Also, employees, agents, representatives or designees of a covered entity that are covered entities themselves are exempt to the extent they are covered by the covered entity's cybersecurity program. Exempted covered entities must file a notice of exemption annually, and have 180 days from the end of its fiscal year in which it no longer qualifies for exemption to comply with the requirements.

The N.Y. cyber rules, like most regulations, are in the nature of a mandatory risk-management approach to cybersecurity. A risk-management approach is the generally accepted "best practice" method for cybersecurity. Essentially what types of data and information do you have, how is that data and information accessed, used and stored, what are the attendant vulnerabilities or risks associated with that data, and what protections or safeguards are available. Many of the requirements have been modified from the original proposed rules published in September 2016. The changes were in response to comments on the proposed rules and are generally along the lines of making the N.Y. cyber rules more fluid and flexible in terms of how they are implemented by any particular covered entity, and thus more in the nature of a true risk-management approach. For example, Section 500.02 regarding the cybersecurity program was revised to state that the program shall be based on the covered entity's risk assessment and address enumerated items rather than simply saying it will address the enumerated items. Another example is that the frequency of certain events was lessened. Penetration testing and vulnerability assessments need only be periodic if continuous monitoring is in place, otherwise penetration testing needs to occur at least annually and vulnerability assessments need to occur at least biannually. Originally penetration testing was required at least annually and vulnerability assessments were required quarterly. The risk assessment was also changed from annual to periodic.

The other major change made from the proposed regulations is that the requirements of the N.Y. cyber rules are now to be phased in affording Covered Entities more time to come into full compliance. The first round of compliance is to be within 180 days (Aug. 28), except as otherwise provided for by longer compliance periods; compliance with Sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(a)(2) within one year (March 1, 2018); compliance with Sections 500.06, 500.08, 500.13, 500.14(a)(1), and 500.15 within 18 months (Sept. 1, 2018); and, compliance with Section 500.11 within two years (March 1, 2019). The first compliance certification is due Feb. 15, 2018.

As a practical matter, compliance with many of these items should not be that difficult for entities that are already committed to robust cybersecurity measures and are in compliance with existing federal regulations. Many of the requirements are similar in nature to existing requirements for banks, insurers and financial institutions under existing federal law and are consistent with what is generally regarded as best practices with respect to cybersecurity. For example, regulations promulgated under Gramm-

Leach-Bliley already require board involvement with cybersecurity, risk assessments and cybersecurity programs. See, 12 C.F.R. Part 30 Appendix B (national banks) and Part 208 Appendix D-2 (state member banks). Likewise, best practices for cybersecurity involve employee training and awareness programs, regular monitoring of activity, and penetration and other vulnerability testing in order to identify suspicious activity and to identify weaknesses in the existing security protocol. With that said, compliance with the N.Y. cyber rules will likely cause added burden for most companies, in particular small and medium sized ones, because certain elements are mandatory and are not solely left to a risk benefit analysis. The risk assessment is the key component of the program as it drives what is required to comply with other sections and is mandatory for all covered entities even if exempt from certain of the other requirements. Again, for most companies committed to cybersecurity this will not be a major shift as this is a fundamental component of developing and maintaining a cybersecurity program. The real impact figures to be in the fact that periodic risk assessments are now mandatory, that a CISO must be appointed (even if a third-party is utilized for this role), and the reporting requirements. The reporting requirements include both annual reports from the CISO to the board of directors on enumerated topics as well as annual certifications by the board of directors or senior officers of compliance with the N.Y. cyber rules. As noted above, these requirements open the door for litigation against the board members or senior officers signing the compliance certification in the event of a data breach or other cyber event for fraud and similar claims along the lines of security fraud claims based on statements in required filings.

While no one can doubt the importance of strong and proactive cybersecurity, it remains to be seen if this is something that can be effectively addressed through regulation. The N.Y. cyber rules are certainly an ambitious attempt at providing a framework for comprehensive industry wide standards. There is already speculation that they will serve as the model for similar regulations in other states. Yet the question remains whether this will serve to truly increase cybersecurity, something that is much more art than science and is neither perfect nor one size fits all, or merely add another layer of regulatory burden and increased potential liability for the impacted industries.

Christopher M. Brubaker of Clark Hill concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups.