ALERT MEMORANDUM

SEC Issues Risk Alert Based on Cybersecurity Survey

August 11, 2017

This week, the Securities Exchange Commission ("SEC"), Office of Compliance Inspections and Examinations (the "OCIE"), published a Risk Alert describing its findings from its second cybersecurity survey of regulated entities (the "Cybersecurity 2 Initiative").[1] The survey covered 75 registered broker-dealers, investment advisers, and investment companies and built upon OCIE's prior round of cybersecurity examinations in 2014 (the "Cybersecurity 1 Initiative").[2]

While OCIE found improvements in cybersecurity preparedness since the Cybersecurity 1 Initiative, it also identified areas for improvement. Among other things, OCIE concluded that it is not sufficient for firms to simply establish written cybersecurity policies and procedures—such policies must also be maintained, sensibly enforced, and capable of addressing cybersecurity deficiencies as they arise.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

The full text of the Risk Alert can be accessed via this link:

https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

[1] *See* OCIE Risk Alert, "Observations from Cybersecurity Investigation" (August 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.
[2] *See* OCIE Risk Alert, "Cybersecurity Examination Sweep Summary" (February 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

OCIE's Findings

OCIE's Cybersecurity 2 Initiative focused on the following areas of cybersecurity preparedness: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response. In general, OCIE found improvements in cybersecurity practices in these areas since its Cybersecurity 1 Initiative.

Among other things, OCIE noted that "all broker-dealers, all funds, and nearly all advisers" that were examined maintained written policies and procedures relating to the protection of customer or shareholder information; during the Cybersecurity 1 Initiative, "comparatively fewer" broker-dealers and advisers had such policies. OCIE also observed that firms were conducting periodic risk assessments and penetration tests to identify threats and vulnerabilities, as well as using systems or tools to prevent, detect, and monitor for leaks of personally identifiable information. Most firms also had policies addressing the SEC's Regulation S-ID,[3] aimed at preventing identify theft, and Regulation S-P,[4] which covers the privacy of consumer financial information.

Despite these improvements, OCIE "observed one or more issues in the vast majority of the Cybersecurity 2 Initiative examinations." One way that firms went wrong was by instituting polices that were not reasonably tailored to address situations employees are likely to face. For example, some policies were too general, vague, or lacked specific guidance for implementing policy requirements. The survey also revealed that some firms did not consistently enforce their policies and procedures. Specifically, while firm policies required periodic reviews of customer protection and security protocols, in practice those reviews were performed less frequently than called for by the policies. In addition, policies requiring cybersecurity training for employees were not always enforced. Significantly, OCIE also found that some firms did not adequately conduct system maintenance or remediate identified cybersecurity shortcomings. For instance, firms failed to install software patches needed to address identified security vulnerabilities or relied on outdated operating systems that were not supported by such security patches. Firms also failed to promptly remediate even high-risk findings identified in their penetration tests and vulnerability scans.

Implementing Robust Policies and Procedures

By way of guidance, OCIE identified certain hallmarks of strong cybersecurity policies and procedures that firms "may wish to consider" implementing. Examples of robust policies and procedures observed in the survey included the following:

- *Inventory*: Maintaining a complete inventory of the firm's data and information and corresponding classification of its risks, vulnerabilities, and business consequences, organized by service provider and vendor, as applicable.

- *Instructions*: Preparing detailed cybersecurity-related instructions. For example, by establishing policies and procedures for reviewing the effectiveness of the firm's security solutions, monitoring and auditing of the firm's information security framework, tracking access rights, and reporting and mitigating the loss or disclosure of sensitive information.

- *Data Testing and Vulnerability*: Creating schedules and processes for testing the integrity and vulnerability of firm data. For example, by conducting scans of IT infrastructure to identify weaknesses (and rectify any issues), and implementing policies for the rollout of security patches needed to correct identified problems.

- *Access*: Establishing and enforcing controls related to accessing data and systems. For example, by implementing "acceptable use" policies governing employee conduct on firm

[3] *See* 17 C.F.R. Part 248, Subpart C—Regulation S-ID: Identity Theft Red Flags.

[4] *See* 17 C.F.R. Part 248, Subpart A—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information.

networks and equipment, instituting controls for mobile devices connected to firm networks (such as passwords or encryption), obtaining logs of third-party vendor activity on firm networks, and requiring prompt termination of access for employees leaving the firm.

- *Training*: Instituting mandatory information security training for new employees and periodically thereafter, as well as policies to ensure compliance.

- *Oversight*: Requiring senior management approval of cybersecurity policies.

Takeaways

OCIE's Cybersecurity 2 Initiative and the resulting Risk Alert reflect a continuing regulatory focus on cybersecurity preparedness.[5] OCIE has identified cybersecurity as a priority for 2017,[6] and the Risk Alert itself states that OCIE plans to conduct additional cybersecurity examinations in the future. The SEC's newly installed Directors of Enforcement have also said that they view cybersecurity as a top priority for the agency.[7] Going forward, firms should continue to enact robust, tailored, and detailed cybersecurity policies and procedures. Firms should also ensure that their policies are enforced, address likely risks, provide for remediation of any lapses, and require appropriate documentation of any incidents.

…

CLEARY GOTTLIEB

[5] In a similar vein, the Federal Trade Commission ("FTC") recently launched a new weekly blog series aimed at providing data security insight gleaned from its closed investigations. *See* Thomas Pahl, "Stick With Security: Insights into FTC Investigations" (July 21, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.

[6] OCIE, "Examination Priorities for 2017", https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf.

[7] Sarah N. Lynch, *Exclusive: New SEC Enforcement Chiefs See Cyber Crime as Biggest Market Threat, Reuters* (June 9, 2017) *available at* https://www.reuters.com/article/us-usa-sec-enforcement-exclusive-idUSKBN18Z2TX.