Emory Corporate Governance and Accountability Review

Volume 4
Issue 2 *Law & Innovation Issue*

2017

Cybersecurity Is Not a Product, It's a Process: Financial Service Regulators Hold Insurance Company Boards Responsible for Cybersecurity

Alice T. Kane

Phillip A. Goldstein

CYBERSECURITY IS NOT A PRODUCT, IT'S A PROCESS: FINANCIAL SERVICE REGULATORS HOLD INSURANCE COMPANY BOARDS RESPONSIBLE FOR CYBERSECURITY

Alice T. Kane
Phillip A. Goldstein[*]

INTRODUCTION

Over the last few years, the insurance industry has been recognized as a significant target of cybersecurity threats.[1] In 2015, the data breach at Anthem, Inc., resulted in the information of millions of individuals being compromised.[2] On the same day, hackers are estimated to have stolen up to 11 million customer records at Premera Blue Cross.[3] Hackers have realized that data held by insurance companies can, in fact, be more valuable over time than credit card information.[4] For example, insurance companies store data on where the insureds live, spouses' names and serious medical conditions.[5] In the age of technological turbo-change, cybersecurity risk will not be going away

---

[*] Alice T. Kane practices in the area of insurance law and has extensive experience in both the legal and business aspects of the insurance industry. Ms. Kane counsels insurers and other participants in the insurance sector on a wide range of regulatory and transactional matters. Ms. Kane advises property and casualty, life and health insurance clients. Ms. Kane has served as the Group General Counsel at two Fortune 100 Insurance Companies. Ms. Kane is a graduate of New York University School of Law, Manhattanville College, and attended the Harvard Business School Executive Program.

Philip A. Goldstein practices in the area of corporate, including mergers & acquisitions and public offerings. Mr. Goldstein has particular knowledge and experience in government contracting, insurance regulatory, and various commercial law issues. Philip Goldstein is a graduate of Cornell Law School and Cornell University.

[1] Alice T. Kane & Phillip A. Goldstein, *New Cybersecurity Regulations for NY Insurers and Banks*, LAW 360 (Oct. 13, 2016, 12:15 PM), https://www.law360.com/articles/851076/new-cybersecurity-regulations-for-ny-insurers-and-banks.

[2] Charles Riley, *Insurance giant Anthem hit by massive data breach*, CNN MONEY (Feb. 6, 2015, 10:52 AM), http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/.

[3] Kate Vinton, *Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical and Financial Data*, FORBES (Mar. 17, 2015, 6:54 PM), http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#53a351d02143.

[4] Alice T. Kane & Phillip A. Goldstein, *New Cybersecurity Regulations for New York Insurers and Bank*, DUANE MORRIS LLP (Oct. 13, 2016, 12:15 PM), http://www.duanemorris.com/articles/static/Kane_Goldstein_Law360_1016.pdf.

[5] *Id.*

anytime soon - it will only become more complicated and potentially more dangerous.[6]

This ever-present danger of cybersecurity risks is generating state and federal regulators to propose corporate governance cybersecurity requirements for insurance company Boards of Directors (the "Board" or "Boards") and management. Financial service regulators are taking action to safeguard the insurance industry from cybersecurity threats by requiring programs and policies to be approved and monitored by Boards and implemented by management. Our focus is on the proposed insurance regulations that approach cybersecurity risk with a regulatory stick by mandating the implementation of cybersecurity policies and programs with rigorous Board oversight, and, in one instance, Board certification of compliance. If management and directors of financial institutions that experience future cyber incidents are subsequently found to be noncompliant with such a regulation, then Boards will be further exposed to litigation. Such litigation would likely be covered under D&O policies and, therefore, most likely would result in increased D&O premiums.[7]

In late 2016, there was a frenzy of regulatory activity on the federal and state level. the New York Department of Financial Services ("NYDFS"), a consortium of federal regulators and the National Association of Insurance Commissioners ("NAIC")—which tends to influence the legislative and regulatory insurance laws of many states—each considered regulations to curb cybersecurity risks.[8] All three have corporate governance requirements. The first ever cybersecurity regulation was released by the NYDFS on September 13, 2016.[9] Following a barrage of industry comments, Superintendent Maria Vullo issued an updated cybersecurity regulation.[10][11] Nationally, insurance

---

[6] Andrea Bonime-Blanc, *A Strategic Cyber-Roadmap for the Board*, HARVARD LAW FORUM ON CORP. GOVERNANCE AND FIN. REGULATION (Jan. 12, 2017), https://corpgov.law.harvard.edu/2017/01/12/a-strategic-cyber-roadmap-for-the-board/.

