CORE COMPLIANCE & LEGAL SERVICES, INC.

Risk Management Update
May 2014

CYBERSECURITY – IMPORTANT CONSIDERATIONS FOR INVESTMENT ADVISERS AND BROKER-DEALERS

Both the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA") have announced that they are conducting exams focused on the strength of financial firms' "cybersecurity."[1] FINRA is examining member broker-dealers, with the following four main goals in mind: (i) to understand better the types of threats that such firms face; (ii) to increase their understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT systems; (iii) to appreciate better firms' approaches to managing cyber threats, including through risk assessment processes, IT protocols, application management practices and supervision; and (iv) as appropriate, to share observations and findings with firms.[2]

The SEC's Office of Compliance Inspections and Examination ("OCIE") is examining both broker-dealers and SEC registered investment advisers, and according to the Risk Alert issued on April 15, 2014,[3] will be assessing, among other things:

- Cybersecurity governance;
- Identification and assessment of cybersecurity risks;
- Protection of networks and information;
- Risks associated with remote client access and fund transfer requests;
- Risks associated with vendors and other third parties;
- Detection of unauthorized activity; and
- Experience with cybersecurity threats.

This month's Risk Management Update focuses on some of the higher risks associated with cyber threats and provides suggestions on various testing and internal controls that both broker-dealers and investment advisory firms should consider in order to address, mitigate and/or eliminate risks and help ensure they have a strong cybersecurity program.

High Risk Areas Associated with Cybersecurity

Exposure to cybercrimes comes in many shapes and sizes, and mainly revolves around the use of technology, including computers, smart phones, and network servers. Risks pertaining to cyber breaches may differ between firms, primarily due to the variation in business practices and technological structures. Following is a list of five risks commonly attributable to weak cybersecurity management.

---

[1] Techopedia defines cybersecurity as "…preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management."
[2] *See* http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219.
[3] *See* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

1. *Lack of Involvement by Senior Management:* One of the highest risks surrounding cybersecurity is a firm's lack of understanding and identification of how cyber threats can affect the firm, its clients, and its employees. Firms with senior management who believe that the assessment of cyber crime exposure rests solely with the firm's compliance or technology personnel runs the risk that such lack of oversight may in fact further expose a firm if the compliance personnel are not fully cognizant of all aspects of a firm's business and technology use. It is critical that senior managers supervise the overall assessment process to confirm inclusion of all applicable business areas, practices, and firm personnel.

2. *Not Considering Associated Regulations:* Another risk is not being aware of the various regulations impacting cybersecurity programs. Both broker-dealer and investment advisory firms should consider regulatory requirements surrounding the following topics during their assessment of cyber risk:

- Privacy and safeguard controls for non-public information;
- Disaster recovery/business continuity planning;
- Anti-money laundering procedures;
- Custody and safeguarding of client assets;
- Identity theft protections; and
- Electronic data storage and destruction processes.

3. *Being Underinsured:* Firms also run a risk if they haven't considered insurance coverage and reviewed their current insurance policies to determine whether or not they have appropriate coverage in the case of a cybercrime. A number of insurance carriers now provide insurance covering cybercrimes, but it's important to understand exactly what is and is not covered and what steps are required upon the discovery of a cybercrime.

4. *Not Providing Training to Employees:* One critical component for any cybersecurity program is employee training. Lack of knowledge can carry with it a large risk of exposure for the firm. Not only should employees be thoroughly trained on the firm's cybersecurity policies and procedures, but such training also should include an explanation of some of the more commonly known cybercrimes. Common cybercrimes include phishing (also known as spoofing or spam); hacking of computer systems, identity and data theft, extortion and criminal copyright infringement. Be sure that the training includes every day examples of how activities can lead to cybercrimes, including unlawful access to confidential information, fraudulent withdrawal and transfer instructions, and unauthorized online transactions. Consider whether it would be helpful to hire a third party IT consultant to assist with your cybersecurity training program.

5. *Inadequate Due Diligence of Service Providers:* Firms risk culpability ramifications by not performing detailed reviews of service providers, such as IT vendors and other online data providers at least annually. Depending on circumstances, due diligence measures should include issuance of due diligence service provider questionnaires, requests for internal control reports, business continuity plans and cybersecurity measures, onsite demonstrations of controls, interviews with senior management, and certifications by the service provider related to their firm's cybersecurity safeguards.

Testing and Control Considerations

Included in the SEC's Risk Alert on Cybersecurity is a sample copy of the document request letter being sent to the firms they are auditing. The requested information is divided into the following categories:

- Identification of Risks/Cybersecurity Governance
- Protection of Firm Networks and Information
- Risks Associated with Remote Customer Access and Funds Transfer Requests
- Risks Associated with Vendors and Other Third Parties
- Detection of Unauthorized Activity
- Other

Financial firms should consider using the letter as a risk assessment tool to help identify potential gaps in their information security processes and assess the strength of their cybersecurity protection programs. Assessments of a firm's cybersecurity should be performed at least annually, with findings and any remedial action documented.

In addition, assess whether any of the following testing and control steps could be taken to address your firm's cyber risks:

- Establish a governance structure with appropriate senior management and department heads (as applicable)
- Appoint a person responsible to monitor and review cybersecurity and report to senior management
- Have overarching cybersecurity policies and procedures that contemplate and reference other applicable procedures (*i.e.*, safeguarding non-public information, identity theft, etc.) and outline reporting and corrective steps to be taken in case of an incident
- Maintain a current inventory of technology used, along with a list of personnel, independent contactors, and service providers that have access to such technology and the method(s) of accessibility
- Perform due diligence reviews at least annually on applicable service providers to confirm they have strong cybersecurity
- Ensure all firewalls, anti-virus and spyware software remain up to date
- Require strong passwords for all business hardware
- Use software that encrypts all documents being delivered via email
- Conduct penetration tests, run vulnerability scans, and consider information leak scenarios to help identify potential vulnerabilities and weaknesses
- Review contracts with service providers to ensure adequacy of security and confidentiality provisions
- Maintain adequate cybersecurity insurance
- Increase awareness and provide continual training to employees on cybersecurity
- Incorporate cyber threats as potential business disruptions in business continuity plans
- Utilize employee and service provider termination checklists
- Have detailed destruction procedures for computers and smartphones no longer in use
- Remain aware and alert to potential issues and report accordingly

Conclusion

The world of technology is ever growing and cybercrimes are keeping pace and getting more sophisticated by the day. Therefore, firms should make sure they allocate the appropriate amount of resources in both dollars and personnel to their cybersecurity programs to adequately safeguard against cybercrimes and prevent attacks.

Author: Tina Mitchell, Lead Sr. Compliance Consultant; Editor: Michelle L. Jacko, CEO, Core Compliance & Legal Services, Inc. ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues. For more information about this topic and other compliance consultation services, please contact us at (619) 278-0020, info@corecls.com or visit www.corecls.com.