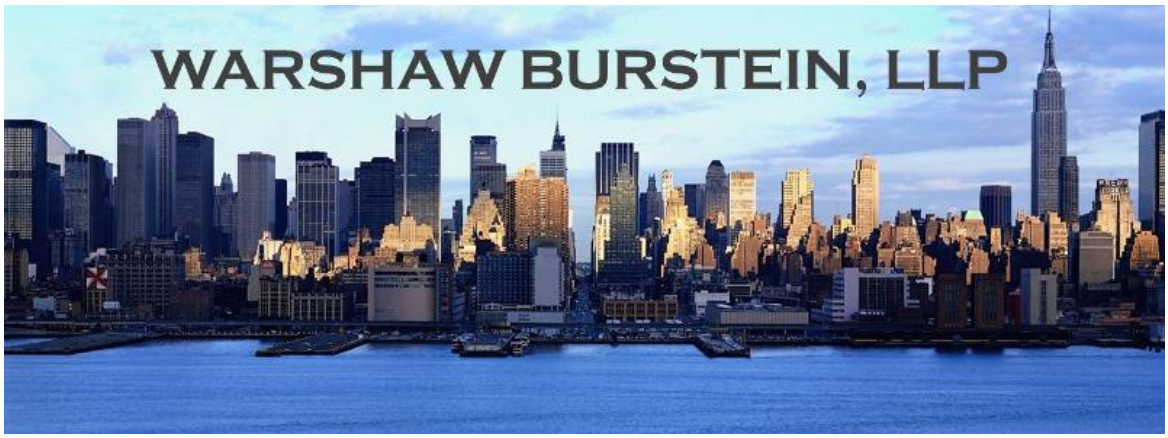

May 19, 2015

CLIENT ALERT

SEC Releases New Guidance on Cybersecurity for Investment Managers and Investment Advisers

The SEC's Division of Investment Management issued a Guidance Update on cybersecurity on April 28, 2015.[1] This Guidance Update follows a National Exam Program Risk Alert published by the Office of Compliance Inspections and Examinations ("OCIE") on February 3, 2015 that summarizes OCIE's observations from examinations of broker-dealers and investment advisers conducted under OCIE's Cybersecurity Initiative, and the SEC Cybersecurity Roundtable held on March 26, 2014. The Guidance Update reiterates the importance of cybersecurity and suggests actions that funds and investment advisers should include to make their cybersecurity protections more robust. The Guidance Update provides an overview that does not intend to be comprehensive and recognizes that "[B]ecause funds and advisers are varied in their operations, they should tailor their compliance programs based on the nature and scope of their businesses."

The Guidance Update highlights the need for firms to review their cybersecurity measures and suggests the following three-step process for funds and advisers to consider in order to address cybersecurity risks in their organizations.

1. Assess periodically:

    - the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
    - internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
    - security controls and processes currently in place;
    - the impact should the information or technology systems be compromised; and

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

- the effectiveness of the governance structure for managing cybersecurity risk.

2. Create a strategy to prevent, detect and respond to cybersecurity threats. This would include:

- controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening[2];
- data encryption;
- protecting against loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events;
- data backup and retrieval; and
- development of an incident response plan.

3. Implement the strategy created through:

- written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

In addition, firms should consider educating investors and clients about how to reduce their exposure to cybersecurity threats concerning their accounts.

The Guidance Update also focuses on the connection between cybersecurity and the federal securities laws, emphasizing that compliance policies and procedures should be "reasonably designed to prevent violations of the federal securities laws" and specifically suggests that compliance programs address "cybersecurity risk as it relates to identity theft and data protection, fraud and business continuity, as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions."

The Guidance Update also suggests that because funds and advisers rely on outside service providers to carry out their operations, they may wish to assess the protective cybersecurity measures that are in place at their relevant service providers.

Conclusion

The SEC recognizes it is not possible for a fund or adviser to anticipate and prevent every cyber attack. However, increased awareness and implementation of appropriate measures described in the Guidance Update will enable funds and advisers to better mitigate the impact of any such attacks should they occur, and the related effects on firm investors and advisory clients.

[2] System hardening means making technology systems less susceptible to unauthorized intrusions by removing all non-essential software programs and services, unnecessary usernames and logins, and by ensuring that software is updated continuously.

****

If you would like us to review your existing cybersecurity policies and procedures or would like us to prepare cybersecurity policies and procedures suitable for your business, please contact Meryl Wiener, any of the undersigned or your regular Warshaw Burstein attorney.

Frederick R. Cummings, Jr.	FCummings@wbcsk.com	(212) 984-7807
Thomas Filardo	TFilardo@wbcsk.com	(212) 984-7806
Marshall N. Lester	MLester@wbcsk.com	(212) 984-7849
Murray D. Schwartz	MSchwartz@wbcsk.com	(212) 984-7701
Stephen W. Semian	SSemian@wbcsk.com	(212) 984-7764
Kyle A. Taylor	KTaylor@wbcsk.com	(212) 984-7797
Meryl E. Wiener	MWiener@wbcsk.com	(212) 984-7731