MAY 2015 SPECIAL REPRINT
NSCP CURRENTS

What the SEC's New Cybersecurity Guidance Means for Investment Advisers and Investment Companies

By Janaya Moscony, CPA; Irshad Karim; Linda Smith; Claire Owens, SEC Compliance Consultants

The ever-growing reliance on technology by all business sectors, as well as on a personal level, opens the door to various cyber threats and risks. It is important to remember that while cybersecurity is a relatively new frontier, it presents a wide range of serious issues across the board, not just in the securities world.

The Department of Homeland Security's cybersecurity overview details those issues by saying that "Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes is now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences." Additionally, the cybersecurity overview provided by the agency outlined the struggle faced when dealing with these growing threats. "Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission."[1]

As bad as the industry thinks the U.S. Securities and Exchange Commission ("SEC" or "Commission") is with regard to taking more of a reactive approach, the Commission appears to be more proactive when it comes to cyber concerns. On April 28, 2015, the Commission's Division of Investment Management released new guidance[2] ("Guidance") regarding cybersecurity for registered investment advisers and investment companies. Over the past several months, the Commission has repeatedly identified cybersecurity[3] as an important issue for funds and advisers.

In the Guidance, the Commission stated that given the rapidly changing nature of cyber threats and the increased dependence on technology in the financial services sector, they will continue to focus on cybersecurity and monitor events in this area. In addition, David Glockner, director of the Commission's Chicago Regional Office, said at the Practising Law Institute's Annual SEC Speaks[4] conference in March that "Cyber security . . . is an area where we have not brought a significant number of cases yet, but is high on our radar screen".

The Commission has, up to this point, been raising awareness of cybersecurity issues in the industry. OCIE released a Risk Alert[5] in April 2014 that set forth a detailed set of questions that advisers and broker-dealers were expected to be able to respond to during an SEC examination. The Commission then followed up with sweep exams of over 100 broker-dealers and investment advisers in 2014, and published their summary findings in a February 2015 Cybersecurity Risk Alert[6].

The Commission also recently announced plans to conduct a second phase of cybersecurity exams this summer[7]. With the publication of the new Guidance, we expect that the Commission's exams will now move from education to testing what firms have done regarding cybersecurity, and the extent to which their policies and procedures are implemented as written.

In the new Guidance, the Commission highlighted a number of specific practices and measures that funds and advisers should be considering to address their cybersecurity risks, including the following:

- *Conduct a periodic assessment* of:

  (1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;

  (2) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;

  (3) security controls and processes currently in place;

  (4) the impact should the information or technology systems become compromised; and

  (5) the effectiveness of the governance structure for the management of cybersecurity risk.

1 http://www.dhs.gov/cybersecurity-overview
2 http://www.sec.gov/investment/im-guidance-2015-02.pdf
3 http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf
4 http://www.pli.edu/Content/Seminar/The_SEC_Speaks_in_2015/_/N-4kZ1z129yu?ID=225334
5 https://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf
6 https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf
7 http://www.iawatch.com/Content/View/?id=269004

ABOUT THE AUTHORS

Janaya Moscony is President with SEC3, www.seccc.com. She can be reached at janaya@seccc.com.

Irshad Karim and **Linda Smith** are Managing Directors with SEC3. They can be reached at ikarim@seccc.com and lsmith@seccc.com respectively.

Claire Owens is Associate Consultant with SEC3. She can be reached at cowens@seccc.com

An effective assessment would assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk.

• *Have a strategy designed to prevent, detect and respond to cybersecurity threats*. Such a strategy could include:

(1) 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 to prevent cyber threats from insiders;

(2) data encryption;

(3) 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;

(4) data backup and retrieval; and

(5) the development of an incident response plan.

Routine *testing* of strategies could also enhance the effectiveness of any strategy.

• Implement the strategy through *written policies and procedures and training* that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures. Firms may also wish to educate investors and clients about how to reduce their exposure to cyber security threats concerning their accounts.

