NEW YORK'S FINANCIAL CYBERSECURITY REGULATION: TOUGH, FAIR, AND A NATIONAL MODEL

Jeff Kosseff*

CITE AS: 1 GEO. L. TECH. REV. 436 (2017)
https://perma.cc/8HY4-A6AC

INTRODUCTION

Soon after the New York Department of Financial Services (DFS) proposed a comprehensive cybersecurity regulation in September 2016, fear rippled throughout the financial services and technology industries.[1] The proposal imposed unprecedented obligations on banks, insurance companies, and other financial services firms under the jurisdiction of New York's Department of Financial Services. Two months later, DFS significantly revised the proposal and issued a regulation that went into effect on March 1, 2017.[2]

The following will discuss the new requirements New York's financial regulators will impose on its regulated companies, and argue that the revised regulation is a model of a rigorous, fair, and technologically sound cybersecurity regulation. New York's regulation could serve as a model for a uniform nationwide cybersecurity regulation that would provide certainty and

---

* Assistant Professor of Cybersecurity Law, United States Naval Academy; J.D. Georgetown University Law Center; M.P.P., B.A. University of Michigan; The views expressed in this Article are only those of the author and do not reflect the views of the Naval Academy, Department of Navy, or Defense Department.

[1] Joel Stashenko, *Financial Industry Groups Slam NY's Proposed Cybersecurity Rules*, LAW.COM (Nov. 30, 2016), http://www.law.com/sites/almstaff/2016/11/30/financial-industry-groups-slam-nys-proposed-cybersecurity-rules/?slreturn=20170114182937 [https://perma.cc/NL98-96NN] ("National groups including the Securities Industry and Financial Markets Association, the American Bankers Association, and the Financial Services Sector Coordinating Council have filed public comments that are critical of nearly every major aspect of the state's cybersecurity plan.").

[2] N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

clarity to companies while protecting the confidentiality, integrity, and availability of information and systems. Cybersecurity law in the United States currently is a patchwork of outdated privacy and computer crime laws;[3] New York's regulation, in contrast, is a model cybersecurity statute for the modern era.

BACKGROUND OF NEW YORK'S FINANCIAL CYBERSECURITY RULES

As every industry becomes increasingly dependent on technology, they become increasingly vulnerable to cyberattacks. Wall Street is a particularly attractive target for criminals and state actors worldwide, as the results of a successful attack could lead to mass economic disruption and a financial windfall for the hackers.[4] In 2016, the U.S. Justice Department revealed that over five years, hackers linked to the Iranian government had attacked more than four dozen U.S. financial institutions, including Bank of America Corp., the New York Stock Exchange, and JPMorgan Chase & Co.[5]

On September 13, 2016, New York Governor Andrew Cuomo announced a "first-in-the-nation regulation" designed to protect the cybersecurity of banks, insurance companies, and other financial institutions that are regulated by the New York DFS.[6] The proposed regulation would require regulated companies to establish cybersecurity programs and policies, conduct annual cybersecurity assessments, and take other specific steps to secure information and networks.[7] In a written statement, Cuomo boasted that New York "is leading the nation in taking decisive action to protect

---

[3] *See, e.g.,* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008); Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2002).

[4] *See* Portia Crowe, *The pillars of American finance are under attack*, BUS. INSIDER (Oct. 18, 2015, 2:06 PM), http://www.businessinsider.com/wall-street-cyberattacks-2015-10 [https://perma.cc/E4QJ-3JFN] ("Wall Street has a cybersecurity problem. Hackers have gone after banks, brokerages, and news wires, and now it looks as if they may have gone after business reporters as well.").

[5] Erik Larson, Patricia Hurtado, & Chris Strohm, *Iranians Hacked From Wall Street to New York Dam, U.S. Says*, BLOOMBERG (March 24, 2016, 6:12 AM), https://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt [https://perma.cc/9P8S-53V6].

[6] Press Release, New York Governor's Press Office, *Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions* (Sept. 13, 2016), https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-first-nation-cybersecurity-regulation-protect-consumers-and [https://perma.cc/7V37-SWQ3].

[7] *Id*.

consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises."[8]

Regulated financial institutions were not as enthusiastic about the proposal. In a November 14, 2016 letter to DFS, representatives from institutions such as the American Bankers Association and the National Association of Mutual Insurance Companies wrote that although they "strongly support" New York's goal of protecting financial institutions' customer information and information technology systems, the proposal was not "risk-based, flexible, [or] workable."[9] Among their concerns with the initial proposal, the required cybersecurity programs and policies did not account for the amount of risk that a company faces.[10] Moreover, they argued, certain proposed requirements, such as annual assessments of all service providers, are "practically unworkable or technically infeasible."[11] DFS responded on December 28, 2016 with a revised proposal, which went into effect on March 1, 2017.[12] The new proposed regulation incorporated many of the concerns that industry groups raised, and eased some of the other proposed requirements. For instance, the American Insurance Association praised the New York regulators for addressing "our concerns regarding some of the more restrictive and burdensome requirements of the regulation[.]"[13]

OVERVIEW OF NEW YORK'S FINANCIAL CYBERSECURITY REGULATION

New York's cybersecurity regulation is among the most detailed and thorough in the United States. This section provides an overview of the regulation's key provisions.

---

[8] *Id*.

[9] Letter from American Bankers Association et al., to Hon. Maria T. Vullo, Superintendent, New York Dep't of Financial Services (Nov. 14, 2016), http://www.aba.com/Advocacy/LetterstoCongress/Documents/Cybersecurity-11-14-16-Final-NY-JT_Trades.pdf#_ga=1.179490980.181372631.1485112938 [https://perma.cc/87FE-SF7Q].

[10] *Id.* at 1.

[11] *Id*. at 2.

[12] 23 NYCRR § 500, *supra* note 2.

[13] Press Release, Am. Ins. Ass'n., AIA Encouraged by Revised New York Department of Financial Services Cyber Regulation (Dec. 29, 2016), http://www.prweb.com/releases/2016/12/prweb13951245.htm [https://perma.cc/2ETB-KW69].

Under the regulation, regulated companies must conduct periodic assessments[14] that consider the risks particular to the companies' cybersecurity, information system, and nonpublic information, which includes: (1) business information that could cause a "material adverse impact" to the company if disclosed; (2) individual's personal information, which is a name or other identifier in combination with a social security number, drivers' license number, financial account number, financial account password, or biometric information; or (3) certain health information.[15] Companies must use these risk assessments to develop cybersecurity programs that: (1) address risks to the security and integrity of nonpublic information; (2) use "defensive infrastructure" to protect systems and nonpublic information; (3) detect cybersecurity events, which are broadly defined as act or attempts "to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System[;]"[16] (4) respond to cybersecurity events and reduce harm; (5) recovery from cybersecurity events; and (6) fulfill reporting requirements.[17]

The cybersecurity program must require monitoring and testing to regularly evaluate the program's effectiveness.[18] If an agency does not continuously monitor for vulnerabilities, they must annually conduct penetration tests to determine whether the systems are accessible to hackers.[19] Companies that do not continuously monitor also must conduct bi-annual vulnerability assessments.[20] The programs also must develop programs to ensure the ongoing security of applications that have been developed in-house.[21] Moreover, companies must securely dispose of nonpublic information once it is no longer necessary for business purposes.[22] Cybersecurity programs also must include written incident response plans, which address the processes and goals for responding to cybersecurity events, the roles and responsibilities of decision-makers, internal and external communications, remediation procedures, and reporting incidents.[23]

---

[14] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.09.
[15] tit. 23, § 500.01(g).
[16] tit. 23, § 500.01(d).
[17] tit. 23, § 500.02.
[18] tit. 23, § 500.05.
[19] *Id*.
[20] *Id*.
[21] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.08 (2017).
[22] tit. 23, § 500.13.
[23] tit. 23, § 500.16.

