Preparing for SEC cybersecurity checks

Four critical areas asset managers need to strengthen

In the wake of high-profile attacks on several well-known retailers, the Securities and Exchange Commission (SEC) announced that cybersecurity will be a key focus of its 2014 review of asset managers. Although formal guidance and/or new regulations may be coming in the future for investment companies, investment advisors, broker-dealers, transfer agents and clearing agencies, they will all face greater scrutiny regarding the safeguards they have in place related to cybersecurity. The question these firms must ask themselves is, “Will we be ready”?
1. C-level sponsorship

Cybersecurity is everyone’s responsibility, but a top-down approach usually works best. Executive management, and the board and/or founders, must be directly involved in setting the tone at the top, reviewing and approving policies, building awareness, authorizing resources and facilitating new programs. For example, some firms have formed oversight committees of C-level executives and board members. These committees have ultimate responsibility for cybersecurity and oversee that leading practices are followed throughout the organization. For day-to-day implementation, risk management and control, many firms are appointing a single C-level executive – often the chief information officer or chief information security officer – to oversee strategy and its implementation. Most importantly, whoever is chosen for this role should have direct access to the CEO and board. This will create conditions where a cybersecurity anomaly can be identified, addressed immediately, documented and reported to the appropriate parties.

2. Employee ownership

C-level involvement is also important to engender a sense of employee ownership of information security issues, and to make sure that cybersecurity policies and procedures have been clearly communicated to all employees. Just as leading firms have developed a “compliance culture” around new mandates and expectations in the wake of the financial crisis, today’s asset managers must develop an “information security awareness culture.” Employees should be thoroughly educated about the type of threats to look for, which can be both internal and external to the organization, as well as how to respond appropriately to each incident. Security threats can include everything from hacking a CEO’s email to a breach in Human Resources data management systems, and unauthorized access to non-public property and client data. Training should be ongoing, with quarterly updates and frequent tests of employees’ ability to understand and identify potential threats.
3. Third-party oversight

Because investment advisors and funds generally outsource many of their middle- and back-office functions, it is critical to establish ongoing oversight programs. As in the retail space, service providers to financial firms can become targets of cyber criminals who are trying to reach bigger targets. Most firms do validate new vendors very carefully with regard to their cybersecurity practices, but due diligence when retaining a firm is not enough. Dealing with cyber threats is an ever-changing challenge. Just as your organization’s own systems must be continually tested, updated and refined, it is important that your service providers do the same. Keep an open line of communication with vendors, and perform regular reviews to keep your information security practices in synch in order to identify and mitigate potential vulnerabilities.

4. Cyber attack response

Firms should have a “playbook” in place that clearly spells out how to detect and respond to an attack. The playbook should also include the chain of command involved in dealing with potentially damaging incidents. Early detection is important. The question is not if your systems will be breached, but when. Many cyber attacks take months to plan, and can usually be detected with the proper safeguards in place in addition to an educated workforce. Firms should also test their entire security ecosystem for likely internal and external threats and regularly develop new scenarios for potential threats. Finally, management should be familiar with federal and state disclosure rules to determine when and to whom breaches should be communicated.

Cybersecurity represents an ongoing war – one that will continue to threaten the financial services industry and drive new regulation. There is no single answer to combatting its many threats, but one thing has become abundantly clear: the SEC has made cybersecurity a priority and will expect firms to meet a very high standard going forward. Will your firm be ready?
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace
Nearly 43,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,900 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY’s Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY’s financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2014 Ernst & Young LLP.
All Rights Reserved.

SCORE no. CK0823

1405-1256405 NY
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com