Proskauer

Cybersecurity Guidance for Registered Investment Advisers

May 5, 2015

On April 28, the Securities and Exchange Commission (SEC) released a Guidance Update addressing the importance of cybersecurity and the steps registered investment advisers (and registered investment companies) may wish to consider in light of growing cybersecurity risks. This Guidance Update is the latest instance of the SEC's increased emphasis on cybersecurity as a priority for advisers. A Cybersecurity Roundtable was hosted by the SEC on March 26, 2014 and the Office of Compliance Inspections and Examinations released a Risk Alert on February 3, 2015 summarizing its cybersecurity examinations of over 100 advisers and broker-dealers.[1]

The Guidance Update provides several measures that advisers may wish to consider when creating a cybersecurity policy. These suggestions are not, however, intended to be comprehensive and advisers should tailor their cybersecurity policies to the particular nature and scope of their businesses.

Assessments

The Guidance Update suggests that to assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk, advisers should consider conducting a periodic assessment of the following:

- the nature, sensitivity and location of information that the adviser collects, processes and/or stores, and the technology systems utilized;
- the internal and external cybersecurity threats to and vulnerabilities of the adviser's information and technology systems;
- the security controls and processes currently in place;
- the impact on the adviser in the event that the information or technology systems become compromised; and

the effectiveness of the governance structure for the management of cybersecurity risk.

Cybersecurity Strategy

The Guidance Update also suggests that advisers should consider whether to develop, and routinely test, strategies to prevent, detect and respond to cybersecurity threats. Such strategies could 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 (*i.e.,* removing all nonessential software programs and services, unnecessary usernames and logins and diligently updating software);
- data encryption;
- protecting against the 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
- the development of an incident response plan.

Implementation

The Guidance Update further encourages advisers to implement cybersecurity strategies through written policies and procedures, as well as personnel training. Training of officers and employees should include a discussion of the applicable cybersecurity threats and the measures to prevent, detect and respond to such threats. The Guidance Update suggests advisers should routinely monitor their compliance with the cybersecurity policies and procedures.

The Guidance Update also states that advisers may wish to educate investors and clients about reducing their exposure to cybersecurity risks with respect to their accounts. Furthermore, the Guidance Update suggests that advisers consider assessing the adequacy of the cybersecurity measures employed by their service providers and determine whether their service-provider contracts sufficiently address technology issues and related responsibilities that arise in the case of a cyberattack. A service provider's access to an adviser's technology systems may also grant unauthorized access to sensitive data. Advisers may consider whether insurance coverage related to cybersecurity risks is necessary or appropriate.

Conclusion

Cybersecurity remains a prevalent business concern for advisers, and failure to identify points of vulnerability could result in unexpected cyberattacks. Cybersecurity threats should be addressed through the creation of specific policies and procedures, personnel training and ongoing testing and monitoring. For example, the compliance program could 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 investor transactions. When designing, implementing and monitoring cybersecurity programs, the Guidance Update suggests that advisers be mindful of their obligations under the federal securities laws. Advisers should consider continuously assessing cybersecurity risks, tailoring cybersecurity programs to the nature and scope of their businesses and regularly monitoring compliance with such programs. The staff recognizes that it is not possible for an adviser to anticipate and prevent every cyberattack. Appropriate planning to address cybersecurity and a rapid response capability may, nevertheless, assist advisers in mitigating the impact of attacks and any related effects on investors and clients, as well as compliance with federal securities laws.

If you have any questions regarding the Guidance Update or cybersecurity issues in general, please feel free to contact your usual lawyer at Proskauer or any of the Proskauer lawyers listed in this alert.

[1] Please see our February 6, 2015 client alert for more information on the SEC's Risk Alert.