Companies must notify DFS within 72 hours of determining that a cybersecurity event occurred.[24]

In addition to developing cybersecurity programs, regulated companies must develop written cybersecurity policies, approved by a senior officer or the board of directors, that address the following topics, if applicable:

- Information security;
- Data governance and classification;
- Asset inventory and device management;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and third party service provider management
- Risk assessment; and
- Incident response.[25]

The regulation also requires companies to have a Chief Information Security Officer (CISO), employed directly by the company, an affiliate, or a third-party vendor.[26] The CISO is responsible for compliance with the cybersecurity regulation and must submit a written report to the Board of Directors, at least annually, that documents the company's cybersecurity program and risks.[27] Companies also must ensure that cybersecurity personnel receive updated and sufficient training,[28] and they must ensure that third-party service providers adhere to adequate cybersecurity policies and practices.[29] Companies also should maintain "audit trails" that allow them to reconstruct financial transactions after cybersecurity events and help them detect and

[24] tit. 23, § 500.17.
[25] tit. 23, § 500.03.
[26] tit. 23, § 500.04.
[27] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04 (2017).
[28] tit. 23, § 500.10.
[29] tit. 23, § 500.11.

respond to potentially harmful attacks.[30] The regulation also requires companies to use "effective controls" to prevent unauthorized access, and suggests that these controls may include multi-factor authentication or risk-based authentication, which requires additional information at log-in if the system detects anomalies.[31]

The regulation also strongly encourages companies to encrypt nonpublic information both while the information is being transmitted across networks and while it is in storage (or "at rest").[32] However, the regulation allows companies to determine whether encryption is appropriate based on their risk assessments.[33] If companies determine that encryption is infeasible, the CISO must approve alternative controls and review them at least once a year.[34]

The regulation is less onerous on small businesses, which have fewer than 10 employees (including independent contractors, less than $5 million in gross annual revenues over the previous three fiscal years, or less than $10 million in year-end total assets.)[35] Those companies are exempted from the following requirements: having a CISO, monitoring and testing their networks, maintaining audit trails, application security policies, training cybersecurity personnel, using multi-factor authentication or encryption, and maintaining an incident response plan.[36]

Regulated businesses must comply with much of the regulation by September 1, 2017, though they will receive more time to adopt some of the requirements.[37]

THE STRENGTH OF NEW YORK'S REGULATION

New York's revised regulation could serve as a national model for modern cybersecurity law, particularly due to its sensible, risk-based approach instead of an across-the-board, bright-line rule that applies regardless of the actual risk of harm. Under New York's risk-based approach, a company would be wise to focus its cybersecurity efforts on the protection of highly sensitive information, such as bank account numbers. In other words, New

[30] tit. 23, § 500.06.
[31] tit. 23, § 500.12.
[32] tit. 23, § 500.15.
[33] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.15 (2017).
[34] *Id*.
[35] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19 (2017).
[36] *Id*.
[37] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.22 (2017).

York's regulation provides an incentive for companies to more effectively allocate their cybersecurity resources.

To be sure, the risk-based framework might create uncertainty for companies, which could legitimately fear that a regulator might believe their safeguards are insufficient for the amount of risk that the company faces. However, companies likely could overcome this uncertainty by carefully documenting the reasoning behind their decision to store data in a certain manner. As DFS implements the rule, it would be useful for the Department to issue non-binding guidance that provides examples of compliance with this risk-based framework.

New York's financial cybersecurity regulation also is unique in that it refers to some of the most relevant and current safeguards, such as multi-factor authentication and vulnerability testing. About a dozen states have enacted data security statutes, but most of those laws only generally require the companies to adopt "reasonable" security procedures.[38] Even Massachusetts, which has the most rigorous general data security requirements[39] of the dozen states, is not as detailed and current in its requirements as the New York regulation.

Financial institutions also face data security regulations under the federal Gramm-Leach-Bliley Act,[40] a 1999 statute that broadly requires agencies to adopt safeguards to "insure the security and confidentiality" of customer records, to protect the security and integrity of the records, and to protect those records from unauthorized access.[41] Individual financial regulators have promulgated somewhat more specific regulations under the statute,[42] but they focus primarily on data security, and not on cybersecurity.[43]

The two are similar, but distinct, and can implicate different concerns. Data security refers to the protection of information stored by a system;

---

[38] *See, e.g.,* Cal. Civ. Code § 1798.81.5 ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").

