By Thomas D. Giachetti

SEC Clarifies RIAs' Cybersecurity Obligations

The SEC is conducting its second round of cyber exams, so RIAs must take three steps right away to ensure compliance

In April 2014, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert indicating the SEC will focus on cybersecurity as a major issue. Almost 18 months later, many RIAs are still confused about what they are required to do to comply with SEC guidance to protect their clients' confidential information.

Two recent developments clarified those obligations. Simply put, RIAs are obligated to implement robust technical controls to protect their clients' sensitive and confidential information from reasonably foreseeable threats, and to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of that information.

THE SEC's CYBERSECURITY INITIATIVE

On March 26, 2014, the SEC sponsored a cybersecurity roundtable, during which Chairwoman Mary Jo White discussed the "compelling need for stronger partnerships between the government and private sector" to address cyberthreats.

On April 15, 2014, OCIE released a Risk Alert saying it would conduct examinations of more than 50 financial institutions, including RIAs, focused on: 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.

The Risk Alert attached a list of sample questions comprising 28 requests

ILLUSTRATION: DAN BEJAR/© THEISPOT.COM

with multiple sub-parts. For example, one of the simpler questions is whether a firm maintains an inventory of its physical devices and systems. Some more complex and technical questions include whether a firm maintains protection against distributed denial of service (DDoS) attacks for critical Internet-facing IP addresses, or aggregates and correlates event data from multiple sources to detect unauthorized activity on its networks or devices.

SEPTEMBER 2015 DEVELOPMENTS

On Sept. 15, 2015, OCIE released another Risk Alert to elaborate upon "the areas of focus for OCIE's second round of cybersecurity examinations, which would involve more testing to assess implementation of firm procedures and controls."

According to OCIE, this next round of examinations would focus on an RIA's governance and risk assessment, access rights and controls, data loss prevention, vendor management, staff training and incident response.

Much like the previous Risk Alert, the September Risk Alert also attaches an appendix with a list of information that OCIE "may review as part of its cybersecurity examinations."

Critically, a footnote in the September Risk Alert references Regulation S-P, Rule 30(a), which requires RIAs to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, which must be reasonably designed to: ensure their security and confidentiality; protect against anticipated threats; and protect against unauthorized access to or use of customer records or information.

In the context of this Risk Alert, the footnote signals that RIAs that do not adopt these written policies and procedures are potentially violating Rule 30(a).

THE TAKEAWAY

In light of these developments, I strongly recommended all RIAs undertake the following action without delay:

1. Consult with IT staff or vendors to implement technical controls and safeguards to better protect the firm's network and clients' information.

2. Evaluate and potentially purchase an insurance policy to cover damages rising from a hacking event or other form of data breach.

3. Adopt a written cybersecurity policy addressing the two appendices attached to the April 2014 and September 2015 Risk Alerts. The written cybersecurity policy should be tailored to the firm's actual business practices and IT framework, and should include means to test the efficacy of the policy. **IA**

Thomas D. Giachetti is chairman of the Securities Practice Group of Stark & Stark. He can be reached at tgiachetti@stark-stark.com.