MorrisonCohen LLP

Law Firm to the Middle Market®

SEC TO FOCUS ON CYBERSECURITY PRACTICES OF REGULATED ENTITIES

June 2, 2015 - "Cybersecurity" is the new watchword at the Securities and Exchange Commission, as the Commission announced in April that it would routinely examine the data security practices of registered investment companies and registered investment advisers.

The SEC said that the compliance examination would look to determine whether funds and advisers have created strategies and adopted and implemented practices designed to prevent, detect and respond to cybersecurity risks, and have periodically tested those practices to evaluate their sufficiency given the nature and scope of its particular business

What does all of this mean for funds and advisers, from a practical perspective?

Conducting the Risk Assessment

According to the SEC's guidance, each adviser and fund must regularly conduct a risk assessment in order to understand the types of informational leakage and loss risks that it is exposed to based on its operations, and thus to plan against and prevent. These include not only risks of disclosure of sensitive data to unauthorized parties, but also risks of data loss or corruption, whether through operational errors or outside infiltration, such as ransomware. While not technically a compliance issue, the reputational damage resulting from a cyber event may exceed any possible fine or recovery cost.

The risk analysis should consider:

1. The types of data collected, processed and stored (e.g., does the adviser collect and store social security numbers? Does the adviser store such information in the same databases as it stores the name and address of clients or investors, such that, in the event of a breach, an unauthorized third party can obtain sufficient information to commit identity theft?).

2. What technology is used to collect, store and protect critical or private data? (e.g., online data collection tools through its website, or only in person collection? If in person collection only, how is the paperwork from the client/investor handled once the information is input to the adviser's databases (e.g., is it shredded, and if so how and by whom)? If online only, what security means are utilized to ensure encryption of data in transit? Does the adviser use encryption only for information in transit, such as email, or also for data at rest?).

3. What technology is used to protect the sensitive data from disclosure? (e.g., Does online data collection occur only through encrypted communications? What type and level of encryption is used when transferring or storing that data? Are employees restricted from using personal email while at work? Has it disabled USB drives? Does it scan all incoming communications for viruses and malware? Does it prevent any employee from launching executable files that might contain malicious software? What controls does it have in place to ensure that when a client or investor requests a reset of online access privileges, the access is granted to the correct individual? What information is required to confirm identity (e.g., does the adviser use two-factor authentication; does the adviser require that clients/investors log into a secure website to obtain access to sensitive data about them, or can certain information be provided to a client/investor over the phone or via email)? Does the adviser accept and execute online or electronic trading instructions or only voice instructions from known individuals?).

4. On whom does the adviser rely in evaluating its risks and prevention efforts? Does the adviser employ trained cybersecurity personnel or is this an outsourced activity? Is senior management involved in the process of risk analysis, policy creation and implementation? Has the adviser evaluated the security of its network and systems by performing ethical hacks and penetration testing?

5. What procedures are in place to deal with the possibility or even the likelihood of an internal threat (e.g., a disgruntled employee who may compromise data or grant access to a third party out of spite, or in exchange for money)? Has the organization implemented any scanning or key logging software to monitor activities of its employees and consultants?

6. What training does the organization provide to its employees in an attempt to prevent unauthorized disclosures, loss or corruption of key data (e.g., do employees know that links in emails should always be suspect? Are employees trained not to give out personal information or access codes over the phone?).

7. Are employees allowed to access information systems remotely, and if so, what systems are in place to prevent system or network access by unauthorized parties (e.g., if the adviser uses a virtual private network to allow remote access, is the employee's web surfing ability restricted while connected to the adviser's systems on the same computer? Does the adviser prevent mobile devices from logging into unknown or unsecured Wi-Fi networks?).

8. What would be the impacts of a breach which resulted in unauthorized disclosure, corruption, or loss of data?

Creating a Strategy to Prevent, Detect and Respond to Threats

Once risks have been identified, the organization must develop well documented written policies and procedures to address all risks identified in the assessment. The SEC, in its auditing process, will expect strict compliance with all such policies, so the documents should not only be designed to effectively mitigate any cyber risks, but the adviser must also be able to comply with all of the requirements that it sets for itself in such policies and procedures.

As the SEC has previously recommended with respect to an adviser's compliance manual, it is important to tailor the adviser's policies and procedures to its specific strategies and structure. This tailoring effort will allow the adviser to perform a more effective risk assessment, and will also allow the adviser to prevent or mitigate the most likely risks encountered. A strong, detailed compliance program, with comprehensive input from senior management, such as the Chief Compliance Officer (and Chief Information Security Officer, if the organization employs one) as well as a commitment to a culture of compliance will also increase the likelihood of a more seamless and positive audit experience.

Implementing the Strategy

The best and most tailored assessment, coupled with an ideal set of policies and procedures, will not result in an adviser's compliance if adviser has not also developed a comprehensive set of procedures to respond to cyber incidents. Those procedures must themselves be tested periodically.

Conclusions and Recommendations

The common aphorism running through law enforcement and the information security industry is that there are two types of organizations: 1) those whose security has been compromised; and 2) those who don't know that their security has been compromised. The SEC has concluded that data loss, corruption or disclosure present fundamental risks to the safety and integrity of trading markets and to investments. Asset and investment managers are well advised to concentrate substantial executive attention to protecting their systems from cybersecurity threats as best as they can.

If you have any questions, please contact your Morrison Cohen attorney, or contact any of the following:

David Lerner
dlerner@morrisoncohen.com

Jessica Colombo
jcolombo@morrisoncohen.com

Jessica Lipson
jlipson@morrisoncohen.com