CLIENT ALERT

OCIE Issues New Report on Cybersecurity Practices

Aug.15.2017

On August 7, 2017, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a National Exam Program Risk Alert reporting its observations from its second round of cybersecurity examinations (Cybersecurity 2 Initiative). Although the OCIE Staff noted improvements since its 2014 examinations, the Cybersecurity 2 Initiative involved more validation and testing of procedures and controls, and pointed out areas needing additional improvement. OCIE also noted that investment advisers and funds lag behind broker-dealers in their cybersecurity programs.

In particular, the Staff cautioned against policies and procedures that are too generalized, firms not following their own procedures and scheduling, and firms not acting quickly to remediate identified problems.

OCIE noted that many policies and procedures did not provide employees with well-articulated implementation procedures that include detailed instructions regarding notification instructions and what other steps to take in the event of a breach or data loss. OCIE also found instances of instructions that contradicted other instructions, for example, inconsistency between remote customer access policies and policies for investor fund transfers.

Another area of concern was firms not following their own procedures. For example, reviews categorized as ongoing were conducted periodically or not at all, annual reviews were conducted less frequently, and firms did not ensure that employees actually completed cybersecurity training.

The OCIE Staff noted certain Reg SP concerns, including that some firms did not install patches in a timely fashion, used outdated and unsupported operating systems, and did not remediate high-risk findings from penetration tests or vulnerability scans.

OCIE stated that firms would benefit from considering certain best practices it observed during its examinations, including:

- Cybersecurity-related instructions: (1) specific points to be reviewed in penetration tests; (2) details regarding testing methodologies for security monitoring and system auditing of a firm's system; (3) specifics of tracking access rights modifications; and (4) listing contact persons in the event of data loss.
- Testing schedules and processes: (1) vulnerability scans of core IT infrastructure, with prioritized action items for identified concerns; and (2) beta testing patches prior to firm wide release.
- Established and Enforced Access Controls: (1) detailed "acceptable use" of firm IT; (2) controls for firm connected mobile devices (passwords and encryption); (3) requiring third-party vendors to periodically provide logs of their activity on firm systems; and (4) immediate termination of access for terminated employees and very prompt access termination for employees leaving voluntarily.
- Employee training: mandatory, with procedures to ensure training completed.
- Engaged senior management: vetting and approving policies and procedures.

The issues noted by OCIE and listing of best practices provide a wake-up call to firms to modify their procedures to better protect themselves from threats, such as ransomware and denial of service attacks that can cripple a firm, as well as from loss of customer data that can subject a firm to reputational risk as well as regulatory sanctions. OCIE concluded that cybersecurity remains one of the top compliance risks for financial firms. OCIE will continue to examine for cybersecurity compliance procedures and controls, including testing firms' implementation of those procedures and controls. In following the usual regulatory pattern, OCIE has progressed from examining whether policies and procedures are in place, to assessing their adequacy, and now to determining whether they are being implemented as written.For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com