WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Companies Face a Maze of Cybersecurity Regulations and Heightened Risk Management

July 27, 2017

AUTHORS

Elizabeth P. Gray | Daniel K. Alvarez | Katherine Doty Hanniford | Neal E. Kumar | Marc J. Lederer

Recent developments in the cybersecurity landscape – from the devastating Petya and WannaCry ransomware attacks to efforts by regulators to solve the cybersecurity puzzle – underscore the importance that senior management and corporate boards embrace and manage cybersecurity as an enterprise risk and implement a well-tested and evolving cybersecurity program, including a well-considered incident response plan to maximize resiliency. The heightened focus by the press, investors, and regulators on cybersecurity and cyber-resiliency poses unique challenges to companies, particularly financial services firms, that are subject to multiple regulators and differing regulatory approaches to cyber-risk management.

In this Memo, we highlight some of the major regulatory issues that financial services firms need to consider as they seek to manage cybersecurity risk. As discussed below, irrespective of their stated approach to cyber-risk management, regulators at every level of government – from the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC"), to state-level regulators in New York and Colorado, to international regulators such as the United Kingdom's Financial Conduct Authority (the "FCA") and the European Union data protection authorities (now implementing the new General Data Protection Regulation) – expect a "security culture," with comprehensive and constant board, senior management, and employee commitment to cybersecurity.

I. Federal Regulators Focus on Cybersecurity

In the United States, policymakers at the highest levels of the Federal government are focused on the task of managing cyber-risk. Treasury Secretary Steven Mnuchin has underscored the importance of regulatory agencies focusing on cybersecurity in all their oversight responsibilities.[1] SEC Chairman Jay Clayton and CFTC Acting Chairman J. Christopher Giancarlo both have signaled the importance of cybersecurity risk management.

1. SEC Expects Comprehensive Cybersecurity Programs.

The SEC has an established track record of cybersecurity oversight on which to expand its focus and reach. Over the past few years, the agency has implemented cybersecurity regulations, conducted cybersecurity examinations, and brought enforcement actions to enforce its cybersecurity regulations against investment advisers and broker-dealers. The SEC will continue its oversight of cyber-risk of SEC registrants under its new chairman, Jay Clayton.

SEC registrants—including public companies—should expect an increased focus on public disclosures and cybersecurity risk management, including cyber-resiliency. The SEC is expected to focus on the adequacy and accuracy of SEC registrants' public disclosures about their cybersecurity programs, cyber-risks, and cyber-events.[2] Accordingly, public companies and registered entities should be prepared to revisit their disclosures to ensure that cybersecurity risks and events are discussed in an accurate and complete fashion. While the SEC has not yet brought an action against a public company for inadequate disclosures relating to cybersecurity breaches and risk management, the SEC has been actively investigating instances in which data breaches may not have been disclosed in a timely or complete manner to investors.[3]

In addition, Chairman Clayton has stated that he will expect public companies as well as investment advisers and broker-dealers to have comprehensive and appropriately evolving cybersecurity programs, with tested incident response plans in place.[4] This cybersecurity risk management extends to due diligence regarding cybersecurity risk in connection with initial public offerings and acquisitions. The SEC focus on cybersecurity risk management is further highlighted by the SEC's release of a cybersecurity risk alert on May 22, 2017, which strongly encouraged investment advisers and broker-dealers to review their cybersecurity programs in light of the recent WannaCry ransomware attack that affected thousands of computers and businesses in over 100 countries around the world.[5] The risk alert signals that Chairman Clayton will act on the concerns he has expressed regarding cybersecurity risk in the financial markets, and further indicates the SEC's

---

1 Axios interview with Steven Mnuchin, March 24, 2017, available here.

2 Jay Clayton, SEC Nominee, Senate Banking, Housing, and Urban Affairs Committee Confirmation Hearing (Mar. 23, 2017), available here. Jay Clayton, Remarks at the Economic Club of New York (July 12, 2017), available here.

3 Aruna Viswanatha and Robert McMillan, *Yahoo Faces SEC Probe Over Data Breaches*, WALL ST. J. (Jan. 23, 2017), available here.

4 *Clayton Backs Improvements to Cybersecurity Disclosures*, THOMSON REUTERS TAX & ACCOUNTING NEWS (Mar. 27, 2017), available here.

5 Willkie Client Memorandum, *OCIE Reminds SEC Firms About Cybersecurity Following Global Ransomware Attack*, May 22, 2017, available here.

continued interest in requiring firms to test the sufficiency of their cybersecurity programs. Firms that fail to conduct regular risk assessments and penetration testing that incorporate current threats may be considered inadequate by SEC examiners and face investigative risk by the SEC's Division of Enforcement.

