Building a better working world

October 2015

Cybersecurity – addressing rising expectations

Five critical areas asset managers need to strengthen

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly sophisticated and targeted. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, the pace of technology innovation, adoption and diversification is increasing. For many wealth and asset management organizations, technology risks and vulnerabilities are heightened through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our financial ecosystems of digitally connected entities, and people and data, increases the likelihood of exposure to cyber crime.

Security incidents continue to rise across the financial markets and other key industry sectors and will continue to be a top-of-mind item for wealth and asset managers and industry regulators as the number of high-profile attacks on companies increases. On February 3, 2015, the Securities and Exchange Commission (SEC) published its 2014 cybersecurity examination sweep summary. The results were released by the National Examination Program (NEP) of Compliance Inspections and Examinations (OCIE), which included 57 registered broker-dealers and 49 registered investment advisors. The 2014 examinations included reviews of cybersecurity documents, interviews with key personnel and testing of reported cybersecurity practices. The exam results noted that the vast majority of firms examined adopted written cybersecurity policies, conducted firmwide periodic risk assessments and used encryption in some form. Most of the examined firms had been the subject of a cyber-related incident, either directly or through the firms' vendors. Another key theme highlighted by the examination results was that vendor oversight relating to cybersecurity risk varied greatly, as did the firms' approach to assigning organizational responsibility for cybersecurity. The use of cybersecurity insurance was also found to vary greatly at the examined firms.

In April 2015, the SEC Division of Investment Management released additional cybersecurity guidance for registered investment companies and advisors, and on September 15, 2015, OCIE NEP issued a

Risk Alert highlighting its 2015 cybersecurity examination priorities. Although more detailed guidance and/or new regulations may be coming in the future for investment companies, investment advisors, broker-dealers, transfer agents and clearing agencies, all will face greater scrutiny regarding the safeguards they have in place related to cybersecurity. Organizations must ask themselves, "Will we be ready when a cyber attack occurs?"

Based on our experience working in the market and discussions with our clients, the 2014 OCIE cybersecurity exam results, the April 2015 Division of Investment Management's Cybersecurity Guidance and the September 2015 OCIE NEP Risk Alert, EY has identified five critical areas on which firms should increase their focus and that firms should be sure to incorporate into their cyber program.

C-level sponsorship

Cybersecurity is everyone's responsibility, but a top-down, cross-functional 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, investing in resources and facilitating new programs. The 2014 OCIE cybersecurity exam noted that less than 30% of advisors had a designated Chief Information Security Officer (CISO). Instead, 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 Technology Officer (CTO) — to oversee strategy and its implementation. Most important, whoever is chosen for this role should have direct access as well as regular and open communications with the CEO and board. This will help to enable an environment where a cybersecurity anomaly can be identified, addressed immediately, documented and reported to the appropriate parties. In addition, organizations should ensure that they are including information related to cybersecurity in their communications with key stakeholders.

Employee involvement and ownership

C-level involvement is also important to instill 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 regarding new mandates and expectations in the wake of the financial crisis, today's asset managers must develop an information security awareness culture. This was highlighted in the April 2015 Division of Investment Management release that directed firms to implement written policies and procedures to help facilitate awareness. Employees should be thoroughly educated about the types 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 suspicious emails sent to employees, especially employees in sensitive positions, to a breach in human resources' and financial data management systems, to advanced persistent threats and unauthorized access, to non-public intellectual property and sensitive client data. Information security awareness training should be ongoing, with quarterly updates and frequent tests of employees' ability to understand and identify potential threats. Additionally, the September 2015 OCIE Risk Alert highlighted the need for identity and access management (IAM) programs that include controlling access to systems and data through the use of multifactor authentication, user credentials and authorization methods.

