Cybersecurity, Privacy & Data Protection Alert

May 1, 2015

SEC Issues New Cybersecurity Guidance for Investment Funds

On April 28, the Securities and Exchange Commission (SEC) Division of Investment Management (the "Division") published a Guidance Update setting forth cybersecurity concerns and advice for the registered investment companies and investment advisers it regulates. This is the most recent instance of the SEC's continued focus on cybersecurity. Cybersecurity was highlighted in the spring of 2014 as part of the National Exam Program (NEP) Examination Priorities released by the SEC's Office of Compliance Inspections and Examinations (OCIE). OCIE's cybersecurity priorities were discussed in more detail in the SEC's Compliance Outreach Program, which highlighted compliance-related issues that should be addressed by compliance officers and other senior executives of investment funds and advisers. Subsequently, in February of this year, the OCIE issued a Risk Alert following sweep exams conducted to analyze cybersecurity threats faced by investment advisers and broker-dealers. The results increased the SEC staff's concern regarding preparation of investment advisers for cybersecurity threats, especially as compared to that of broker-dealers.

The Division is now providing practical advice and specific measures that funds and advisers can implement in order to better prepare for the barrage of cybersecurity threats facing funds and all companies on a daily basis.

The Division suggested that funds and advisers:

1. Conduct a periodic assessment of:
    A. the nature, sensitivity and location of information that the firm collects, and the technology systems it uses
    B. internal and external cybersecurity threats to, and vulnerability of, the firm's information and technology systems
    C. security controls and processes currently in place
    D. the potential impact if the information or technology were compromised
    E. the effectiveness of the governance structure for the management of cybersecurity risk.
2. Create and implement a comprehensive strategy that is designed to prevent, detect and respond to cybersecurity threats, which could include:
    A. controlling access to systems and data via user credentials, authentication and authorization methods, firewalls, tiered access to sensitive information and system hardening (removing all non-essential software programs and unnecessary logins and ensuring software is continuously updated)

B. data encryption

C. restricting the use of removable storage media and deploying software to monitor for unauthorized intrusions and exfiltration of sensitive data

D. data backup and retrieval

E. an incident response plan.

3. Implement this cybersecurity strategy through written policies and procedures and training programs that provide guidance for monitoring threats; measures to prevent, detect and respond to such threats; and internal compliance with cybersecurity policies and procedures.

Notably, the Division reiterated its view that funds and advisers may be particularly vulnerable to data breach because of the prevalent use of third-party vendors and service providers, including fund managers, administrators, transfer agents and prime brokers. Accordingly, "funds and advisers may also wish to consider assessing whether protective cybersecurity measures are in place at relevant service providers." Further, firms should educate investors and clients about how to reduce their exposure to cybersecurity threats as well. A breach can just as easily occur through the actions or lack of data security by the clients themselves.

Finally, the Division focused on the connection between cybersecurity and violations of the federal securities laws. The Division noted that cyber attacks and data breaches can result in actions, or failures to act, that constitute violations of federal securities laws. For example, cybersecurity failures could impact identity theft, fraud and business continuity obligations.

It is clear that the SEC remains intently focused on cybersecurity concerns. While the Division's suggested measures are phrased as actions that funds and advisers may wish to consider, the Division is also sending a message regarding its expectations for funds and advisers. The failure to address the Division's guidance could result in examination deficiencies, enforcement action or private litigation. Cybersecurity is not merely a technology issue; rather, it has broad business, reputation and regulatory implications. Accordingly, funds and advisers should take heed of the Division's warnings: create comprehensive and specifically tailored cybersecurity policies and procedures, and persistently monitor their and their clients' data and risk.

Contact Information

If you have any questions regarding this alert, please contact:

Prakash H. Mehta
pmehta@akingump.com
212.872.7430
New York

Kelli L. Moll
kmoll@akingump.com
212.872.8041
New York

Eliot D. Raffkind
eraffkind@akingump.com
214.969.4667
Dallas

Stephen M. Vine
svine@akingump.com
212.872.1030
New York

Ian Patrick Meade
imeade@akingump.com
+44 20.7012.9664
London

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520
Abu Dhabi

Michelle A. Reed
mreed@akingump.com
214.969.2713
Dallas

David S. Turetsky
dturetsky@akingump.com
202.887.4074
Washington, D.C.

Jenny M. Walters
jwalters@akingump.com
214.969.4654
Dallas