The Guidance also recommends that funds and advisers review both their internal operations and compliance programs to ensure they have in place adequate policies and procedures to mitigate exposure to any cybersecurity risks. For example, a fund or an adviser could address cybersecurity risk as it relates to:

- identity theft and data protection (e.g., Regulations S-P[8] and S-ID[9])
- fraud
- business continuity and other disruptions that could affect, for instance, a fund's ability to process shareholder transactions

Third Party Vendor Risk

The Guidance also highlights the cybersecurity risks associated with vendors and other service providers. Where funds and advisers rely on service providers in carrying on their operations, the Commission suggests assessing those service providers for adequate cybersecurity measures, especially where providers have access to a firm's technology systems and data.

Funds and advisers should also consider reviewing contracts with their service providers to determine whether the contracts sufficiently address technology issues and related responsibilities in the case of a cyber attack. Funds and advisers may also wish to consider assessing whether any insurance coverage related to cybersecurity risk is necessary or appropriate.

Given some of the practical suggestions included in the Guidance, and our understanding of how the exam staff operates, we expect the Commission will want firms to have addressed the specific items in the Guidance, with a presumption that the Guidance will be followed.

Accordingly, advisers and funds would be well advised to use the Guidance as a roadmap, and benchmark their cybersecurity preparedness against the specific items noted in the Guidance, including documenting testing, and policies and procedures

Based on the areas highlighted in the Guidance, taken together with the infrastructure and business activities we see with our typical adviser and fund clients, we believe advisers and funds should consider reviewing and taking action in several areas we outline below. Where no further action is taken, determine – and even be prepared to demonstrate -- that such items are not relevant.

Periodic Risk Assessments

Firms are advised through the IM Guidance to conduct a periodic risk assessment of their data, systems, and vendors, and identify whether there are any risks that should be mitigated. Chair Mary Jo White drove home this advice during the ICI General Membership Conference in May 2015, stating, "cybersecurity should be at the top of a firm's risk assessment."[10] The risk assessment should be conducted periodically, and updated for any changes in vendors, systems and business activities.

The Commission expects risks to be prioritized and mitigated accordingly, and therefore firms should rate/rank risks, as all risks are not created equal. Risks, in this context, relate to a firm's activities, infrastructure and systems, and are not related to the size of a firm. In fact, a smaller firm with fewer resources and more dependent on outsourcing functions may have greater risk exposure than a firm with a dedicated CISO or IT person for example.

Written Security Policy and Procedures (WISP)

Another suggestion the Guidance provided was to have a written information security policy and procedures (WISP) that outline the safeguards in place to ensure confidential data is protected (e.g., network firewalls; controlling access to more sensitive data). Having such policies and procedures in place aid in avoiding or decreasing knowledge gaps as well as educating new hires, and helping maintain institutional memory in the event of staff turnover.

These policies and procedures should include the following safeguards:

- Mapping of who has access to what data including a tiered system for more sensitive data
- Established password policies, encryption and other user authentication protocols
- Limiting the use of removable storage media which is a common vector for malware and viruses to prevent data theft and providing exceptions where warranted

The WISP should cover specific topics that commonly present cybersecurity risks. Increasingly, advisers are facing cyber risks from internal policies relating to BYOD (bring your own device); remote access to programs and or data by employees; and cloud service limitations. Accordingly, the WISP should describe the adviser's business continuity and recovery plans as well as the risks associated with identity theft or other fraud from both inside and outside actors.

8 https://www.sec.gov/rules/final/34-42974.htm
9 https://www.sec.gov/rules/final/2013/34-69359.pdf
10 http://gmm.ici.org/

Assessment of Governance and Oversight of Risks

A best practice is to update fund boards and offshore boards on cybersecurity actions as they are implemented. This is also a good opportunity to determine who bears the losses related to cybersecurity as well as if it would be beneficial for the adviser to consider cyber liability insurance coverage. Firms may also consider establishing a cybersecurity committee which would keep up with the changes in industry practices, and assist in fostering the importance of cybersecurity throughout the firm rather than working under the assumption that these risks are only an IT issue. We have seen that some firms have appointed a Chief Information Security Officer (CISO) who is an internal person that will maintain accountability, but also liaises with, and delegates specific tasks to third parties.

