The Business, Entrepreneurship & Tax Law Review

Volume 1
Issue 2 *Fall 2017*

Article 10

2017

Password Please: The Effectiveness of New York's First-in-Nation Cybersecurity Regulation of Banks

Melissa Knerr

Follow this and additional works at: https://scholarship.law.missouri.edu/betr

 Part of the Internet Law Commons

Recommended Citation

Melissa Knerr, *Password Please: The Effectiveness of New York's First-in-Nation Cybersecurity Regulation of Banks*, 1 Bus. Entrepreneurship & Tax L. Rev. 539 (2017).
Available at: https://scholarship.law.missouri.edu/betr/vol1/iss2/10

This Comment is brought to you for free and open access by the Law Journals at University of Missouri School of Law Scholarship Repository. It has been accepted for inclusion in The Business, Entrepreneurship & Tax Law Review by an authorized editor of University of Missouri School of Law Scholarship Repository.

COMMENT

Password Please: The Effectiveness of New York's First-in-Nation Cybersecurity Regulation of Banks

*By Melissa Knerr**

ABSTRACT

In March of 2017, New York enacted new cybersecurity legislation focused on regulating banking security. Cybersecurity attacks on the financial sector have risen recently and the federal and state governments are looking to combat data breaches. The regulations themselves strive to regulate security conduct by the financial institutions, including required testing and risk assessment, training for cybersecurity personnel, and mandated reporting to upper-level staff as well as the New York Department of Financial Services. While these regulations are the first of their kind and strive to set in place certain basic requirements for cybersecurity, it remains to be seen how effective they will truly be. There is concern that the regulations are sometimes redundant, and at other times not far reaching enough to have an impact on security concerns. Still, these regulations could be used as a framework for other government institutions going forward. The effectiveness will likely not be seen until the requirements have been put in place by banks and then tested by cyberattacks.

I. INTRODUCTION

Cybersecurity is the new "hot topic of the day."[1] Cybersecurity is a popular issue, especially because it is a developing field that changes rapidly as technology evolves.[2] Discourse of cybersecurity was rampant during the 2016 presidential election campaign, with a question about cybersecurity even making it into a presidential debate.[3] In response to difficulties faced by financial institutions and the dangers to consumer privacy with cybersecurity attacks, regulators are starting to step in to impose cybersecurity regulations on banks.[4] The New York Department of Financial Services ("NYDFS") proposed a "first in the nation" cybersecurity legislation for banks that increase banking security.[5] These proposed regulations were recently adopted, and went into effect on March 1, 2017.[6]

One of the most important areas of ensuring quality cybersecurity is banking.[7] Currently, almost every bank has some sort of online platform for handling accounts and transactions.[8] Computerized banking applications ("apps") are becoming increasingly popular, allowing customers to see account balances and even deposit checks purely through the app.[9] Some banks also accept account or credit card applications through mobile apps or online sites.[10]

Increased innovation has helped banking become more accessible and easier to use.[11] Many banks have taken specific steps to gain a larger online presence.[12] For example, in 2012, Capital One purchased ING Direct, a former Dutch online banking service, to serve as its own online banking service, now called Capital One 360.[13] Unfortunately, with all the innovation required to keep up with competition, cybersecurity can sometimes be left underdeveloped.[14]

---

* Melissa Knerr is a third-year student at the University of Missouri School of Law. Melissa is originally from Philadelphia and received her bachelor's degree in History and Classic Civilizations from Duquesne University.

1. Gregory S. McNeal, *Banks Challenged by Cybersecurity Threats, State Regulators Acting*, FORBES (May 26, 2014, 6:01 PM), http://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/#62bf22e87c2c.

2. *Id.*

3. Eyragon Eidam, *Presidential Debate 2016: Cybersecurity Highlights Significant Differences in Policy, Understanding Between Candidates*, GOV'T TECH. (Sept. 27, 2016), http://www.govtech.com/security/Presidential-Debate-2016-Cybersecurity-Highlights-Significant-Differences-in-Policy-Understanding-Between-Candidates.html.

4. McNeal, *supra* note 1.

5. Judith Germano, *Proposed NY Cybersecurity Regulation: A Giant Leap Backward?*, FORBES (Dec. 2, 2016, 2:32 PM), http://www.forbes.com/sites/realspin/2016/12/02/proposed-ny-cybersecurity-regulation-a-giant-leap-backward/#68fb19642e78.

6. *New York Finalizes Cybersecurity Rules*, ABA BANKING J. (Feb. 16, 2017), http://bankingjournal.aba.com/2017/02/new-york-finalizes-cybersecurity-rules/

7. McNeal, *supra* note 1.

8. *Online Banking 101*, FORTUNE (Jan. 11, 2017), http://fortune.com/video/2017/01/11/online-banking-101/.

9. *Id.*

10. *Id.*

11. *Id.*

12. Jim Marous, *The Rise of the Digital-Only Banking Customer*, FIN. BRAND (June 6, 2017), https://thefinancialbrand.com/65628/digital-banking-consumer-trends/.

13. Lawrence C. Strauss, *Capital One Financial's Savvy Plan for Growth*, BARRON'S (Sept. 24, 2016, 1:00 AM), https://www.barrons.com/articles/capital-one-financials-savvy-plan-for-growth-1474693214.

14. Robert Hackett, *Cybercrime is Outwitting, Outpacing Security*, FORTUNE (May 28, 2014), http://fortune.com/2014/05/28/cybercrime-is-outwitting-outpacing-security/.

Cyberattacks on the financial sector rose by about 937% between 2015 and 2016.[15] A recent report found that the financial "industry is attacked 65 percent more often than any other resulting in more than 200 million records being breached in 2016. . . ."[16] This was a departure from previous cybercrime activity, as 2015 saw cyberattacks "focus[ed] on healthcare and retail [industries]."[17] Around "58 percent of the attacks were due to insiders with only five percent of those being done maliciously."[18] Meaning that a majority of cybersecurity breaches resulted from employee errors.[19]

How then can banks protect themselves from these types of attacks, which often come from places around the globe and are very hard to trace?[20] Many banks have taken significant steps to heighten their cybersecurity programs, but each innovation is challenged by the fast rate of technological change and threats that are increasingly more sophisticated.[21] Banking institutions have found that it is difficult to keep up with cybersecurity developments while also keeping pace with market pressures to have new and cutting edge technologies in their products.[22] The majority of banks, about 90%, have certain "key pillars" in place to safeguard their information security framework.[23] These key pillars include the following: "a written information security policy, security awareness education and employee training, risk management of cyber-risk, inclusive of identification of key risks and trends, information security audits, and incident monitoring and reporting."[24] Banks are relying on internal and external departments to manage their IT needs.[25] There are many tools at a bank's disposal to guard against cyberattacks: "anti-virus software, spyware and malware detection, firewalls, server-based access control lists, intrusion detection tools, intrusion prevention systems, vulnerability scanning tools, encryption for data in transit, and encrypted files."[26]

While it is commendable for a state legislature to try to address a widespread problem, it is unclear how effective these regulations will be. Ineffective regulations will not be helpful, and could make the situation worse. Regulations that include "inflexible and far-reaching state required mandates, only add to the growing clamor of distractions about how companies should best secure their systems."[27] There is concern that an inflexible and far-reaching mandate is the type of regulations the NYDFS is enacting.[28] The drafters of the regulations claim that regulated standards for cybersecurity risks are needed, as long as they do not overextend

15. Doug Olenick, *Financial Services Sector Most Attacked in 2016: IBM*, SC MEDIA (Apr. 28, 2017), https://www.scmagazine.com/financial-services-sector-most-attacked-in-2016-ibm/article/653706/.
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/#.
21. McNeal, *supra* note 1.
22. *Id.*
23. *Id.*
24. *Id.* (it should be noted that the corresponding numbers for the list of items in the original source have been removed by the author).
25. *Id.*
26. *Id.*
27. Germano, *supra* note 5.
28. *Id.*

them.[29] It is unclear, however, whether the actual regulations are appropriate and warranted.

This article will seek to first discuss the content of the regulations, paying specific attention to the requirements placed on financial institutions' cybersecurity systems, personnel, and senior officers. Next, the positive qualities of the regulations will be discussed. These positive qualities include innovation, an emphasis on testing and risk assessment, and mandating several good, basic cybersecurity principles. Finally, the negative qualities of the regulations will be critiqued as to their effectiveness at accomplishing the goal of the regulations: reducing cybercrime. These negative qualities include redundancy when compared to existing cybersecurity guidelines, the scope of the required testing and risk assessment, and the potential burdens placed on covered entities. Potential solutions, where applicable, will be offered to increase the regulations' effectiveness, as well as providing guidance for future cybersecurity regulations on how to avoid the mistakes of the New York Regulations.

II. NEW YORK'S FIRST-IN-NATION CYBERSECURITY REGULATION

The new regulations from the NYDFS goes into effect on March 1st of 2017 and banks will be given a period of 180 days to comply.[30] The introduction to the regulations describes them as being "designed to promote the protection of customer information as well as the information technology systems of regulated entities."[31] Specifically, the "regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion."[32] The regulation's goal seems to have "certain regulatory minimum standards . . . while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances."[33] The regulations place many requirements on the banks that are covered by the regulations and some of them may be redundant with cybersecurity procedures that banks already have in place, but this may differ from institution to institution.

The first requirement under the new regulation states that "[e]ach [c]overed [e]ntity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the [c]overed [e]ntity's [i]nformation [s]ystems."[34] A "covered entity" is "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [b]anking [l]aw, the [i]nsurance [l]aw or the [f]inancial [s]ervices [l]aw."[35] An "information system" is "a discrete set of electronic information resources organized for the collection, processing, maintenance . . . of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and

29. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017).
30. *Id.* §§ 500.21, 500.22(a).
31. *Id.* § 500.00.
32. *Id.*
33. *Id.*
34. *Id.* § 500.02(a).
35. *Id.* § 500.19(c).

environmental control systems."[36] Therefore, any bank subject to New York's banking law must have a cybersecurity program in place to protect its electronic databases.

