



FEBRUARY 2014

*If you have any questions  
about this Advisory,  
please contact:*

RICHARD LEVAN  
215.988.8316  
rlevan@wiggin.com

CONOR MULLAN  
215.988.8319  
cmullan@wiggin.com

## SEC to Examine RIAs and B-Ds for Cyber Security Procedures and Protections

At the SEC's recent compliance outreach program, a high-level SEC official announced that the National Examination Program ("NEP") will be reviewing investment advisers' policies and procedures for preventing cyber attacks. In particular, the SEC is looking at the risk created by investment advisers who give vendors access to their information technology systems.

As reported by *Reuters*, Jane Jarcho, National Associate Director of the SEC's investment adviser/investment company examination program, stated, "We will be looking to see what policies are in place to prevent, detect and respond to cyber attacks."

Jarcho's statement about investment advisers continues a theme recently articulated in the NEP's 2014 examination priorities. Among other things, NEP examiners will review firms' vendor due diligence procedures and ensure that investment advisers report cyber intrusions to their regulators.

### CURRENT SEC AND FINRA POLICY

Cyber security was previously identified as a priority for the SEC's investment adviser and broker-dealer examination programs, as well as for FINRA in its 2014 Regulatory and Examination Priorities Letter. Unfortunately,

neither the SEC nor FINRA has published specific guidance for registrants as the SEC did back in 2011 for public companies.

Ironically, the SEC was identified in a Congressional report this week as one of several U.S. agencies that possessed inadequate safeguards for protecting company and securities exchange data. According to the minority report of the Senate Homeland Security and Governmental Affairs Committee, cyber attacks directed at the SEC pose a serious risk to the public through the transmission of sensitive non-public information on major financial institutions, including stock exchanges, through SEC officials' personal e-mail and personal computers, sometimes on unsecured public networks.

Last April, when SEC Chair Mary Jo White took over the helm of the agency, U.S. Senate Commerce Committee Chairman Jay Rockefeller asked her to consider releasing more formalized Commission-level guidance to help ensure investors get information they need. White said she felt the guidance the commission issued in 2011 regarding public companies has been "helpful in improving disclosures." However, she added, the SEC plans to "continuously review" the issue to see if it should do more, as Rockefeller suggested.

CONTINUED ON NEXT PAGE

## SEC to Examine RIAs and B-Ds for Cyber Security Procedures and Protections CONTINUED

### SUPPLEMENTAL ADVICE

The SEC's new focus on cyber security augments the new and emerging issues and initiatives identified last month by its Office of Compliance, Inspections and Examinations. Those issues and initiatives include:

- Never-Before Examined Advisers
- Wrap Fee Programs
- Quantitative Trading Models
- Presence Exams
- Payments to Intermediaries for Distribution in Guise
- Fixed Income Investment Companies

### CONCLUSION

In light of the coming focus by the SEC on cyber security, registrants would be well advised to review their internal and external IT protocols, as well as their policies and procedures -- including business continuity plans -- to ensure all reasonable and necessary steps are being taken to safeguard client and firm data.

*Please feel free to contact us if you have any questions regarding this update or any other SEC-related matter.*

*This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.*