2. CFTC Signals Collaborative Approach to Cybersecurity.

Chairman Giancarlo has signaled a "bottom-up, principles-based" approach to cybersecurity risk management by the CFTC, based on his stated belief that "markets themselves, reflecting the myriad actions of the broad sway of participants, remain the most efficient agents of change known to humankind."[6]

The CFTC's 2016 System Safeguard Rules are consistent with this approach and expressly embrace a requirement to follow "generally accepted standards and best practices" for safeguarding market infrastructure. The System Safeguard Rules were designed to prevent increasingly sophisticated cyber-attacks and help companies recover quickly through the regular updating of adequate policies and procedures.[7] The System Safeguard Rules apply to entities that form part of the futures and swaps market infrastructure, including the exchanges, clearing organizations, and swap data repositories. As of March 2017, the firms subject to the rule were expected to be in compliance with the provisions relating to vulnerability testing and security incident response plans. As of September 2017, regulated firms are expected to be in compliance with the provisions relating to penetration testing, certain controls testing, and enterprise technology risk assessments.

In a recent meeting of the CFTC's Market Risk Advisory Committee, industry urged the CFTC to develop a flexible approach to cybersecurity. In light of the CFTC's bottom-up, market-driven approach, the emerging industry view appears to be that although the Internet cannot be fully protected, market participants should be familiar with leading industry standards for cybersecurity risk management, such as the National Institute of Standards and Technology ("NIST") framework. The CFTC continues to explore the frontier of public-private coordination in understanding and responding to cybersecurity threats.

II. State Regulators Join the Cybersecurity Fray

At the state level, New York and Colorado have established a blueprint for state regulators to use to press forward with cybersecurity regulations that require specific procedures and risk assessments to mitigate cyber-related vulnerabilities. Under these regulations, covered entities must develop a clear understanding of what a "security culture" entails.

---

6 Keynote Address of CFTC Commissioner J. Christopher Giancarlo before the 2015 ISDA Annual Asia Pacific Conference, Oct. 26, 2015, available here.

7 Willkie Client Memorandum, *The New Administration: Potential Cyber and Privacy Issues,* Dec. 21, 2016, available here.

1. NYDFS Offers Guidance for Regulatory and Reporting Compliance.

The New York Department of Financial Services ("NYDFS") cybersecurity regulation, which became final and effective on March 1, 2017, requires covered entities to be in compliance by August 28, 2017 and to provide the first annual certification by February 15, 2018.[8] "Covered entities" are those entities supervised by the DFS that are doing business in New York and "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" of New York, such as banks and insurance companies. As covered entities come into compliance, the NYDFS has released guidance in the form of Frequently Asked Questions ("FAQs"), which it has periodically updated.[9] The FAQs offer insight into NYDFS expectations regarding the notice, third party oversight, and continuous monitoring provisions of the cybersecurity regulations, among others.

The FAQs clarify that covered entities are required to notify the NYDFS of "Cybersecurity Events," including those that involve consumer harm, whether actual or potential.[10] Specifically, even though New York's information security breach and notification law requires notice to affected consumers following a data breach, such a breach must also be separately reported to the NYDFS. Covered entities must notify the NYDFS as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred. The FAQs also note that covered entities' cybersecurity programs and policies will need to address, to the extent possible, consumer data privacy and other consumer protection issues.

In addition, the FAQs underscore that the requirements with respect to covered entities' oversight of third-party service providers do not impose a "one size fits all solution" but rather mandate a risk assessment to determine appropriate controls based on the unique facts and circumstances presented.

The FAQs further clarify the requirement of effective continuous monitoring as a component of a cybersecurity program's penetration testing and vulnerability assessment. The NYDFS does not require the use of a specific technology in this context, but it requires the "ability to continuously, on an ongoing basis, detect changes or activities within a Covered Entity's Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity." The FAQs specifically contrast this notion of continuous monitoring with periodic or non-continuous manual review of logs or firewall configurations, which would be insufficient for purposes of this requirement.

---

8 Key Dates under New York's Cybersecurity Regulation (23 NYCRR § 500), available here. Willkie Client Memorandum, *New York Department of Financial Services Issues Amended Cybersecurity Regulations Affecting Financial Institutions, Insurers and Other Covered Entities*, Jan. 11, 2017, available here.

9 NYDFS Frequently Asked Questions Regarding 23 NYCRR Part 500, available here.

10 Cybersecurity Requirements for Financial Services Companies, 23 NYCRR §500 (2017), available here.

2. Colorado Division of Securities Nears Final Rules.

Colorado recently adopted cybersecurity regulations that became effective on July 15, 2017, and require broker-dealers and investment advisers regulated by the Colorado Securities Division (the "Division") to establish and maintain written procedures reasonably designed to ensure cybersecurity. The Division recently released rules that clarify "what factors the Division will consider when determining if the procedures by the firm are reasonably designed to ensure cybersecurity."[11] The rules set forth a list of optional factors for a firm to consider in determining whether its cybersecurity procedures are reasonably designed, require covered broker-dealers and investment advisers to include cybersecurity as a part of their risk assessment, and list specific components that should be included in a firm's cybersecurity procedures "to the extent reasonably possible." These components include an annual risk assessment, the use of secure email for the transmission of "Confidential Personal Information,"[12] authentication practices and procedures, and client risk disclosures.