Periodic risk assessment

Ongoing assessments of your cyber risk security program are key to safeguard its effectiveness to identify, prioritize and mitigate breaches or incidents. This has been highlighted as a focus area for OCIE's 2015 cybersecurity examinations. Firms should ensure that their risk assessment includes the type, sensitivity, and location of their data and systems to assess the impact of internal and external threats and vulnerabilities. This includes data classification, as well as the mechanisms to monitor how and which data is being transferred outside of an

organization, whether via employees or third parties. After key cyber risks have been identified, organizations should determine which controls and processes are in place to mitigate those risks, and determine the potential impacts of a breach in their data systems. Firms have been encouraged to utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST 800-53 framework to assist with creating their risk and control framework. Once a risk and control framework has been put into operation, firms should perform tests of operating effectiveness. This will enable the organization to confirm that controls are designed appropriately and are operating as intended. A cyber risk and control inventory should be updated at least annually.

Third-party oversight

While the 2014 OCIE exams indicated that a majority of firms examined conduct periodic cybersecurity risk assessments, only one-third of wealth and asset managers conducted periodic cybersecurity risk assessments at their vendors. Third-party oversight will continue to be a key area of focus for the 2015 OCIE cybersecurity examinations, due to a number of high-profile data breaches that occurred as the result of a breached third-party vendor platform. Since many firms generally outsource much of their middle- and back-office functions, it is important to establish ongoing third-party oversight programs that are grounded in continuous, compliance-driven reporting. As in the retail space, service providers to financial firms can become targets of cyber criminals who are trying to reach other, more lucrative targets. Most firms today validate new vendors carefully with regard to their cybersecurity practices, but initial due diligence when retaining a firm is not enough. Dealing with ongoing cyber threats is an ever-changing challenge. Just as your organization's own systems must be continually tested and monitored, updated and refined, it is important that your service providers do the same. One potential solution is to ask your vendors for attestation reports, such as a SOC 2 report, which describes their security and confidentiality protocols. In the event that your vendors do not have a SOC 2 report, ongoing vendor due diligence procedures, based on the risk posed by the vendor, can be performed through a combination of periodic on-site vendor visits, compliance-driven governance, risk and control reporting, and the use of vendor security practice questionnaires. Organizations should also request metrics and reporting from their vendors as it relates to protecting information assets. Maintaining open lines of communication with vendors, and performing regular risk-based reviews to keep your information security practices in synch, will assist a firm's ability to identify and mitigate potential vulnerabilities.

Cyber attack response

The 2014 OCIE cybersecurity examination results revealed that a majority of companies examined encountered a cyber-related incident or breach. The Division of Investment Management has highlighted the criticality of firms creating a cyber strategy that allows their organizations to protect their key digital assets. Firms should have a robust detection and monitoring program backed up by a "playbook" in place that clearly spells out how to detect, analyze and respond to cybersecurity incidents and attacks. The playbook should also include the chain of command involved in dealing with potentially damaging incidents, including report protocols. Early detection is important. The question is not whether 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. Organizations must also have robust patch management and system configuration controls in place to facilitate organizations' mechanisms to quickly protect themselves from new vulnerabilities and ensure that changes to their systems and infrastructure do not introduce unintended security vulnerabilities into the technology environment. Finally, management should be familiar with federal and state disclosure rules to determine when and to whom breaches should be communicated.

The advent of the digital world and the inherent connectivity of people, devices and organizations open up a whole new playing field of vulnerabilities. Cyber threats will continue to multiply and continue to threaten the financial services industry, driving new regulation and examination expectations. While there is no single answer to combating its many threats, two things have become abundantly clear: cybersecurity is a priority and board members, shareholders, stakeholders and regulators will expect firms to meet a very high standard going forward. Proactive measures taken now will help ease the regulatory burden and protect companies from future attack. Will your firm be ready?

Key contacts

Alan Fish
alan.fish@ey.com
+1 617 585 0796

Jaime Kahan
jaime.kahan@ey.com
+1 212 773 7755

Ralph Mittl
ralph.mittl@ey.com
+1 202 327 7188

Chip Tsantes
chip.tsantes@ey.com
+1 703 747 1309

EY | Assurance | Tax | Transactions | Advisory

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.

SCORE No. CK0977
1507-1574028 NY
ED None

ey.com