[39] MASS. GEN. LAWS ch. 93H, § 2 (2007).

[40] 15 U.S.C. §§ 6801-6809 (2011).

[41] *Id.*

[42] *See, e.g.,* Membership of State Banking Institutions in the Federal Reserve System, 12 C.F.R. § 208, App. D-2 (2017).

[43] *Id.* ("These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.").

cybersecurity refers to the integrity of a technological system. A compromise to the system could mean that an adversary has accessed private information stored by it, or it could mean the system has been rendered unusable. If Wall Street firms were focused only on securing the *data*, then they might not devote sufficient focus to detecting and repelling a threat to the *cybersecurity* of their entire system and networks. A massive denial of service attack could hobble Wall Street by making it impossible for securities to be traded for weeks, and the result would be an economic catastrophe.

Data security is, of course, an important component of cybersecurity. But cybersecurity is more broadly focused on attacks on networks and systems, in addition to information, which the New York regulation acknowledges. That more nuanced approach is why New York's cybersecurity regulation is better suited for today's threats than the data security laws that were passed in the late 1990s and early 2000s. By defining "cybersecurity event" as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such information system,"[44] New York has focused not only on data security, but on cybersecurity as a whole.

The New York regulation also has benefits compared to the approaches of state and federal regulators, which often bring enforcement actions under general consumer protection statutes. For instance, the Federal Trade Commission (FTC) has brought dozens of data security cases under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[45] The statute defines "unfair" practices as those that cause or are likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[46] The FTC finds practices to be deceptive "if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[47] The FTC has not promulgated any formal regulations as to the types of data security that are unfair or deceptive, though it has produced some informal recommendations

[44] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(d).
[45] 15 U.S.C. § 45(a)(1) (2006).
[46] 15 U.S.C. § 45(n) (2006).
[47] FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception [https://perma.cc/8GKK-Z2UG].

based on previous enforcement actions.[48] While the New York regulation does not prescribe specific steps to satisfy the requirements, it provides more details as to the types of issues that companies must address in their cybersecurity programs and policies.

The New York regulation is forward-looking, unlike many of our current approaches to cybersecurity. For instance, immediately after a data breach, a company must focus on how to properly notify consumers under the data breach notice laws of 47 states and the District of Columbia, each of which has unique requirements for the types of information that trigger the notice and the contents of the notice.[49] While there are valid reasons for notifying customers – both to be transparent and to incentivize to invest in adequate security – our cybersecurity world has become hyper-focused on notifying consumers and regulators *after* a breach has occurred. Why not focus on rigorous and appropriate requirements that help to *prevent* breaches from occurring in the first place?

CONCLUSION

Although New York's regulation only applies to banking, insurance, and financial services companies that are regulated by DFS, the vast majority of the regulatory structure is industry-neutral and could be used in cybersecurity laws that apply to any industry. I am not suggesting that every industry regulator in every state develop its own data security framework based on the New York financial regulation. Indeed, complying with a patchwork of overlapping data security requirements would be confusing, if not impossible, for many companies, similar to the difficulty of complying with 48 data breach notification laws. Rather, the New York regulation could serve as a model for national cybersecurity legislation. For more than a decade, Congress has considered many bills that would set a standard for national data security and breach notification, preempting state laws. Those proposals have failed to gain traction. However, these proposals generally have suffered from the same shortcoming of other state and sector-specific

---

[48] FED. TRADE COMM'N, START WITH SECURITY (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/3PUK-CVZC].

[49] For a complete list of state data breach notification laws, visit: *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/B66P-9JWL].

laws – they focus narrowly on data security, and not on modern cybersecurity threats. The New York regulation, in contrast, addresses many of the most pressing cybersecurity issues that companies face every day, and does so in a way that fairly accounts for the burdens that regulations impose on small companies that have limited information technology budgets. Although a national law might ultimately look quite different from the New York regulation, this at least provides a framework as we begin to think about the contours of a strong, fair, and rigorous national cybersecurity law.