III. International Regulators Also Focus on Cyber and Data Security

The focus on cybersecurity does not stop at the shoreline. As evidenced by the recent WannaCry and Petya attacks, the threats posed by cyber-attacks are transnational, and a number of non-U.S. jurisdictions are already taking steps to address it.

1. FCA Focuses on Coordination and Resiliency.

The UK's FCA has prioritized cybersecurity and especially cyber-resilience as a regulatory focus over the coming year. In its 2017-2018 Business Plan, the FCA has stated that it intends to (1) establish coordination groups across the sectors it regulates to share experiences and foster innovation; (2) undertake technology and cyber-capability assessment on all firms considered more at risk of attack; and (3) analyze cyber-resilience risks created by new regulatory initiatives.[13]

The FCA considers good cybersecurity measures to include "effective risk management, complemented with good basic controls such as malware prevention, user education and awareness, and incident management arrangements." In addition to these measures, firms are encouraged to collaborate and share intelligence to keep the industry safe and secure in the future.

---

[11] Draft Statement of Basis and Purpose, Promulgation of Amendments to Division Rules, Colorado Division of Securities, March 6, 2017.

[12] "Confidential Personal Information" is defined as "a first name or first initial and last name" used in combination with any of the following information: (1) Social Security number; (2) driver's license or identification card number; (3) account, debit, or credit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; (4) an individual's digitized or electronic signature; or (5) user name, email address, or other unique identifier in combination with a password, access code, security questions, or authentication information that would permit access to an online account.

[13] FCA Business Plan 2017/18, available here.

In the view of FCA Executive Director Nausicaa Delfas, the most prominent cybersecurity threats affecting the financial services sector include distributed denial-of-service (DDOS) attacks and the installation of "ransomware" software on firms' networks.[14] To combat these threats, the FCA expects firms to "maintain online and offline backups to ensure that data can be restored without the need to pay a ransom."[15]

2. New Security Requirements in the GDPR.

As we have explained in previous Client Memoranda,[16] the GDPR significantly expands the scope of requirements applicable to entities that handle personal data of any EU data subject. In particular, the GDPR's focus on the security of personal data places significant emphasis on firms' taking a systematic approach to managing cyber-risk.

Under the GDPR, organizations must implement an "appropriate level of security" for the personal data they collect and hold, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. As defined in the regulation, the "appropriate level of security" takes into account a number of factors, among them the state of the art; the costs of implementation; the nature, scope, context, and purposes of the processing; and the risks and severity of harm to the data subjects. The regulation does not prescribe any particular strategy, tool, or tactic, but it does suggest that pseudonymization and encryption should be strongly considered as part of an organization's security toolkit.

In addition, GDPR requires that organizations that intend to engage in processing that is likely to result in high risk to the rights of the data subject conduct a data protection impact assessment ("DPIA") prior to processing such information. When a DPIA finds that the processing presents high risk, the GDPR requires the company to consult and cooperate with the local data protection authority, who may then provide guidance and instruction.

Finally, one of the most-discussed components of the GDPR is the requirement that certain organizations designate a Data Protection Officer to oversee processing operations. While this may not be a new requirement for all organizations – some EU countries already require appointing a DPO in certain circumstances – the GDPR's EU-wide mandate reinforces that policymakers expect organizations to make cybersecurity risk management a constant and integral component of their overall risk management efforts.

---

[14] Speech by Nausicaa Delfas, Executive Director at the FCA, delivered at the Financial Information Security Network (Apr. 24, 2017), available here.

[15] *Id.*

[16] Willkie Client Memoranda, *T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?*, May 25, 2017, available here; *New European General Data Protection Regulation Officially Adopted*, May 10, 2016, available here; and *Agreement on EU General Data Protection Regulation Sets the Stage for New Obligations and Higher Penalties for Noncompliance*, Dec. 17, 2015, available here.

IV. Conclusion

As cybersecurity continues to be a regulatory priority and cyber-threats continue to grow, public companies and financial services firms should work closely with their legal advisers to follow regulatory developments and manage cybersecurity risk, meet regulator expectations, and position themselves well for resiliency in response to a cybersecurity event. Those firms that are led by engaged senior managers and boards who treat cybersecurity as an enterprise risk will, by their very nature, more closely align their risk management practices with regulatory expectations, and should in theory be better positioned to withstand the impact of adverse cyber-events.

If you have any questions regarding this memorandum, please contact Elizabeth P. Gray (202-303-1207, egray@willkie.com), Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Katherine Doty Hanniford (202-303-1157, khanniford@willkie.com), Neal E. Kumar (202-303-1143, nkumar@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

July 27, 2017