STRADLEY RONON ATTORNEYS AT LAW

Adviser Alert

A Publication of the Stradley Ronon
Investment Management Group

WWW.STRADLEY.COM

MAY 2014, NO. 4

Stradley Ronon Stevens & Young, LLP
2005 Market Street, Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
Malvern, Pa.
Harrisburg, Pa.
Wilmington, Del.
Cherry Hill, N.J.
New York, N.Y.

CYBERSECURITY UPDATE: What Information Will Be Requested by the SEC's Office of Compliance Inspections and Examinations During an Examination?

By Kenneth L. Greenberg

On April 15, as part of a National Exam Program Risk Alert published by the Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC), OCIE announced that it will conduct examinations of more than 50 registered broker-dealers and investment advisers focusing on the following cybersecurity issues:

- Cybersecurity governance,
- Identification and assessment of cybersecurity risks,
- Protection of networks and information,
- Risks associated with remote customer access and funds transfer requests,
- Risks associated with vendors and other third parties,
- Detection of unauthorized activity, and
- Experiences with certain cybersecurity threats.

This examination sweep follows on the heels of the Financial Industry Regulatory Authority's (FINRA) targeted examination sweep to assess brokerage firms' approaches to managing cybersecurity threats. FINRA similarly focused on approaches to information technology risk assessment, business continuity plans in case of a cyber-attack, organizational structures and reporting lines, processes for sharing and obtaining information about cybersecurity threats, understanding of concerns and threats faced by the industry, assessment of the impact of cyber-attacks on the firm over the past 12 months, approaches to handling distributed denial of service attacks, training programs, insurance coverage for cybersecurity-related events, and contractual arrangements with third-party service providers.

OCIE attached to its Risk Alert a sample information and document request that will be used in its examinations. It is very detailed in identifying the cybersecurity policies, procedures and practices that the OCIE staff expects to see from examined firms. This request serves as a road map for firms to use in assessing their own cybersecurity preparedness. In contrast, Rule 30 of Regulation S-P, the customer records and information safeguards rule, merely sets forth a general obligation and requires every SEC-registered broker, dealer, investment company and investment adviser to adopt written policies and procedures that address "administrative, technical, and physical safeguards for the protection of customer records and information" that are "reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to

the security or integrity of customer records and information; and (3) protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

As noted in the Risk Alert, some of OCIE's requests track information outlined in the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity."[1] The framework provides risk management processes for firms to identify, detect and protect against cybersecurity threats and respond to and recover from cybersecurity events. The framework also provides a series of implementation tiers that allows firms to assess the "rigor and sophistication" of their cybersecurity risk management practices and their integration into their overall risk management practices.

Time will tell what the objective(s) is (or are) of OCIE's cybersecurity examination initiative. Is it a means to better understand how prepared the investment management industry is in handling cybersecurity threats and thus determine what constitutes cybersecurity best practices? Or is it to serve as a springboard for enforcement actions to make an example of those firms that OCIE perceives as not having met their obligations to safeguard customer records and information?

The attached appendix summarizes the policies and practices that OCIE will be expecting to review and lists certain of OCIE's information requests regarding cybersecurity events. For many of the items on OCIE's document and information request, OCIE also asked a number of questions about the item. These questions have been omitted in the appendix. The appendix can be used as a checklist to assess your own firm's cybersecurity preparation. To the extent that your firm does not have a particular practice or policy in place, now is the time to implement such a policy or practice, or at minimum, develop a sound explanation as to why such a policy or practice is not necessary for your firm. The NIST framework is also a good resource for assessing a firm's cybersecurity practices.

If you would like more information, contact Kenneth L. Greenberg at kgreenberg@stradley.com or 215.564.8149.

---

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.