The question then becomes, what is a cybersecurity program and what programming criteria is required? This program must be based on the bank's "risk assessment."[37] The risk assessment is a periodic assessment "of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part."[38] The assessment should evaluate and categorize cybersecurity risks,[39] assess confidentiality, integrity, security, and availability of the bank's information systems and confidential information,[40] and describe how risks will be mitigated, accepted, and addressed by the bank's cybersecurity program.[41]

The cybersecurity program should perform certain cybersecurity tasks such as the following: identify and assess internal and external cybersecurity risks,[42] use defensive infrastructure and implement policies and procedures to protect information systems and confidential information from cybersecurity attacks,[43] detect cybersecurity attacks,[44] respond to cybersecurity attacks to lessen negative effects,[45] recover from cybersecurity attacks and restore normal operations and services,[46] and fulfill regulatory reporting requirements.[47] Information regarding the cybersecurity program must then "be made available to the superintendent upon request."[48] Presumably, this is because the NYDFS wants access to the cybersecurity programs to ensure that they meet the above listed qualifications.

The program should also have an incident response plan. This plan should be "designed to promptly respond to, and recover from, any [c]ybersecurity [e]vent materially affecting the confidentiality, integrity or availability of the [c]overed [e]ntity's [i]nformation [s]ystems or the continuing functionality of any aspect of the [bank's] business or operations."[49] The incident response plan should address the internal process for responding to a cybersecurity attack: goals of the plan, definitions of clear roles, responsibilities and levels of decision-making authority, external and internal communication and information sharing, identification of requirements for the remediation of weaknesses in information systems, documentation and reporting regarding cybersecurity attacks, and the evaluation and revision of the incident response plan following a cybersecurity event.[50]

The cybersecurity programs must also "include monitoring and testing, developed in accordance with the [c]overed [e]ntity's [r]isk [a]ssessment, designed to assess the effectiveness of the [c]overed [e]ntity's cybersecurity program."[51] This

36. *Id.* § 500.01(e).
37. *Id.* § 500.02(b)(1).
38. *Id.* § 500.09(a).
39. *Id.* § (b)(1).
40. *Id.* § (b)(2).
41. *Id.* § (b)(3).
42. *Id.* § 500.02(b)(1).
43. *Id.* § (b)(2).
44. *Id.* § (b)(3).
45. *Id.* § (b)(4).
46. *Id.* § (b)(5).
47. *Id.* § (b)(6).
48. *Id.* § (d).
49. *Id.* § 500.16(a).
50. *Id.* § (b).
51. *Id.* § 500.05.

monitoring and testing must "include continuous monitoring or periodic [p]enetration [t]esting and vulnerability assessments."[52] Penetration testing is a form of testing "in which assessors attempt to circumvent or defeat the security features of an [i]nformation [s]ystem by attempting penetration of databases or controls from outside or inside the [c]overed [e]ntity's [i]nformation [s]ystems."[53] The cybersecurity program must include continuous or annual testing of the program's security features to ensure that they will hold up against a cybersecurity attack.[54] The testing should be "based on relevant identified risks in accordance with the [r]isk assessment . . . ."[55] If continuous testing is unavailable, banks must conduct penetrative testing along with "bi-annual vulnerability assessments, including any systematic scans or reviews of [i]nformation [s]ystems reasonably designed to identify publicly known cybersecurity vulnerabilities in the [c]overed [e]ntity's [i]nformation [s]ystems based on the [r]isk [a]ssessment."[56]

In addition to testing requirements that must be included in the cybersecurity program, the cybersecurity program also must include restrictions on other areas including mobile apps, data storage, and encryption.[57] There are requirements that include guidelines on the development of mobile banking apps within a bank's cybersecurity program.[58] The cybersecurity program must include "written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the [bank], and procedures for evaluating, assessing or testing the security of externally developed applications . . . ."[59] The cybersecurity program must include procedures relating to data retention, specifically, a policy on how to dispose of data that is no longer necessary.[60] The cybersecurity program must include encryption to protect confidential information that is "held or transmitted by the [bank] both in transit over external networks and at rest."[61] If the bank is unable to ensure encryption at rest or in transit they may use alternative methods that must be approved and reviewed annually by the Chief Information Security Officer ("CISO").[62]

Affected banks must also have a cybersecurity policy that stems from their cybersecurity program.[63] Each affected institution "shall implement and maintain a written policy . . . approved by a Senior Officer or the [c]overed [e]ntity's board of directors . . . setting forth the [c]overed [e]ntity's policies and procedures for the protection of its [i]nformation [s]ystems and [n]onpublic [i]nformation stored on those [i]nformation [s]ystems."[64]

The cybersecurity policy also needs to be based on the bank's risk assessment.[65] This written policy should address: information security, data governance and classification, asset inventory and device management, access controls and identity

52. *Id.*
53. *Id.* § 500.01(h).
54. *Id.*
55. *Id.* § 500.05(a).
56. *Id.* § (b).
57. *Id.*
58. *Id.*
59. *Id.* § 500.08(a).
60. *Id.* § 500.13.
61. *Id.* § 500.15(a).
62. *Id.* §§ (a)(1)-(2), (b).
63. *Id.* § 500.03.
64. *Id.*
65. *Id.*

management, business continuity and disaster recovery planning and resources, system operations and availability concerns, systems and network security and monitoring, systems and application development and quality assurance, physical security and environmental controls, customer data privacy, vendor and third party management, risk assessment, and incident response. [66] Essentially, the cybersecurity policy should be a written explanation of the cybersecurity program's functions.