[7] *Fitch: NY Cyber Rules Could Raise Loss Exposures for US Insurers*, ADVISEN (Feb. 13, 2017), http://www.advisen.com/tools/fpnproc/fpns/articles_new_1/P/275590472.html?rid=275590472&list_id=1.

[8] *See About the NAIC*, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, http://www.naic.org/index_about.htm (last visited Mar. 2, 2017).

[9] Press Release, N.Y. State Dep't of Fin. Servs., Governor Cuomo Announces Proposal of First-In-The-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions (Sept. 13, 2016), http://www.dfs.ny.gov/about/press/pr1609131.htm).

[10] Press Release, N.Y. State Dep't of Fin. Servs., DFS Issues updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016), http://www.dfs.ny.gov/about/press/pr1612281.htm).

[11] Governor Cuomo Announces Proposal of First-In-The-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions, *supra* note 9.

regulators at the NAIC have been busy working toward developing an Insurance Data Security Model Law (the "Model Act") to establish insurance industry standards for data security.[12] In response to industry comments, the Model Act is now on its third draft and is expected to be finalized later this year.[13] Finally, at the federal level, a joint advance notice of proposed rulemaking ("ANPR") for enhanced cyber risk management standards for large and interconnected and federally regulated financial institutions was jointly released, in October, by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (the "Federal Regulators").[14]

Surveys completed by Spencer Stuart/Corporate Board Member and PWC's Governance Insights Center show that public company Boards view cybersecurity risk as a serious problem that needs more attention.[15] With that said, the aforementioned regulatory proposals mandate corporate governance requirements for insurance company Boards. Boards of insurance companies now not only have a fiduciary responsibility and duty of care to the company, policyholders and shareholders, but also have to comply with regulatory mandates.

Part 1 of this Article will address the corporate governance mandates of the updated, proposed cybersecurity regulation issued by the NYDFS and how the mandates have changed from the initial, proposed regulation. Part 2 will focus on the NAIC Model Act's corporate governance requirements. Lastly, Part 3 will discuss how corporate governance is approached by the ANPR issued by the Federal Regulators.

I. NYDFS REGULATION

After surveying nearly 200 of its regulated insurance companies and banks for industry insight, the NYDFS proposed the first-ever cybersecurity

---

12 Gloria Gonzalez, *NAIC cyber security model law to be released in 2017*, BUSINESS INSURANCE (Dec. 12, 2016, 10:11 AM), http://www.businessinsurance.com/article/00010101/NEWS06/912310924/NAIC-cyber-security-model-law-to-be-released-in-2017.

13 *Id.*

14 Enhanced Risk Management Standards, 81 Fed. Reg. 74315 (Oct. 26, 2016).

15 Bonime-Blanc, *supra* note 6; Melanie Nolen & Kimberly Crowe, *What Directors A Corporate Board Member/Spencer Stuart Survey*, N.Y. STOCK EXCH. (2016), https://www.nyse.com/publicdocs/What_Directors_Think_2016.pdf.

regulation to protect against the growing threat of cyber-attacks.[16] Following a 45-day comment period,[17] where over 150 comments were submitted,[18] NYDFS issued an updated draft on December 28, 2016.[19] NYDFS made it clear that the revised regulation was a result of careful consideration of the submitted comments.[20]

A. Initial Regulation

Both the initial and the most recent drafts of the cybersecurity regulation create corporate governance obligations for insurance company Boards. Insurance companies are required to establish a cybersecurity program and policies to ensure the confidentiality, integrity and availability of their information systems and nonpublic information.[21] A Chief Information Security Officer ("CISO") must also be designated to be responsible for implementing, overseeing and enforcing the program and policies.[22] The cybersecurity policy must address specific areas, such as system and information security, customer data privacy, and vendor and third-party service provider management.[23] Initially, the draft regulation required at least an annual Board review of the cybersecurity policy and biannual CISO reports to the Board.[24] A certification of compliance from the Board or senior officer to NYDFS is required to affirm that the insurance company is in compliance with the cybersecurity regulation.[25]

---

[16] *First-Ever: Cybersecurity Regulations Released by New York Department of Financial Services*, DUANE MORRIS LLP, (Sept. 16, 2016), http://www.duanemorris.com/alerts/first-ever_cybersecurity_regulations_released_by_new_york_department_financial_services_0916.html.

[17] DFS Issues updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions, *supra* note 10.