Testing and Monitoring of Systems and Controls

Firms should be conducting routine testing and monitoring of systems and controls (whether on a periodic or continuous basis) to ensure that they are current and incorporate the latest security patches. Common types of testing performed include penetration and intrusion testing. However, broader vulnerability testing may also be considered appropriate. Evidence of testing should be maintained and a log of unauthorized access or activity should be kept.

In the event of a cybersecurity breach or threat, firms should have in place an incident response plan, which would be created and implemented to have rapid response capability in the event of such an incident. The incident response plan might include an incident response team that designates who is responsible for which tasks. Other important factors the incident response plan should take into account are: at what point should incidents be reported to clients or counterparties; who are the relevant regulators law enforcement that should be notified; and what factors or considerations are to be weighed in deciding whether to report or not. Firms should also be cognizant of any contractual requirements to provide notice to any individual or entity.

Due Diligence of Service Providers

Appropriate due diligence should be conducted on all service providers. This is especially important if the firm is dependent on them to complete activities for the fund or the adviser. It is understood that firms will perform due diligence on their IT vendors, but is also appropriate to do so for any third parties that provide services or support to critical business activities and functions. Due diligence is best performed before entering into an engagement with a third party service provider, but also would be done on an ongoing periodic basis to ensure any changes are captured and understood. Many advisers have adopted a policy to provide a due diligence questionnaire to service providers to confirm security reviews and reports (e.g. SOC 2 or other SSAE 16 reports).

Questions that advisers might ask of providers during the due diligence process include:

- Does the service provider maintain cyber liability insurance coverage? If yes, does it cover third parties for losses (such as funds and advisers)?
- Who is responsible for any losses?;
- What is the standard of liability (and are there any carveouts?); and
- Are sub-contractors permitted? If so, firms should consider pass through of contractual requirements, or consent to use of sub-contractors

In conjunction with the above-mentioned questions, advisers should also consider limiting access of third party service providers to just the functions and areas necessary to provide services to the firm. Firms should also make sure they have the right to conduct an audit of their service providers at any time.

Assess the Need for Cyber Liability Insurance

Advisers should be aware that standard insurance policies (e.g., E&O, D&O) may not cover cyber related losses, and therefore might consider the value of cyber liability insurance in addition to their current insurance policies. Currently, however, most cyber insurance policies are geared towards consumer oriented businesses and consumer data breaches. These types of policies may have to be tailored to many advisers with more institutional clients to make them an effective protection for such advisers.

It is important to note that the results from the February 2015 Cybersecurity Risk Alert[11] indicated few investment advisers actually carried cyber insurance (only 21% of the advisers maintained insurance for cybersecurity incidents), but given that a majority of broker-dealers did carry such insurance, advisers may want to show that they at least considered or evaluated cyber insurance even if they choose not to carry it.

Training

The weak link in cybersecurity tends to be human error; so effective firm-wide training is critical. Once an adequate policy is in place, the next step is to ensure personnel understand the firm's risks and know their responsibilities associated with protecting the firm and client data. Training on this topic should be conducted as least annually, and upon hiring of new personnel or consultants. The Guidance also proposed that advisers consider educating investors and clients about how to reduce cybersecurity threats to their accounts.

Conclusion

Because funds and advisers are varied in their operations, the Commission expects funds and advisers to tailor their cyber security programs based on the nature and scope of their businesses. The Guidance suggests that funds and advisers will be better prepared if they consider the measures discussed based on their particular circumstances when planning to address cybersecurity and a rapid response capability.

The Commission stated it recognizes that is it not possible for a fund or adviser to anticipate and prevent every cyber attack, but that the Commission expects funds and advisers to have a plan that addresses cybersecurity risks, and in the event of an incident, to have controls in place to mitigate the risks.

It is possible that a failure by an adviser or a fund to have sufficiently addressed cybersecurity risks consistent with the Guidance could lead to SEC deficiency findings or an enforcement action, even in the absence of a cyber attack or other incident. A failure to address the Guidance could also result in potential exposure to private litigation.

In short, the Commission has raised the bar for advisers and funds in the area of cybersecurity preparedness and provided a clear roadmap: benchmark practices and processes against those described in the Guidance; tailor those practices and processes where appropriate for your business; continue to monitor your systems and processes and ensure they are up to date; and train your personnel and clients on the risks involved. ✦

11 https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf