Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Problems With SEC's Cybersecurity Approach

Law360, New York (September 30, 2015, 10:35 AM ET) --

Brian Rubin

You leave your home and lock the door. Your new 88-inch curved HDTV is visible from your front lawn. You come home later that evening. The door is slightly open. The lock is broken. You go inside and see that the drawers and cabinets have been ransacked. You determine that nothing is missing. You call the police department to report that someone has broken into your house. When the police officer arrives, you answer all questions and offer information to try to help the police find the bad guy. The police thank you for your help but give you a ticket because you failed to turn on your alarm system.

You park your car. You lock the door with your remote control key. Your new iPad Pro is sitting on your dashboard. You come back several hours later and find your windows are broken. You look inside the car. Your seats have been cut open. You open the door, look inside, and discover that nothing is missing and the iPad hasn't been moved. You call the police. A different officer comes to assist you. You tell the officer you saw two youths running from your car. The police officer gives you a ticket because when you purchased your car, you didn't pay $2,000 for the anti-theft car alarm system.

The Cyber Victim: An Investment Adviser

The U.S. Securities and Exchange Commission recently brought an enforcement action against an investment adviser that, like a large number of companies, was the victim of a cyberattack, under circumstances somewhat similar to the scenarios described above.[1] The investment adviser stored sensitive personally identifiable information (PII) of its clients and other persons on its third-party-hosted Web server. An unauthorized, unknown intruder "attacked" the firm's Web server and "gained access rights and copy rights" to the PII of more than 100,000 individuals, including thousands of the investment adviser's clients. While the data was "vulnerable to theft," the SEC's settlement order did not allege that the intruder used the data. Thus, there was a breach but no proof that anything was "taken" or used by the hacker. Indeed, according to the SEC, "[t]o date [more than two years later], the firm has not learned of any information indicating that a client has suffered any financial harm as a result of the cyber attack." Thus, this case stands in stark contrast to other SEC enforcement actions where data was actually accessed and used. See, e.g., Admin. Proc. (Sept. 29, 2009), https://www.sec.gov/litigation/admin/2009/34-60733.pdf (unauthorized person accessed accounts and entered unauthorized purchases); Admin. Proc. 3-13181 (Sept. 11, 2008), https://www.sec.gov/litigation/admin/2008/34-58515.pdf (hacker had access to customer information

customers and attempted to place unauthorized trades in customer accounts).

The Firm's Extraordinary Remedial Conduct

After the breach, the firm took the following extraordinary steps for which the SEC gave it some credit (although not enough, considering that the investment adviser was formally charged):

- Upon discovery of "a potential cybersecurity breach," the investment adviser "promptly" retained more than one cybersecurity consulting firm to confirm the attack and assess the scope of the breach.

- After those consulting firms "could not determine the full nature or extent of the breach," the investment adviser "soon" afterwards retained another cybersecurity firm to review the initial findings and "independently assess the scope of the breach."

- Shortly after the breach, the IA provided notice of the breach to "all of the individuals whose PII *may* have been compromised" (emphasis added) and offered them free identity monitoring through a third-party provider.

According to the order, the firm also took the following "remedial efforts" to "mitigate against any future risk of cyber threats":

- Appointed an information security manager to oversee data security and protection of PII;
- Adopted and implemented a written information security policy;
- Stopped storing PII on its Web server;
- Encrypted any PII stored on its internal network;
- Installed a new firewall and logging system to prevent and detect malicious incursions; and
- Retained a cybersecurity firm to provide ongoing reports and advice on the firm's information technology security.

The SEC's Response: An Enforcement Proceeding

So, what did the SEC staff do? Did they say, "We are sorry you were a victim of a cybersecurity attack"? Did they say, "Good job, investment adviser. You responded to the breach quickly, you retained experts to find out what happened, you contacted all of the individuals who 'may' have been affected, despite finding no evidence that any data was taken and used, and, just in case, you provided free monitoring"? No. Instead, the SEC "considered the remedial acts promptly undertaken by [the firm] and the cooperation [the firm] afforded the Commission staff," and brought an administrative cease-and-desist action, censured the firm, and ordered it to pay a civil money penalty of $75,000.

The SEC's charges relate to the "reasonableness" of the firm's policies and procedures for safeguarding customer information. Often, when the SEC finds that a firm doesn't have reasonable policies and procedures, it tells the firm to cure the deficiency. Here, instead, the SEC sanctioned the firm for its

allegedly unreasonable policies and procedures. As shown below, however, while the SEC charged the firm with failing to implement certain specific policies and procedures, the SEC's rules and regulations do not mandate these "best practices," and the SEC has never issued guidance advising firms that they should institute those practices. (Indeed, the SEC order ignored countless other "best practices" that were arguably relevant to this breach.) As discussed below, the SEC chose to provide guidance by punishing the victim, rather than issuing a regulatory notice or adopting new rules.

The SEC rule at issue is Rule 30(a) of Regulation S-P,[2] which requires registered investment advisers (and other regulated entities) to adopt written policies and procedures that are reasonably designed to safeguard customer records and information. Thus, the standard is "reasonableness." As such, in its order against the investment adviser, the SEC alleged the following violation:

The firm failed to "adopt written policies and procedures reasonably designed to protect customer records and information," in violation of Rule 30(a).

In this case, the SEC did not charge the firm for not having any policies and procedures. The SEC has, of course, previously sanctioned other firms for such failures. See, e.g., Admin. Proc. File No. 3-15616 (Nov. 19, 2013), https://www.sec.gov/litigation/admin/2013/ia-3719.pdf (firm failed to have written procedures "concerning three important areas of private fund management: (i) valuation of fund assets, (ii) the accuracy of disclosures to fund investors about the valuation practice, and (iii) cross trades between clients"); Admin. Proc. File No. 3-14644 (Nov. 28, 2011), https://www.sec.gov/litigation/admin/2011/ia-3324.pdf (firm failed to have any written compliance program and failed to have a written code of ethics). (If the SEC does decide to sanction firms for not having any policies and procedures, it appears that many firms could be charged. According to the SEC's February 2015 National Exam Program Risk Alert Cybersecurity Examination Sweep Summary, 17 percent of advisers examined did not adopt written information security policies.[3])

Implicit in this charge is that if the investment adviser had better policies and procedures, then the breach would not have occurred. However, the order is problematic because it does not allege any facts to establish this proposition (other than to state that a breach occurred). The order suggests that a breach, in and of itself, is prima facie evidence that a firm's procedures were not reasonable. This strict liability standard and post hoc rationale eliminates the need to establish any causal relationship between the alleged procedural inadequacies and the breach.

The order then provides specific "examples" of policies and procedures that the firm did not have. These are simply a list of certain "best practices," which are not mandated by Rule 30(a). The following are the SEC's "example[s]" of the types of policies and procedures that the investment adviser did not have in place "for protecting its clients' information":

- Conducting periodic risk assessments;
- Employing a firewall to protect the Web server containing client PII;
- Encrypting client PII stored on that server; and
- Establishing procedures for responding to a cybersecurity incident.

The SEC could have easily listed dozens of other relevant "best practices," such as timely application of security patches; testing and validation of software updates on a test server before installation onto a production server; requiring dual-factor authentication to access administrative functions on the server; choosing strong passwords; implementing intrusion detection software; implementing data exfiltration

monitoring and prevention software; keeping detailed logs of security-related events; and periodically reviewing those logs. It is unclear why the order listed certain practices but ignored others.

There are several problems with the SEC's approach. First, the SEC failed to allege facts establishing that any of these "examples" (or best practices) was reasonably required under the circumstances. For example, is it reasonable or required that all firms conduct periodic risk assessments or only some firms? If the former, what frequency is always reasonable? If the latter, what facts made periodic risk assessments reasonable in these circumstances?

Second, the order failed to allege that lack of these best practices led to the breach. For example, did the SEC have evidence (not alleged in the order) that periodic risk assessments would have prevented the breaches? In contrast, where other firms have been charged with not having reasonable policies and procedures, those policies and procedures often directly relate to the "bad" conduct that the policies should have prevented. For example, in one enforcement action, the SEC's order stated that the firm's failure to adopt and implement written compliance policies and procedures reasonably designed to prevent violations of the Investment Advisers Act of 1940 "resulted in" the firm's "engaging in hundreds of principal transactions with its advisory clients' accounts without making the proper disclosures and obtaining consent in violation of Section 206(3) of the Advisers Act."[4] The order here did not contain a similar finding.

Third, by providing its list of examples in the order, the SEC appears to be turning these "best practices" into rule requirements without the benefit of formal notice-and-comment rule-making. The U.S. Court of Appeals for the D.C. Circuit in KPMG LLP v. SEC, 289 F.3d 109, 116 (D.C. Cir. 2002), acknowledged that the SEC "may broadly construe its rules" but the SEC may not interpret its rules such that a regulated entity is penalized when it has not "received fair notice of a regulatory violation." For example, the SEC in William R. Carter and Charles J. Johnson Jr., 47 S.E.C. 471, 508 (1981), declined to find "improper professional conduct" by two attorneys because the applicable standards "ha[d] not been so firmly and unambiguously established that we believe all practicing lawyers can be held to an awareness of generally recognized norms" and because "the Commission ha[d] never articulated or endorsed any such standards."[5] Here, there was no prior notice from the SEC that the listed best practices were required to be instituted.