[18] Consumer Fin. Servs. & Privacy & Data Security Grps., *NYDFS Revises Cybersecurity Regulation, Extends Effective Date to March 1,* 2017, BALLARD SPHAR LLP, (Dec. 28, 2016), http://www.ballardspahr.com/alertspublications/legalalerts/2016-12-28-nydfs-revises-cybersecurity-regulation-extends-effective-date.aspx.

[19] *NYDFS Revises Cybersecurity Regulations, Extends Effective Date to March 1, 2017*, *supra* note 18.

[20] Press Release, N.Y. State Dep't of Fin. Servs., Governor Cuomo Announces First-In-The-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1, (Feb. 16, 2017), http://www.dfs.ny.gov/about/press/pr1702161.htm.

[21] N.Y. COMP. CODES R & REGS. tit. 23, § 500.02(a) (2017).

[22] N.Y. COMP. CODES R & REGS. tit. 23, § 500.04(a) (2017).

[23] N.Y. COMP. CODES R & REGS. tit. 23, § 500.03(a) (2017).

[24] N.Y. COMP. CODES R & REGS. tit. 23, § 500.04(b) (2017).

[25] N.Y. COMP. CODES R & REGS. tit. 23, § 500.21 (2017).

B. Revised Regulation

On December 28, 2016, NYDFS released an extensively revised cybersecurity regulation.[26] Most notably, the annual review requirement by the Board of the cybersecurity policy has been eliminated.[27] Under the revised regulation, either a senior officer *or* the Board are required to approve the written cybersecurity program and polices.[28] This option of either senior officers or the Board permits the Board to rely solely on management for the cybersecurity program's approval.

Initially, the regulation required a biannual report by the CISO to the Board assessing the information systems, exceptions to the cybersecurity policies and procedures, identifying the cyber risks and assessing the effectiveness of the cybersecurity program, along with proposing steps to remedy any inadequacies and a summary of all cybersecurity events.[29] The revised regulation requires an annual report by the CISO on material cyber risks, overall effectiveness of the program and eliminates any remediation steps for program inadequacies.[30] A summary of cybersecurity events and external reporting of cyber breaches is raised from all events to material events.[31]

II. NAIC MODEL ACT

In the U.S., insurance regulation is largely a state based system where each state has its own insurance law and regulator.[32] The NAIC is the regulatory support and standard-setting organization operated by the insurance regulators from all 50 states and the U.S. territories.[33] Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and

---

[26] Governor Cuomo Announces First-In-The-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1, *supra* note 20; Thomas M. Dawson & Yuliya Feldman, *NYDFS Proposes Revised Cybersecurity Requirements for Financial Services Companies*, DRINKERBIDDLE.COM (Dec. 29, 2016), http://www.drinkerbiddle.com/insights/publications/2016/12/nydfs-proposes-revised-cybersecurity-requirements.

[27] *See Cybersecurity Requirements for Financial Services Companies*, N.Y. STATE DEP'T OF FIN. SERV., http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

[28] N.Y. COMP. CODES R & REGS. tit. 23, § 500.03 (2017).

[29] Theodore Augustinos, *New York DFS Promulgates Cybersecurity Requirements for Financial Services*, JDSUPRA BUSINESS ADVISOR (Oct. 3, 2016), http://www.jdsupra.com/legalnews/new-york-dfs-promulgates-cybersecurity-13218/.

[30] N.Y. COMP. CODES R & REGS. tit. 23, § 500.04(b) (2017).

[31] N.Y. COMP. CODES R & REGS. tit. 23, § 500.04(b)(3) (2017).

[32] The McCarran–Ferguson Act, 15 U.S.C. §§ 1011–1012 (2012).

[33] *About the NAIC*, *supra* note 8.

coordinate their regulatory oversight.[34] In late 2014, the NAIC Executive (EX) Committee appointed the Cybersecurity (EX) Task Force to function as the hub for cybersecurity regulatory activity.[35]

In 2015, the NAIC adopted the 12 Principles for Effective Cybersecurity Insurance Regulatory Guidance[36] and, in March 2016, began working on drafting the Model Act to establish cybersecurity standards for insurance companies which cover data security and investigation and notification of breaches.[37] More recently, the proposed Model Act was discussed at both the 2016 NAIC summer and fall meetings.[38] The initial drafts of the Model Act have been revised after receiving extensive comments from trade associations, market participants and regulators.[39] An ad hoc drafting group was formed to move the Model Act toward finalization. The ad hoc group is currently chaired by Elizabeth Kelleher Dwyer, the Rhode Island Insurance Superintendent.[40] Work on a third draft of the Model Law is continuing into 2017 with biweekly regulator, conference calls.[41]

The Model Act requires much more of insurance company Boards. It establishes clear Board responsibility for cybersecurity by requiring Board approval and oversight of the required comprehensive written information security program including implementation and ongoing management

---

[34] *Id.*

[35] *Cybersecurity*, NAT'L ASS'N OF INS. COMM'RS (last updated Nov. 17, 2016), http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

[36] *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, NAT'L ASS'N OF INS. COMM'RS (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf; *Cybersecurity*, *supra* note 35.

[37] Gloria Gonzalez, *NAIC Cyber Security Model Law to Be Released in 2017*, BUSINESS INSURANCE (Dec. 12, 2016, 10:11 AM), http://www.businessinsurance.com/article/00010101/NEWS06/912310924/NAIC-cyber-security-model-law-to-be-released-in-2017.

[38] Kane & Goldstein, *supra* note 1.

[39] *Id.*

[40] *Legal Alert: NAIC Report: 2016 FALL National Meeting*, EVERSHEDS SUTHERLAND (Dec. 29, 2016), https://us.eversheds-sutherland.com/portalresource/lookup/poid/Z1tOl9NPluKPtDNIqLMRV56Pab6TfzcRXncKbDtRr9tObDdEoKZDm83!/fileUpload.name=/LegalAlert_NAIC-Report_2016-Fall-National-Meeting.pdf.

[41] Jean Adams-Harris, *NAIC 2016 Fall National Meeting Highlights*, JOHNSON LAMBERT (Jan. 31, 2017), https://www.johnsonlambert.com/news-blog/2017/01/31/naic-2016-fall-national-meeting-highlights#.WLDaHOTfOUk; Russell Sommers, *NAIC Cybersecurity Update: Jan. 24 2017*, BAKERTILLY.COM (Jan. 27, 2017), http://www.bakertilly.com/insights/naic-cybersecurity-update-jan-24-2017/; Leah Campbell, Michael Groll, Donald Henderson & Jr. Allison Tam, *NAIC Report: 2016 Fall National* Meeting, WILKIE.COM (Dec. 27, 2016), http://www.willkie.com/~/media/Files/Publications/2016/12/NAIC_Report_2016_Fall_National_Meeting.pdf.

reports.[42] The written program must contain details of the administrative, technical and physical safeguards for protecting personal information.[43] There is also an annual certification of compliance to the Board by management on the overall status of the cybersecurity program, material matters related to the program and the company's compliance with the Model Act.[44]

In the current NAIC drafting meetings, the points of contention that are being debated regarding the language of the Model Act do not include the aforementioned corporate governance requirements.[45] Work on a third draft of the Model Law continues and only time will tell whether the governance requirements will remain in the finalized model legislation.[46]

III. ANPR ISSUED BY THE FEDERAL REGULATORS

Federal Regulators announced a joint ANPR for enhanced cyber-risk management standards for large, interconnected and federally regulated financial institutions in October 2016.[47] The ANPR described plans for implementing cyber-risk management standards at a conceptual level, and presented 39 questions for comment[48], due February 17, 2017.[49] The ANPR, like the NYDFS regulation and the NAIC Model Act, focuses on corporate governance and the role of the Board in establishing a cybersecurity program, enterprise risk management and continued oversight. If issued, the regulation would apply to depository banks that are governed by the Federal Regulators and insurance companies designated as Non-Bank SIFIs by the Federal

---

[42] NAT'L ASS'N OF INS. COMM'RS CYBERSECURITY TASK FORCE, *A New Model: Insurance Data Security Model Law* (Aug. 17, 2016), http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_mod_draft_clean.pdf.

[43] *Id.*

[44] *Id.*

[45] Campbell et al., *supra* note 41.

[46] Adams-Harris, *supra* note 41; Sommers, *supra* note 41; Campbell et al., *supra* note 41.

[47] Press Release, Bd. of Governors of the Fed. Reserve Sys., Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (Oct. 19, 2016), https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm.

[48] *Legal Alert: Enhanced Cyber Risk Management Standards Announced in Joint Rulemaking Initiative by Treasury, Federal Reserve, and FDIC*, EVERSHEDS SUTHERLAND (Dec. 28, 2016), https://us.eversheds-sutherland.com/NewsCommentary/Legal-Alerts/195109/Legal-Alert-Enhanced-Cyber-Risk-Management-Standards-Announced-in-Joint-Rulemaking-Initiative-by-Treasury-Federal-Reserve-and-FDIC.