To enforce both the cybersecurity program and the cybersecurity policy, the bank should designate a CISO.[67] The CISO has the responsibility to report to the board of directors or an equivalent governing body on the cybersecurity program and any "material cybersecurity risks."[68] In preparing the report, the CISO should consider: confidentiality of private information and the integrity and security of information systems,[69] the bank's cybersecurity policies and procedures,[70] material cybersecurity risks,[71] the effectiveness of the cybersecurity program,[72] and cyberattacks involving the bank during the report's time period.[73] The CISO is also responsible for periodically reviewing and updating, as necessary, the procedures, guidelines, and standards around the development of mobile applications.[74]

In addition to the above discussed requirements, the NYDFS requires more reporting and has more rules that banks must follow, which are covered under 23 NYCRR § 500.[75] Banks must maintain systems that "are designed to reconstruct material financial transactions sufficient to support normal operations and obligations"[76] of the bank and "include audit trails designed to detect and respond to [c]ybersecurity [e]vents that have a reasonable likelihood of materially harming any material part of the normal operations" of the bank.[77] Records of material financial transactions must be kept for at least five years.[78] Records of audit trails must be kept for at least three years.[79] Banks must also "limit user access privileges to [i]nformation [s]ystems that provide access to [n]onpublic [i]nformation and shall periodically review such access privileges."[80]

The NYDFS does not stop at security or reporting requirements, it places restrictions on the actions of company personnel as well. The regulations also provide that banks should "utilize qualified cybersecurity personnel . . . to manage the [bank's] cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in the [regulations]."[81] The personnel must also have training to address cybersecurity risks, in addition to verification by the banking employer that they are maintaining their knowledge of changing cybersecurity

66. *Id.*
67. *Id.* § 500.04(a).
68. *Id.* § (b).
69. *Id.* § (b)(1).
70. *Id.* § (2).
71. *Id.* § (3).
72. *Id.* § (4).
73. *Id.* § (5).
74. *Id.* § 500.08(b).
75. *Id.* § 500.00.
76. *Id.* § 500.06(a)(1).
77. *Id.* § (a)(2).
78. *Id.* § (b).
79. *Id.*
80. *Id.* § 500.07.
81. *Id.* § 500.10(a)(1).

risks.[82] Restrictions on personnel should also be placed directly into the bank's cybersecurity program, as discussed above.

The cybersecurity program must "implement risk-based policies, procedures and controls designed to monitor the activity of [a]uthorized users and detect unauthorized access or use of [confidential] information . . ." and "provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the [bank] in its [r]isk [a]ssessment."[83] Restrictions on personnel are also accompanied by restrictions on internal access and procedures on confidential information. The regulations require that the banks use multi-factor or risk-based authentication as part of "effective controls" to protect against unauthorized access to confidential information or the systems they are kept on.[84] Specifically, multi-factor authentication must be used "for any individual accessing the [bank's] internal networks from an external network . . ." unless the bank has approved equal or stricter controls.[85]

The regulations also include stringent notice requirements of cybersecurity events. Specifically, notice of cybersecurity attacks to the superintendent.[86] The superintendent of the Department of Financial Services supervises financial products and services.[87] The superintendent is, incidentally, the person who enforces these regulations.[88] The superintendent should be notified "as promptly as possible but in no event later than 72 hours" after a cybersecurity event has occurred.[89] The event must be reported when notice of the event is required to be sent to a supervising body, or when it has a "reasonable likelihood of materially harming any material part" of the bank's normal operations.[90] It should then be assumed that any failure to provide proper notice would result in some sort of penalty, although these regulations do not seem to outline what the penalty would be, nor how the superintendent would find out about an unreported event. In addition to the requirements for reporting cybersecurity events, banks must also submit an annual report by February 15th of each year to the superintendent that certifies that they are in compliance with the rules of the regulations.[91] The bank must keep all information related to compliance for five years and should keep a record of identified risks and cybersecurity events, along with remediation already taken, and what banks will do in the future to address risks.[92] This information must always be available to the superintendent for inspection.[93] Again, it seems that not meeting these requirements would be accompanied with some sort of punishment from the superintendent or the NYDFS itself, but such a punishment is not outlined in the current regulations.

Banks are given more time to comply with specific sections, outside of the initial 180-day period stated above. For penetration testing and vulnerability

82. *Id.* §§ (2)-(3).
83. *Id.* §§ 500.14(a)-(b).
84. *Id.* § 500.12(a).
85. *Id.* § (b).
86. *Id.* § 500.17(a).
87. *About Us*, DEP'T OF FIN. SERVS., http://www.dfs.ny.gov/about/mission.htm (last visited Dec. 19, 2017).
88. *Id.*
89. § 500.17(a).
90. *Id.* § (2).
91. *Id.* § (b).
92. *Id.*
93. *Id.*

assessments, risk assessments, and the use of multi-factor authentication to access information systems and confidential data, banks have one year from March 1st of 2017 to comply.[94] Banks will also have 18 months from March 1st 2017 to establish an audit trail, having guidelines for the development of mobile apps, data retention, implementing risk-based monitoring of authorized users' access to confidential information, and encryption of confidential information.[95] Finally, banks have two years from March 1st to comply with § 500.11, which governs policies for third-party cybersecurity service providers.[96]

III. EFFECTIVENESS OF THE REGULATIONS: PROS

The NYDFS's regulations are extensive. It is very likely that the NYDFS's regulations will be regarded as a model for what to do and not to do as more governing bodies consider adopting cybersecurity rules for financial institutions, or even other areas of business that deal with confidential data or online transactions.[97] Because the NYDFS's regulations will serve as a sort of model for future regulations, it is important to note what these regulations have done well and what needs to be improved upon. There are aspects to be praised about the regulations, including the overall innovation of the regulations themselves, the focus on regular testing of data systems and measuring risks, and a good foundation of traditional security measures that should be taken.

A. Innovation

First, these regulations should be praised because of their innovation. They are the most innovative of their kind, which in itself, deserves recognition.[98] New York is the first state to take a large step forward to address cybersecurity in the financial sector.[99] Currently, these regulations are the strictest civilian rules in the world.[100] A large state, like New York, with an even larger financial industry is a good place to begin implementing policies to address cyberattacks. These regulations could prove particularly helpful coming from a large state with ties to the financial industry and an influential circuit court because "flagging efforts [by] the federal government to provide any consistency in this area" have not accomplished much.[101] These

94. *Id.* §§ 500.22(a)-(b)(1).
95. *Id.* § (b)(2).
96. *Id.* § (3).
97. Mike Baukes, *New York's Cyber Security Regulations Aren't Perfect, But Other States Ahould Pay Attention to Them*, RECODE (Feb. 28, 2017), https://www.recode.net/2017/2/28/14766044/new-york-cyber-security-regulations-model-governr-cuomo.
98. *Id.*
99. *Id.*
100. Jon Oltsik, *New York State Cybersecurity Regulations: Who Wins?*, CSO (Feb. 23, 2017), http://www.networkworld.com/article/3173689/security/ny-state-cybersecurity-regulations-who-wins.html.
101. Eric Levy, *New York's New Cybersecurity Regulations: The Good, the Bad and the Ugly*, GARDERE (Mar. 16, 2017), http://www.gardere.com/Newsroom/Alerts/204607/New-Yorks-New-Cybersecurity-Regulations-The-Good-the-Bad-and-the-Ugly.

regulations also show a commitment to consumer protection and a policy shift on data privacy.[102]

As policy continues to be developed, these regulations can be used as a model for other regulators, both state and federal, to make the developing process of their own regulations easier. However, while being first does merit recognition, it also indicates that the regulations will be outpaced by technology that much more quickly.[103] The first compliance date has not hit yet but there are already signs that the regulations put forth by the NYDFS are "being outpaced by the reality of business in the internet age."[104] Even if these regulations are outpaced, they can still provide insight for future drafters and are an attempt to combat the rise of cyberattacks against financial institutions.

B. Regular Testing and Assessing of Risks

Second, the NYDFS's regulations place a large focus on regular testing of data systems and assessment risks. This can be seen in §§ 500.05 and 500.09, which outline penetration testing, vulnerability assessments, and risk assessment.[105] The focus on testing is important because it is crucial in understanding how data systems will react to cyberattacks. Testing will ensure that data systems are running well, and it will expose any problems or holes in the institution's systems.[106] Regular testing ensures that the system is being updated frequently enough and that it remains resilient in the face of cyberattacks.[107] Regular risk assessment helps financial institutions prevent confidential information leaks.[108]

Although the focus on testing is good, the regulations do not go far enough in their testing requirements. The regulations are more focused on administrative tasks dealing with the formation of policies, procedures, and positions rather than actual interaction with the bank's cybersecurity system.[109] The basic idea is that regular testing and risk assessment of data systems is good, but more guidance is needed to ensure quality and effectiveness of testing.

C. Foundation for Basic Cybersecurity Principles

Finally, the NYDFS's regulations establish a good basis for traditional cybersecurity practices, including: "limiting the distribution of personally identifiable information or requiring multifactor authentication . . . ."[110] Limiting distribution can be found in § 500.07 and multifactor authentication in § 500.12.[111] In addition, the

102. Michael Krimminger, *New York Cybersecurity Regulations for Financial Institutions Enter Into Effect*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Mar. 25, 2017), https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/.
103. Baukes, *supra* note 97.
104. *Id.*
105. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.05, 500.09 (2017).
106. Baukes, *supra* note 97.
107. *Id.*
108. Rob Lenihan, *Regular Risk Assessments Can Help Mitigate Cyber Exposures*, BUS. INS. (Apr. 11, 2017, 7:00 AM), http://www.businessinsurance.com/article/20170411/NEWS06/912312855/Regular-risk-assessments-can-help-mitigate-cyber-exposures.
109. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017).
110. Lenihan, *supra* note 108.
111. *Id.* §§ 500.07, 500.12.

regulations also require extensive encryption of nonpublic information, both resting with the financial institution, and while in transit via external networks.[112] All of these requirements are specifically technical in nature and are generally important to include in any cybersecurity system to ensure data protection. The NYDFS's inclusion of these requirements is a positive step forward in ensuring all banks are practicing basic cybersecurity techniques.

The regulations also call for ongoing and comprehensive training for cybersecurity personnel within the institution.[113] Ongoing training is a must for in-house cybersecurity departments because technology dealing with cybersecurity is quick to change and rapidly develops unfamiliar problems.[114] Innovative methods are needed to address those problems.[115] In addition, it is speculated that employees are much more likely to cause daily data compromises through negligence or wrongdoing than would an outside breach.[116] These cybersecurity basics are a step forward in the direction of universal cybersecurity procedures. However, it must be noted that these are just basics. It is highly likely that many of the financial institutions covered under the NYDFS regulations already practice the methods required under the regulations, or the third-party company they outsource their cybersecurity to does.[117]

In addition to other positive qualities listed above, the regulations also have the potential to serve as boilerplate requirements for future entities looking to mandate cybersecurity, whether those entities are other states, or the federal government looking to establish universal rules for cybersecurity. On the other hand, there are numerous problems with the regulations that should be addressed either by changing the regulations themselves, or adopting different policies when another governing body creates its own cybersecurity regulations.

IV. EFFECTIVENESS OF THE REGULATIONS: CONS

This section addresses problems with the regulations and suggests potential ways to improve future cybersecurity regulation. Unfortunately, there are aspects of the regulations that are subject to criticism, specifically because they are not effective. These areas are: the redundancy of 23 NYCRR § 500 requirements when compared to already existing guidelines, the scope of the testing requirements, and the potential burden these regulations place on covered financial institutions.[118] The ineffectiveness seems to come from a lack of overall consistency throughout the regulations. Some sections of the regulations feature an overabundance of regulation and not enough in others. Improving upon these regulations is critical for consumers and financial institutions going forward.[119]

---

112. *Id.* § 500.15.
113. *Id.* § 500.10.
114. Stephen Baer, *Why You Should Gamify Your Cybersecurity Training*, FORBES (Oct. 4, 2017, 8:00 AM), https://www.forbes.com/sites/forbesagencycouncil/2017/10/04/why-you-should-gamify-your-cybersecurity-training/#45ff0a7c6271.
115. *Id.*
116. Lenihan, *supra* note 108.
117. Baukes, *supra* note 97.
118. *Id.*
119. *Id.*

A. Redundancy

First, the biggest problem with the regulations is that they are extremely redundant. Not redundant within the regulations itself, but redundant with current existing guidelines for financial institutions on cybersecurity procedures.[120] Specifically, 23 NYCRR § 500 is strikingly similar to cybersecurity regulations and guidance posed by the National Institute of Standards and Technology ("NIST"), and the Federal Financial Institutions Examination Council ("FFIEC").[121]

The NIST published its Cybersecurity Framework in 2014 and drafted a proposed update for the framework in January of 2017.[122] This framework is voluntary and is meant to help "organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid" but has also been used frequently by other types of institutions around the world to help manage cybersecurity risks.[123] The NIST's Cybersecurity Framework provided standards for the communication of cybersecurity risks throughout the organizational levels of the institution,[124] managing cybersecurity risks,[125] and the delivery of critical cybersecurity services.[126] While the cybersecurity framework is voluntary, it includes much of the same material that the mandatory New York regulations cover.[127] Organizational communication is covered extensively by the New York regulations in §§ 500.03 and 500.04, which deal with the creation of the cybersecurity policy and its approval by the board of directors, and the appointment of a CISO.[128] Managing cybersecurity risks and the running of cybersecurity services are both regulated under 23 NYCRR § 500.[129] These regulations share much in common with the Cybersecurity Framework published by the NIST.

In June of 2015, the FFIEC released its Cybersecurity Assessment Tool, a cybersecurity examination work program that allows financial institutions to understand their inherent cybersecurity threats and vulnerabilities when crafting a cybersecurity program.[130] This assessment provided an individualized approach to cybersecurity, construing the assessment around the amount of cybersecurity risk each financial institution faced based on their connections and activities.[131] It assessed inherent risk based upon "the type, volume, and complexity of operational considerations, such as connection types, products and services offer, and technologies

120. Oltsik, *supra* note 100.
121. *Id.*
122. Evelyn A. Brown, *NIST Releases Update to Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH. (Jan. 10, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.
123. *Id.*
124. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. 2 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
125. *Id.* at 3.
126. *Id.* at 5.
127. *Id.* at 2.
128. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.03, 500.04 (2017).
129. *Id.* §§ 500.09, 500.10.
130. *FFIEC Cybersecurity Assessment General Observations*, FED. FIN. INSTS. EXAMINATION COUNCIL 1, https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf (last visited Dec. 19, 2017).
131. *Id.*

used."[132] It also reviewed current practices and made recommendations for improving risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience.[133]

Again, the New York regulations share many similarities with the cybersecurity suggestions in the FFIEC Cybersecurity Assessment Tool. New York's cybersecurity regulations extensively cover risk management,[134] oversight,[135] cybersecurity controls,[136] dependence on external management,[137] and managing cyber incidents.[138] While the Cybersecurity Assessment Tool is not mandatory[139], it does provide far more than the NYDFS in individualized guidelines for financial institutions looking to evaluate their cybersecurity.

The NIST's Cybersecurity Framework and the FFIEC's Cybersecurity Assessment Tool are two of the most well-known guidelines for cybersecurity for businesses, and specifically for financial institutions.[140] While institutions are not required to follow or use either of the guidelines, they do provide direction for companies looking to update their cybersecurity without the pressure of government mandated action on cybersecurity.[141] There are even some areas where the two guidelines work better than the mandated regulations at dealing with cybersecurity issues that many financial institutions face.[142]

The guidelines discussed above are just two examples of many state departments that have programs or guidelines extremely similar to the New York regulations.[143] The regulations are also redundant when compared to guidelines published by the Office of the Comptroller of the Currency and regulations contained in the Gramm-Leach-Bliley Act, which modernized how banks handle private individuals' information.[144] Because there is a great deal of guidance already present for cybersecurity programs used by financial institutions, it is not clear whether the New York regulations were really needed. They just serve to make aspects of the guidelines mandatory, but do so in a less individualized way.

