New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication

Cybersecurity and Privacy

WWW.NYLJ.COM
MONDAY, MARCH 7, 2016

Hone a Plan to Meet Evolving Regulatory Expectations

BIGSTOCK

BY DAVID L. HALL, JOHN B. KENNEDY AND CONOR L. MULLAN

DAVID L. HALL *is a partner in Wiggin and Dana's litigation department,* JOHN B. KENNEDY *is a partner in the corporate department and* CONOR L. MULLAN *is counsel in both the corporate and litigation departments.*

For several years, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) has been gathering information and issuing instructive guidance to investment advisers for protecting against cybersecurity intrusions. But with the announcement of its second round of cybersecurity examinations in September 2015—as well as a recently settled enforcement action against an investment adviser based upon a failure to adopt cybersecurity policies and procedures—the SEC crossed the Rubicon. It is now clear that the SEC expects that investment advisers have implemented comprehensive cybersecurity policies, procedures and practices. In fact, one of the key takeaways from OCIE's most recent guidance is that OCIE will be testing firms' policies and procedures, as opposed to limiting the scope of the examinations to surveying, as seen during its first round of examinations. As a result, investment advisers must take great care in drafting and evaluating their cybersecurity program, while evolving to meet ever-changing regulatory expectations.

Cybersecurity Rules and Regulations

Before compliance and legal personnel create cybersecurity policies and procedures, they should understand the standards that need to be met. For investment advisers, however, these standards come from several sources. One primary

source is Rule 30 of Regulation S-P, which requires SEC-regulated firms to establish written policies and procedures designed to "(a) Insure the security and confidentiality of customer records and information; (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[1]

Regulation S-ID is another source of cybersecurity regulation for certain investment advisers. Reg S-ID requires, among other things, that certain SEC-regulated firms that provide services to "consumers" implement identity theft policies and procedures designed to: (1) identify relevant types of red flags; (2) detect the occurrence of red flags; (3) respond appropriately to red flags; and (4) periodically update the identity theft program.[2] Additionally, Rule 206(4)-7 under the Investment Advisers Act of 1940, as amended (the Advisers Act), requires registered investment advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and its rules, including Regulation S-P and Regulation S-ID.[3]

Investment advisers that are not technically subject to Reg S-P or Reg S-ID, such as investment advisers that only provide services to institutional clients (or any other type of client that falls outside of the definition of "consumer" under Reg S-P or Reg S-ID), still owe a fiduciary obligation to clients under the Advisers Act to safeguard confidential information. Moreover, most institutional clients and third parties (e.g., wrap sponsors, fund administrators) impose contractual obligations that meet or exceed the data security and related requirements imposed under Reg S-P.

Lastly, neither Reg SP nor Reg S-ID preempt state data protection laws, some of which are fairly comprehensive (See, e.g., Massachusetts Data Security Regulations).[4]

Recent OCIE Cybersecurity Guidance

In April 2014, OCIE launched a cybersecurity sweep, which examined investment advisers and broker-dealers picked to represent a wide cross-section of the U.S. financial services industry.[5] On Feb. 3, 2015, OCIE released the result of the sweep in a risk alert (the First Risk Alert), which provides a detailed overview of how investment advisers and broker-dealers are addressing the legal, regulatory and compliance issues associated with the increasing risk from cyber attacks.[6] Finally, on Sept. 15, 2015, OCIE issued another risk alert (the Second Risk Alert) announcing a second round of examinations under its cybersecurity examination initiative.[7] The Second Risk Alert also included information on areas of focus for OCIE's cybersecurity examinations. The guidance set forth in these three documents, as well as guidance put out by the SEC's Division of Investment Management,[8] should be the cornerstone of any cybersecurity compliance program.

Points to Remember

At this stage, most investment advisers have some form of cybersecurity, information security or data protection policies and procedures in place. Often, cybersecurity is covered through a firm's privacy, business continuity, or electronic communications policies and procedures, but it doesn't have to be. There is no one-size-fits-all approach to cybersecurity. Instead, the focus should be on the substance—rather than the form—of a firm's entire body of policies, procedures and practices. With that in mind, below are six practice points to consider:

Stand-Alone Cybersecurity Policies and Procedures Are Not Always the Solution. As noted above, one commonly misunderstood aspect about cybersecurity compliance is that it is a novel compliance area. It's not—cybersecurity and data protection issues are generally just the digitized version of risks that have always been present. For this reason, after conducting an initial risk assessment and gap analysis, a firm may ultimately decide that its existing information security, privacy, business continuity, email, social media, and other policies and procedures, adequately manage risk and meet regulatory expectations. In this case, a new stand-alone set of cybersecurity policies and procedures may not be necessary. On the other hand, a firm might find that its optimal solution is a master cybersecurity policy that carefully incorporates and cross references other existing firm compliance policies and procedures and other firm documents (e.g., employee handbook). One common mistake to be avoided is to create cybersecurity-specific policies and procedures that conflict with other sections of a compliance manual. These inconsistencies can create unnecessary confusion among employees and are low-hanging fruit for examiners.