[49] Richard Hsu, *Cyber$ecurity: Recent Developments in the Protection of Financial Data*, SHEARMAN & STERLING LLP (Jan. 26, 2017), http://www.shearman.com/en/newsinsights/publications/2017/01cybersecurity-protection-of-financial-data.

Stability Oversight Council or insurance subsidiaries of covered depository banks or bank holding companies.[50]

The ANPR is organized into 5 categories, with cyber risk governance and cyber risk management being the first two that are addressed and clearly intend the Boards to play a major role.[51] For example, the risk governance category provides that the Board, or an appropriate Board committee approves the entity's cyber risk management strategy and holds senior management accountable for establishing and implementing appropriate policies consistent with the strategy.[52] To satisfy this requirement the Board must have adequate expertise in cybersecurity or have access to resources or staff with such expertise.[53] Only with such expertise is the Board able to provide credible challenges to management in matters related to cybersecurity and the evaluation of cyber risks and resilience.[54] The cyber risk governance category goes on to require the entity's Board to review and approve the enterprise-wide cyber risk appetite and tolerances and requires the covered entity to reduce its residual cyber risk to the appropriate level approved by the Board.[55]

Senior leaders with responsibility for cyber risk oversight would be independent of business line management and would need to have direct, independent access to the Board.[56] These senior leaders would independently inform the Board on an ongoing basis of the firm's cyber risk exposure and risk management practices, including known and emerging issues and trends.[57]

There would be an independent risk management function that reports to the chief risk officer and Boards, as appropriate, regarding implementation of the firm's cyber risk management framework throughout the organization.[58] The independent risk management would be continually required to assess the

---

[50] Advance Notice of Proposed Rulemaking, Board of Governors of the Federal Reserve System, Enhanced Cyber Risk Management Standards (Oct. 26, 2016) https://www.fdic.gov/news/board/2016/2016-10-19_notice_dis_a_fr.pdf); *Legal Alert: Enhanced Cyber Risk Management Standards Announced in Joint Rulemaking Initiative by Treasury, Federal Reserve, and FDIC*, *supra* note 48; *Federal Banking Agencies Request Comment on Enhanced Cybersecurity* Standards, COVINGTON (Oct. 20, 1016), https://www.cov.com/-/media/files/corporate/publications/2016/10/federal_banking_agencies_request_comment_on_enhanced_cybersecurity_standards.pdf.

[51] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315, 74,320 (Oct. 26, 2016).

[52] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 74,320–74,321.

[53] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 81 Fed. Reg. 74,321.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 74,321–74,322.

firm's overall exposure to cyber risk and promptly notify the CEO and Board, as appropriate, when its assessment of a particular cyber risk differs from that of a business unit, as well as of any instances when a unit of the covered entity has exceeded the entity's established cyber risk tolerances.[59] It is essential that the independent risk management function have and maintain sufficient independence, stature, authority, resources, and access to the Board to ensure that the operations of the entity are consistent with the cyber risk management framework.[60] The reporting lines must be clear and separate from those for other operations and business units.[61]

The Federal Regulators are squarely focused on the safety and soundness of financial institutions and the financial system as a whole, and less on consumer protection[62], which is of critical importance for the NYDFS and the NAIC. The Federal Regulators are seeking comment from stakeholders on the ANPR, and plan to use the information gathered to develop a more detailed proposal, which will also be open to public comment.[63]

CONCLUSION

The latest cybersecurity regulatory activity represents an accelerating trend of heightened cybersecurity standards for financial institutions. Boards are critical to creating such policies and providing much needed oversight. And in the case of NYDFS, even a certification of compliance to the regulator.[64] While achieving effective cyber-risk governance overall will be a difficult and complex task and while perfection in this area will never be achieved[65], it is very important for insurance company Boards to take cyber security seriously. Boards that do not properly address the growing cybersecurity threat and oversee the creation of effective cybersecurity policies and programs with accompanying corporate governance will be at serious risk of failing to provide

---

59 Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 74,322.

60 *Id.*

61 *Id.*

62 *Legal Alert: Enhanced Cyber Risk Management Standards Announced in Joint Rulemaking Initiative by Treasury, Federal Reserve, and FDIC*, *supra* note 48.

63 Luke Dembosky et al., *Federal Financial Regulators to Propose Enhanced Cyber Risk Management* Standards, DEBEVOISE & PLIMPTON (Oct. 25, 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/10/20161025_federal_financial_regulators_to_propose_enhanced_cyber_risk_management_standards.pdf.

64 23 N.Y.C.R.R. 500.17(b) (2017).

65 Bonime-Blanc, *supra* note 6.

required oversight and may also run afoul of the growing body of cyber-regulations.