B. Scope

Second, the requirements in 23 NYCRR § 500 include some of the more basic foundations of cybersecurity policy, including frequent testing of security systems.[145] Such frequent testing is an important requirement to include, since frequent testing is often how weaknesses are identified in cybersecurity systems.[146] Unfortunately, the testing required by the regulations is not required often enough, or

132. *Id.*
133. *Id.* at 2.
134. § 500.09.
135. *Id.* § 500.04.
136. *Id.* § 500.02.
137. *Id.* § 500.11.
138. *Id.* § 500.16.
139. Oltsik, *supra* note 100.
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. Baukes, *supra* note 97.
146. *Id.*

applied to enough aspects of a cybersecurity system to really be of use in helping the financial institution identify weak areas, or protect consumer information.[147] The testing should be required much more frequently and the systems subject to the testing should be expanded.

The regulations only require testing once per year and vulnerability assessments twice per year.[148] Testing done once a year is not nearly often enough to ensure that the financial institution's systems are effective in reacting to threats, as new ones develop.[149] Once a year testing is "akin to checking the weather forecast once a year and hoping it holds . . . for the [rest of the year]."[150] Annual testing, or even bi-annual testing does not provide frequent enough updates to account for how quickly digital threats and information systems can change.[151] While annual, bi-annual, and quarterly timelines can work in other areas of business management, these timelines are much too broad to work for the management of technological aspects of a business.

In addition, only requiring testing once a year "implies that systems should and will remain static for the given certification period."[152] Anything remaining static for a year in a business is likely not good, especially a cybersecurity system.[153] Technology, especially cybersecurity systems and threats against them, have a much more rapid pace of development than other areas that financial institutions review, and therefore, should require more frequent review.[154] For example, requiring monthly testing would do much more to ensure that cybersecurity information systems are staying effective against developing technology. Thus, drastically expanding the frequency of required testing would increase the effectiveness of the regulations.

Currently, the regulations only require annual penetrative testing and bi-annual vulnerability assessments of the financial institution's information systems.[155] Testing of an information system is not enough to ensure that a cybersecurity system is secure against attacks.[156] There are numerous other systems that should be tested in addition to the information systems, since these systems are all interconnected in protecting against breaches.[157] These others systems are data, access, and operational systems.[158] Misconfigurations in systems and even between systems working together will cause 99% of firewall breaches by 2020, rather than pure security or firewall flaws.[159] Regular testing of all systems helps craft efficient cybersecurity policy and "creates trust in the systems themselves."[160] Frequent testing of all systems provides visibility and notification of misconfigurations that could otherwise remain unnoticed until a cybersecurity attack exploits them.[161] While testing of

147. *Id.*
148. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.05(a)-(b) (2017).
149. Baukes, *supra* note 97.
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2017).
156. Baukes, *supra* note 97.
157. *Id.*
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*

information systems is a good start, in order to be more effective at combating cybersecurity issues, testing should be expanded to include all systems used in a bank's cybersecurity framework.

While the regulations take important steps in including testing of information systems, they do not go far enough in scope. To be an effective mandate on cybersecurity policy, the regulations need to increase the frequency of testing from the current one year requirement and increase the amount of systems subject to frequent penetrative testing. Taking these steps will ensure that the regulation requirements are doing all they can to effectively combat cybersecurity threats against financial institutions.

C. Burden on Covered Entities

There are multiple requirements set by the regulations that could prove difficult for the covered financial institutions to comply with, both on a practical and policy level. There are new education requirements on financial institution's cybersecurity personnel that could prove difficult to accomplish due to a shortage of qualified applicants and difficulties in keeping up with training.[162] Also, the new focus on upper management accountability and certification could provide new liability issues in the case of a breach involving customer data.[163] Theses aspects could place a substantial burden on any of the covered entities attempting to comply with the New York Regulations.

The New York Regulations require that covered financial institutions have qualified cybersecurity personnel, provide these personnel with training and updates to address changing cybersecurity risks, and verify that they maintain knowledge of changing threats and countermeasures to cybersecurity systems.[164] Research from the Enterprise Strategy Group ("ESG")[165] showed that 45% of surveyed internet technology and cybersecurity professionals reported a shortage of cybersecurity skills in their organization in 2017.[166] In addition, ESG research from 2016 reported that 42% of surveyed organizations said that it was either difficult, or very difficult for them "to recruit and hire cybersecurity professionals in the first place."[167] These responses are likely because of an increasingly competitive market for cybersecurity talent among banks.[168]

Providing updated training and verifying that cybersecurity employees maintain their knowledge will be at the very least costly, if not outright prohibitive for banks to accomplish.[169] In a series of reports by ESG and the Systems Security

---

162. Jon Oltsik, *New York State Cybersecurity Rules and the Skills Shortage*, CSO (Feb. 21, 2017, 7:55 AM), http://www.networkworld.com/article/3172363/security/new-york-state-cybersecurity-rules-and-the-skills-shortage.html.

163. Tamara Bruno, *New Cybersecurity Regulations from the NY DFS: What Every Insured Should Know*, PILLSBURY: POLICYHOLDER PULSE (Mar. 7, 2017), http://www.policyholderpulse.com/2017/03/07/new-cybersecurity-regulations-ny-dfs-every-insured-know/.

164. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.10 (2017).

165. The Enterprise Strategy Group is a research and strategy firm that provides market intelligence and insight into the global Internet Technology community. *See About*, ESG-GLOBAL, http://www.esg-global.com/ (last visited Dec. 19, 2017).

166. Oltsik, *supra* note 162.

167. *Id.*

168. *Id.*

169. *Id.*

Association, results showed that 56% of surveyed cybersecurity professionals responded that their employer did not "provide them with the right level of ongoing training to keep up with current risks and threats."[170] In addition, the reports showed that there are many cybersecurity workers who feel that they are too busy, or too overworked to dedicate time to training and keeping up with technological advancements on their own.[171] Importantly, financial institutions can discharge these requirements by employing a third party service provider for their cybersecurity needs, which does not discharge their responsibility to ensure that the service provider is following the regulations requirements.[172] While the training and knowledge requirements themselves are a practical requirement, implementation of them among the covered financial institutions could prove difficult because of a shortage of qualified employees, a difficulty in ensuring proper training, and the lack of time employees have for training.

The New York Regulations place an emphasis on management involvement and responsibility in applying cybersecurity policy.[173] This emphasis is present as early as the introduction to the regulations, which states: "[s]enior [m]anagement must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations."[174] There are five sections that refer to approval from upper level management like a board member or the CISO, a position required by the regulations.[175] Certification of compliance by the board, CISO, or another senior officer, could potentially open the entire financial institution and the certifying individuals to liability from customer litigation, or regulatory repercussions in a situation where the financial institution did not comply or where a cybersecurity event occurred involving customer data.[176] The regulations state that they will be enforced "under any applicable laws."[177] The enforcement could include a variety of New York laws, including banking and insurance, that contain both "civil and criminal penalties for intentionally making false statements to DFS."[178]

While the New York Regulations attempt to take steps forward to protect consumer information and financial data systems, these steps come at the cost of a much higher burden to the covered financial institutions.[179] Employee hiring and training requirements will most likely strain companies already struggling to hire and effectively train cybersecurity professionals. The increased focus on managerial involvement could also leave the company, and senior officers, especially the CISO, open to individual liability for compliance problems or cybersecurity attacks.[180] These factors, combined with the pressure they are already under to quickly comply with

170. *Id.*
171. *Id.*
172. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2017).
173. *Id.* § 500.00.
174. *Id.*
175. *Id.* §§ 500.03, 500.04, 500.08, 500.12, 500.15.
176. Bruno, *supra* note 163.
177. § 500.20.
178. Mark Andruskiewicz, Clarke Cummings, & Michael Horn, *Cyber: New York Regulator Moves the Goalposts*, PRICEWATERHOUSECOOPERS: FIN. CRIMES OBSERVER 3 (Sept. 2016), http://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/NY-DFS-proposes-cybersecurity-regulations.
179. Oltsik, *supra* note 162.
180. Bruno, *supra* note 163.

the regulations, will likely place a large burden on the covered financial institutions from a monetary and personnel standpoint.

V. CONCLUSION

The New York regulations are clearly a complex piece of legislation. Cybersecurity concerns affect numerous parts of a financial institution, and so does this legislation. The newly enacted regulations come after a long comment period and extensive revision.[181] The first draft of the legislation had over 150 comments filed on it, which was proposed in September of 2016.[182] Even with the large amount of input, it is unclear if these regulations succeed in their stated purpose, or in combating cybersecurity events at all.

There are aspects of the regulations that should be praised and referred to when future regulations are drafted: innovation, focus on testing of data systems and risk assessment, and a foundation of good cybersecurity practices. However, the regulations are not perfect and it remains to be seen whether they will have as large of an effect as the NYDFS expects them to. The regulations are often redundant with existing cybersecurity guidelines, the testing requirements are not broad enough to really make a difference with evolving cybersecurity threats, and place personnel and monetary burdens on covered banks through hiring and training requirements along with opening both the bank and senior officers to personal liability.

Compliance with the New York Regulations comes with numerous pros and cons and because they are mandatory for any bank doing business in New York, it is likely that many banks will be covered under the regulations. It will be interesting to see how the banks go about compliance, perhaps there will be an increase in third party cybersecurity services. It is yet to be determined as to what kind of an impact these regulations will have on cybersecurity threats, which have only been increasing in complexity and frequency. While these regulations are the first of their kind, and only affect one state, they could easily serve as a framework and springboard for other states and regulatory bodies to craft their own cybersecurity requirements, likely increasing the burden on banks across the nation. These newly enacted regulation's effects will only be known when the results of compliance or non-compliance is seen.

181. Gretchen A. Ramos & Larry P. Schiffer, *New York Revamps Proposed Cybersecurity Regulation for Financial Services and Insurance Entities*, NAT'L L. REV. (Jan. 3, 2017), http://www.natlawreview.com/article/new-york-revamps-proposed-cybersecurity-regulation-financial-services-and-insurance.

182. *Id.*