Cybersecurity Risk Management Standards. Without question, preventing data security breaches is a primary objective in drafting cybersecurity policies and procedures. However, even firms with sound cybersecurity practices can be breached. Accordingly, a second but equally important objective should be adopting policies and procedures that minimize regulatory risk in the event of a breach. This can be accomplished by ensuring that a firm's overall cybersecurity program is objectively reasonable and consistent with industry standards. And OCIE's Risk Alert strongly suggests that "reasonable security measures" are built through the use of published standards, such as the

Framework for Improving Critical Infrastructure Cybersecurity (the Framework), released in February 2014 by the National Institute of Standards and Technology (NIST), a component of the U.S. Department of Commerce.[9] The Framework is, by design, a set of guiding principles and general practices. Specifically, it is intended to "enable[] organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."

Investment advisers and their compliance and legal teams (as well as outside counsel) are sometimes tempted to ignore the Framework, since it is only a collection of best practices from a multitude of sources. The lack of specific, proscribed solutions (such as minimum encryption standards and firewalls specs) as well as the lack of financial services industry-specific guidance often frustrates compliance personnel who, by nature, seek precision and clear solutions. Nonetheless, at a minimum, the five core functional categories of the Framework (identify, protect, detect, respond, and recover) should be utilized by firms of any size or level of cyber complexity as an *initial* step for setting up both the risk assessment process and policies and procedures.

Firms should also examine whether the corresponding subcategories and suggested cybersecurity practices for these core functions provided in the Framework are appropriate for their own cyber risk profiles. Remember that the Framework is an essential first step in the direction of establishing "reasonable security measures," but it does not contain financial services industry-specific guidance. Furthermore, it does not define a safe harbor, and was not designed to.

Multiple Uses of the Risk Assessment. A cybersecurity risk assessment is recommended (if not required) by OCIE and, according to OCIE's findings, 79 percent of advisers are performing some form of cybersecurity risk assessment and utilizing the results in forming policies and procedures. Conducting initial and ongoing assessments is therefore strongly advised.[10] But one of the most valuable and often overlooked aspects of a risk assessment is its role in communicating vulnerabilities to officers and executives (and board members, if applicable) who might not otherwise have a sufficient understanding of cybersecurity risks. It is also a way of evaluating and measuring the work performed by a firm's IT department, which is often difficult to understand from a high-level due to the complexity of a firm's cyber structure. The cybersecurity risk assessment can also be used as a means for generating buy-in from the top of an organization. For this reason, it is important that the risk assessment be written for a broader audience than IT and compliance personnel. And of course, the risk assessment should be handled and distributed with care because it might reveal critical information about the firm's weaknesses.

Before compliance and legal personnel create cybersecurity policies and procedures, they should **understand the standards that need to be met.**

Employee Training. Compliance and legal departments are often under tremendous time pressure to develop new policies and procedures to address new applications being used by the firm or to satisfy client and third-party due diligence inquiries. As a result, sometimes employee education on these new or revised policies and procedures is delayed or overlooked. Although delaying or overlooking training on any new policies and procedures is problematic, the problem is more acute in this area because so many different employees within an organization are responsible for handling and transmitting sensitive data on a daily basis. Stated another way, almost every employee needs to have a basic grasp of information security, whereas only select departments may need to be educated on other compliance areas (e.g., the trading department on trade allocation procedures, the marketing department on advertising procedures, and so on). Indeed, OCIE's risk alert indicates that many of the losses associated with fraudulent emails arose from employees' failure to properly follow basic identity authentication procedures.

In addition to going over specific changes to policies and procedures, cybersecurity training should be used as an opportunity to give firm IT personnel the opportunity to explain the firm's most current security risks and recap its collective experience with common scenarios, such as phishing scams and other fraudulent uses of email. This information is invaluable for protecting firm and client data, but is too infrequently communicated to employees outside of a group setting. This training should also cover employee issues highlighted in OCIE Guidance (i.e., misplaced storage devices, using unsecured Internet connections, downloading attachments from unknown sources), as well as the types of cases that the SEC's Division of Enforcement is focusing on: (1) failures in safeguarding information; (2) theft of material non-public information for purposes of fraudulent insider trading; and (3) incident disclosures (in the context of public companies).[11]

Difficulty Executing Vendor Management. OCIE's Guidance highlights third-party vendor risk as one of the top cybersecurity concerns. Specifically, OCIE noted that examiners may focus on firm practices and controls relating to vendors, such as due diligence with regard to vendor selection, monitoring and oversight

of vendors, and contract terms. Often, however, advisers find themselves without leverage to either (a) negotiate or add the particular cybersecurity representations and provisions to a vendor contract, or (b) persuade a vendor to complete initial and/or ongoing due diligence questionnaires. Generally, the best approach when faced with a non-cooperative vendor is to seek alternatives. Vendors of data and IT services to the financial services industry who wish to remain competitive will need to respond to increasing regulatory scrutiny and risk sensitivity of their client base. However, where alternative vendors are not feasible or desirable, an adviser may look to employ other forms of due diligence, such as requesting: (a) SSAE16 and other third-party reports (which should already be requested under a reasonably designed DDQ); (b) references that you may contact to gain comfort with the vendor's information security practices, as well as confirmation of the vendor's compliance with industry-recognized certifications and standards for information security; and (c) standard disclosures that the vendor provides to other customers.

Cyber Insurance. Insurance can be utilized to reduce the economic consequences of cybersecurity incidents to a firm. OCIE's risk alert notes that the majority (58 percent) of broker-dealers maintain such insurance, while only a small percentage of advisers (21 percent) do. It is important to understand that, while cybersecurity is not a new concept, cyber insurance is a relatively new form of insurance. As a result, the cyber insurance products are not as standard as other forms of business coverage offered by insurance companies. Accordingly, the scope of coverage can vary widely by policy and carrier, and should be carefully evaluated to ensure the appropriate coverage for risk.

Cyber insurance, which can be sold as a separate policy or as a rider to an existing policy, is intended to cover certain costs arising from data breaches that are typically not covered by other types of business policies. Thus, the first step in assessing whether a firm needs a cybersecurity policy is to determine the scope of a firm's present insurance coverage and any potential gaps in coverage related to cybersecurity issues, as well as the potential economic consequences of various cybersecurity issues. The most basic cybersecurity policies are intended to reimburse the following types of costs: (1) the costs of a forensic investigation to determine which data was accessed in a breach and who should be notified; (2) notification and credit monitoring services for affected clients; (3) litigation costs arising from the data breach; and (4) public relations costs arising from the breach. More comprehensive cyber insurance policies are becoming available. These policies may offer coverage not only for data breaches by hackers, but also for other types of costs associated with cyber attacks, such as:

- Data theft by employees;
- Business interruption costs if a website or business is affected by malware or technology issues;
- Costs associated with restoring, updating or replacing business assets stored electronically and damaged or lost;
- Costs arising from cyber terrorism or cyber extortion;
- Damages to third parties caused by negligent transference of malware;
- Costs associated with regulatory compliance or investigation; and
- Content liability for websites, including copyright/trademark infringement.

Potential purchasers should also evaluate whether coverage extends to cloud-based storage systems, vendors and foreign affiliates or subsidiaries. It should also be noted that when issuing cyber insurance policies, insurers focus on risk management. Accordingly, obtaining comprehensive coverage at the best price usually requires a firm to have a cybersecurity plan in place, which includes management involvement and up-to-date intrusion protection measures, as well as disaster recovery plans.

Conclusion

Cybersecurity is one of the top priorities for the SEC, and SEC guidance in this area is still developing to keep up with the fast and evolving pace of cybersecurity threats. As a result, investment advisers should take the long view in designing cybersecurity programs that are both comprehensive yet flexible enough to stay up-to-date on what reasonable and unreasonable cybersecurity practices look like in the eyes of the SEC.

1. 17 C.F.R. § 248.30(a).
2. See Identity Theft Red Flags Rules, 78 FR 23628 (April 19, 2013) (the Adopting Release) available at: https://www.sec.gov/rules/final/2013/34-69359.pdf.
3. 17 C.F.R. 275.206(4)-7.
4. 201 Mass. Code Regs. §17.00.
5. https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert–Appendix—4.15.14.pdf.
6. http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
7. https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
8. Additionally, on April 28, 2015, the SEC's Division of Investment Management released additional cybersecurity guidance for investment companies and investment advisers, available at http://www.sec.gov/investment/im-guidance-2015-02.pdf.
9. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
10. As set forth in the First Risk Alert, that assessment should entail forming a complete understanding of the cyber infrastructure and mapping assets, including physical devices, software, applications, network resources, connections and data flow.
11. "SEC Speaks," Stephanie Avakian, Deputy Director of the SEC's Division of Enforcement, Feb. 19, 2016.

Originally appeared in print as Investment Advisers: Hone a Plan to Meet Evolving Regulatory Expectations