Kilpatrick

Insights: Alerts

Cyber Winter is Here, and Coming to Regulation: The New York Rules and the Future of Cybersecurity Regulation

September 27, 2017

Written by **Jon Neiditz**

The State of New York's response to two large cybersecurity breaches may fuel the transformation of the state regulation of corporate cybersecurity in the U.S. Unlike typical state data breach statutes which focus on notification to individuals about breaches of some types of personal information, New York's new cybersecurity rules impose minimum standards for protecting both critical business and individual nonpublic information, highlighting New York's concern with both consumer protection and the health of the financial sector. In response to the highly-publicized Equifax breach, on September 18, 2017, New York's Governor Andrew Cuomo directed New York's Department of Financial Services (NYDFS) to issue a proposed new regulation[1] requiring credit reporting agencies to comply with New York's high-bar Cybersecurity Requirements for Financial Services Companies (the "Cybersecurity Rules").[2] Governor Cuomo's action signals New York's willingness to expand its new model of cybersecurity regulation, mandating company's protect the confidentiality, integrity, and accessibility of not just individuals' personal information, but also material business information, which we call a company's "knowledge assets" or "crown jewels." On September 25, 2017, the Guardian reported that Deloitte Touche Tohmatsu Limited, the Big Four professional services firm with its operational headquarters in New York City, experienced a cybersecurity breach that affected its email system and client records, among the most critical nonpublic business information of a professional services firm.[3] What, aside from lobbying efforts, is to stop Governor Cuomo from proposing that the New York Cybersecurity Rules cover accounting firms as well?

The History of Cybersecurity Regulation

U.S. regulators have typically issued cybersecurity guidance instead of cybersecurity regulations, heeding legitimate industry concerns over prescribing ineffective "check the box" cybersecurity standards that do not make organizations more secure, and acknowledging that no "one-size-fits-all" cybersecurity solution exists. The ever-evolving nature of cybersecurity threats and technology makes cybersecurity regulation an especially challenging issue. In February 2014, the National Institute of Standards and Technology (NIST), in collaboration with industry and academia, published a voluntary cybersecurity framework to help organizations manage cybersecurity risk.[4] The Department of Homeland Security (DHS) offers voluntary programs and resources for critical infrastructure providers, and works to facilitate public-private cyber information sharing.[5] The Federal Trade Commission (FTC) provides cybersecurity guidance and brings enforcement actions against companies for unfair or deceptive practices that endanger the personal data of consumers.[6] As for credit reporting

agencies, while the Consumer Financial Protection Bureau (CFPB) has authority to enforce violations of consumer protection laws by consumer credit reporting agencies, and the FTC can bring civil lawsuits, the authority of the CFPB and FTC to monitor cybersecurity practices is less clear.

In 2011, noting the risks to registrants associated with cybersecurity, the Division of Corporation Finance of the Securities and Exchange Commission (SEC) released guidance regarding disclosure of cyber risks in SEC filings, noting that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." Focusing on what information an investor would find material in deciding whether to buy or sell securities registered with the SEC, the SEC pioneered disclosure focused on business risks rather than risks to personal information, noting that a cyber attack "may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners...[and] may also be directed at disrupting the operations of registrants or their business partners."[7]

New York's leading-edge Cybersecurity Rules became effective on March 1, 2017. Although the Cybersecurity Rules are risk- and process-based, the Cybersecurity Rules mandate certain governance and technical requirements, making compliance with the Cybersecurity Rules a significant effort for organizations subject to its reach. The Cybersecurity Rules far exceed federal and other state cybersecurity regulatory efforts to impose minimum cybersecurity standards.

New York Cybersecurity Rules – Overview of Requirements

The Cybersecurity Rules apply to an individual or non-governmental entity, including any non-governmental partnership, corporation, branch, agency or association operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law (a "Covered Entity").[8] The Cybersecurity Rules provide for a limited number of exemptions based on such considerations as the size of the entity.[9] NYDFS is not the licensing or regulatory authority for broker-dealers or investment advisers in New York, so those entities are not directly subject to the Cybersecurity Rules.

At the heart of the Cybersecurity Rules is a requirement for a Covered Entity to put in place a risk-based cybersecurity program that protects the confidentiality, integrity, and availability of nonpublic data.[10] Some key provisions include conducting periodic risk assessments, implementing and maintaining written cybersecurity policies, designating a chief information security officer (CISO), and implementing technical controls, including encryption and multi-factor authentication. Executive management must annually certify compliance with the Cybersecurity Rules.[11] The Cybersecurity Rules require the notification of the NYDFS within 72 hours after the identification of a breach.[12] The Cybersecurity Rules also require companies to implement written policies and procedures, including "minimum security standards," for third party service providers.[13] NYDFS is expected to vigorously monitor and enforce compliance with the Cybersecurity Rules.

New York Cybersecurity Rules – Nonpublic Information

Unlike typical state data breach statutes which focus on notification to individuals about breaches of some types of personal information, the Cybersecurity Rules focus on protecting both critical business and individual nonpublic information, looking to protect both consumers and the financial sector as a whole. Under the

Cybersecurity Rules, the definition of "Nonpublic Information" includes "business related information" that if tampered with, disclosed, or accessed "would cause a material adverse impact to the business, operations or security of the Covered Entity," as well as personally identifiable information.[14] By mandating that Covered Entities protect the confidentiality, integrity and availability of both personal information and business-critical nonpublic information, the Cybersecurity Rules reflect growing regulatory acknowledgement that actors, including nation states, are seeking to control, damage, and interrupt systems, and deny access to and destroy business-critical data. NYDFS is mandating that companies include both the protection of personal information and business critical information and systems in cybersecurity assessments and plans. Companies will need to determine what is material nonpublic information in the context of the Cybersecurity Rules, and where that nonpublic information is located on their information systems. Determining what information is most important to the company is foundational for compliance with the Cybersecurity Rules, and also for overall cybersecurity risk management.

