BRACEWELL

INSIGHTS

# SEC Issues New Guidance on Cybersecurity for Investment Companies and Investment Advisors

May 29, 2015

On April 28, 2015, the SEC's Division of Investment Management released a Guidance Update providing cybersecurity guidance for investment companies and investment advisors (firms).[1] The SEC has prioritized cybersecurity as a critical issue for such firms, especially for those that retain confidential client information. The SEC's guidance was issued on the heels of a cybersecurity examination sweep conducted by the SEC's Office of Compliance Inspections and Examinations, in which more than 88 percent of broker-dealers and 74 percent of advisors disclosed that they had been the subject of some form of cybersecurity incident, originating internally from employees or externally from hackers.[2] After this survey of basic cybersecurity practices, the Division of Investment Management's Guidance Update offers more specific directives to investment funds and advisors.

The Guidance Update is quick to point out that there is no one-size-fits-all strategy behind crafting and implementing a cybersecurity program, and that each firm will need to customize its approach to addressing cybersecurity risk by looking to its own individual operations. However, the Guidance Update does provide three measures that firms should consider to address cybersecurity risks:

1. ***Take stock of your current situation.***

Firms should conduct an assessment of the "nature, sensitivity, and location" of their information and determine what kind of detrimental impact any compromise of such information would cause. Firms should also ascertain and weigh potential cybersecurity threats and whether their current security protocols would be effective in handling a cybersecurity incident.

2. ***Create a comprehensive cybersecurity strategy.***

Firms should strategize how to prevent, detect and respond to potential cybersecurity threats. This strategy should consider information governance policies – including controlling who has access to what information, installing firewalls, encrypting data, and creating a data back-up plan. Additionally, firms should consider restricting the use of removable storage media, such as flash drives, to prevent data loss or breach. Firms should also develop an incident response plan and regularly test the effectiveness of their program.

3. ***Implement the strategy.***

Firms should use written policies and procedures to implement a cybersecurity plan. Employees should receive training on the plan and the appropriate response to cybersecurity

threats.

The Guidance Update recognizes that it is "not possible for a fund or advisor to anticipate and prevent every cyber attack." However, ensuring that firms consider at least the three identified measures will assist with mitigating the impact of any cyberattacks and ensure compliance with applicable laws and regulations.

**Takeaways**

Investment firms store vast amounts of confidential client information, making them an attractive target for cyberattacks. In the Guidance Update, the SEC highlights the importance of an effective, comprehensive cybersecurity plan – both to protect client information and to maintain compliance with securities regulations.

Bracewell has extensive experience with crafting and implementing cybersecurity and incident response plans. Should you require additional information regarding the recent Guidance Update or cybersecurity programs, please contact ***Shamoil T. Shipchandler*** (214) 758-1048.

---

[1] The full text of the Guidance Update is available ***here.***

[2] The full text of the Summary is available ***here.***