New York Cybersecurity Rules: *De Facto* National Cybersecurity Standard?

New York's Cybersecurity Rules may become a de facto national cybersecurity standard with global reach. Covered Entities have interconnected systems. Many large institutions gain efficiencies by deploying centrally managed information technology platforms and cybersecurity programs and tools. Thus, if only a part of an organization falls under the Cybersecurity Rules, it would be impractical for the larger enterprise not to adhere to the Cybersecurity Rules. Further, the requirement in the Cybersecurity Rules for a Covered Entity to implement written policies and procedures, including "minimum security standards," for third party service providers may change the vendor landscape throughout the country and abroad. Any vendor working with a Covered Entity will need to conform their security practices to the Cybersecurity Rules. Vendors that cannot meet security requirements will be replaced.

Post-Equifax and Deloitte Breaches – Proposed Regulation Requiring Credit Bureaus – and Who Else? – to Comply with New York Cybersecurity Rules

As noted above, in response to the Equifax breach, on September 18, 2017, Governor Cuomo directed the NYDFS to issue a proposed regulation requiring credit reporting agencies to register with the NYDFS for the first time, and comply with the Cybersecurity Rules.[15] The annual reporting obligation required by the proposed regulation would allow the NYDFS Superintendent to deny and potentially revoke a credit reporting agency's authorization to do business with New York's regulated financial institutions and consumers if the credit reporting agency is found to be out of compliance. Governor Cuomo called the Equifax breach a "wake-up call" and made a call to action to other states noting "New York is raising the bar for consumer protections that we hope will be replicated across the nation."[16] New York Financial Services Superintendent Maria T. Vullo reinforced the need for the Cybersecurity Rules, noting that the "data breach at Equifax demonstrates the necessity of strong state regulation like New York's first in the nation cybersecurity actions."[17] This proposed regulation[18] of credit reporting agencies is subject to a 60-day public comment period, at which point New York State officials expect the proposed regulation to be adopted.

New York's actions after the Equifax breach demonstrates that New York will attempt to regulate any company that might put the financial sector or New York consumers at risk; interstate commerce and federal preemption challenges will no doubt follow, but particularly following disclosure of a cybersecurity breach at Deloitte, professional services firms serving the financial sector should be watching this proposed regulatory expansion

carefully. In addition, other states have already passed cybersecurity regulations similar to the Cybersecurity Rules. For example, the Colorado Securities Divisions recently published a new regulation requiring broker-dealers and investment advisers to implement written cybersecurity procedures and conduct cybersecurity risk assessments, among other requirements.[19] It will be important to monitor developments in other states in the upcoming weeks.

Going Forward

As of August 2017, Covered Entities should already be in compliance with the first of four tranches of Cybersecurity Rules' requirements, and actively working to meet the rest of the requirements, which will phase in over the next two years.[20] In light of the newly proposed New York regulation, credit reporting agencies should be actively getting up to speed on the Cybersecurity Rules, assessing gaps in their cybersecurity programs, and putting plans in place to comply with the Cybersecurity Rules. Putting best practices in place will also benefit credit reporting agencies and other entities working to keep or restore trust, and improve their cybersecurity posture, following recent breaches. Even for entities not subject to the Cybersecurity Rules, conducting risk assessments and implementing robust cybersecurity programs should reduce the likelihood and severity of a breach, and enable companies to respond to and recover from any incident more effectively. Companies adopting best cybersecurity practices will protect their business operations and reputations, reduce regulatory and litigation exposure, and be in the best position to comply with a regulatory environment that is constantly evolving and taking a sharp turn into broader and deeper cybersecurity mandates.

---

[1] "Governor Cuomo Announces New Actions to Protect New Yorkers' Personal Information in Wake of Equifax Breach," September 18, 2017. https://www.governor.ny.gov/news/governor-cuomo-announces-new-actions-protect-new-yorkers-personal-information-wake-equifax.

[2] New York State Department of Financial Services 23 NYCRR 500. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[3] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.

[4] See "Framework for Improving Critical Infrastructure Cybersecurity" at https://www.nist.gov/cyberframework.

[5] See https://www.dhs.gov/topic/cybersecurity.

[6] See https://www.ftc.gov/datasecurity.

[7] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[8] 23 NCRR 500, Section 500.01(c) and (i).

[9] 23 NCRR 500.19.

[10] 23 NCRR 500, Section 500.02.

[11] 23 NCRR 500, Section 500.17(b).

[12] 23 NCRR 500, Section 500.17(a).

[13] 23 NCRR 500, Section 500.17(a).

[14] 23 NCRR 500, Section 500.01(g) Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which

because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

[15] "Governor Cuomo Announces New Actions to Protect New Yorkers' Personal Information in Wake of Equifax Security Breach," September 18, 2017. https://www.governor.ny.gov/news/governor-cuomo-announces-new-actions-protect-new-yorkers-personal-information-wake-equifax.

[16] Stet.

[17] Stet.

[18] New York State Department of Financial Services Proposed 23 NYCRR 201, "Registration Requirements & Prohibited Practices for Credit Reporting Agencies." https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/DFS_CRA_Reg.pdf.

[19] Rules Under the Colorado Securities Act, Current through May 15, 2017, Section 51-4.8 "Broker-Dealer Cybersecurity" https://drive.google.com/file/d/0BymCt_FLs-RGQk11U2JRYlJIRUk/viewm.

[20] 23 NCRR 500, Section 500.22.

Related People

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com