Finally, by identifying some "best practices" but not others (and without identifying any reasons for selecting the cited best practices), the SEC's order could have an unintended effect. It is possible that by listing certain best practices and ignoring others, firms will interpret the SEC's order as not requiring them to institute the "others." This interpretation may be particularly true for firms with limited resources.

Alternatives to an Enforcement Action

Rather than bringing an enforcement action, the SEC had three tools at its disposal. First, the staff could have provided regulatory guidance, such as staff legal bulletins.[6] While the SEC did issue a "Cybersecurity Examination Sweep Summary" in February 2015, its precedential value is questionable because the report stated that it was providing "summary observations from the examinations conducted under the Cybersecurity Examination Initiative," but it did not suggest that any practice discussed was a requirement. (It is worth noting that most of the investment advisers examined apparently did not met the requirements set forth in the order regarding third-party-hosted Web servers. Will the SEC be charging the 68 percent of advisers that do not require cybersecurity risk assessments of vendors with access to their firms' networks?).

The SEC's risk alerts on cybersecurity are not particularly helpful and, in fact, suggest that the SEC was examining firms to establish guidance. The April 2014 National Exam Program Risk Alert titled, "[Office of Compliance Inspections and Examinations (OCIE)] Cybersecurity Initiative," simply announced that OCIE would conduct examinations to "help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats."[7] Similarly, the September 2015 risk alert on OCIE's 2015 Cybersecurity Examination Initiative provided "additional information on the areas of focus for OCIE's second round of cybersecurity examinations." The initiative was "to promote better compliance practices and inform the Commission's understanding of cybersecurity preparedness." These two alerts suggest that, instead of enforcement actions, the SEC would use OCIE's findings to determine what type of guidance to issue to the industry. Consistent with that approach, the SEC could issue comprehensive guidance regarding what it expects firms to do just like the federal banking regulators have done.[8]

Second, the SEC could have issued a report of Investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934, which the commission uses to explain its view about particular practices. It would make sense for the SEC to file such a report in this area. A report could articulate the practices the SEC believes are relevant in determining whether written policies and procedures are reasonably designed to protect customer records and information, without subjecting a firm — which has been a victim of a breach — to an enforcement action.

Finally, the staff could have recommended that the SEC engage in formal rule-making. Notably, when it has engaged in this conduct in the past, consistent with the notice-and-comment obligations discussed above, the SEC provided regulated entities time between the announcement of the rule and its effective date to comply with the new obligations.[9] In the enforcement action against the IA, in contrast, the firm was charged for conduct from September 2009 through July 2013, even though the SEC did not start its cybersecurity initiative until July 2014 and did not summarize its findings until September 2015.

Implications for Firms

Regardless of whether the SEC had an adequate factual or legal basis to bring its action or whether, as a matter of policy and fairness, it should have charged the investment adviser, the SEC's order cannot be ignored. At this point, investment advisers (and probably broker-dealers) may be facing strict liability if they become the victim of a breach. It appears that the SEC may find that a firm's procedures were unreasonable based on the simple fact that a breach occurred. To try to prevent a breach from occurring and to protect the interests of their clients (as well to prevent the initiation of a subsequent enforcement action), firms may want to review the various statements and reports by the commission and its staff (as well as those of the Financial Industry Regulatory Authority[10]) to determine what is reasonable for their business model to protect customer records and information. In addition, to combat rule-making by enforcement, firms may want to consider defending themselves in litigation against the SEC. As explained above, others have successfully challenged regulatory overreach.

—By Brian Rubin and Charlie Kruly, Sutherland Asbill & Brennan LLP

Brian Rubin is the Washington, D.C., office leader of Sutherland's litigation group and the administrative partner in charge of the firm's securities enforcement and litigation team. He is a former deputy chief counsel of enforcement at the National Association Of Securities Dealers (now FINRA) and a former senior enforcement counsel at the SEC.

Charlie Kruly is an associate in the firm's Washington office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Admin. Proc. No. 3-16827 (Sept. 22, 2015), https://www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[2] 17 C.F.R. § 248.30(a).

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

[4] Admin. Proc. No. 3-14645, (Nov. 28, 2011), https://www.sec.gov/litigation/admin/2011/34-65838.pdf.

[5] Cf. Checkosky v. SEC, 139 F.3d 221, 225-26 (D.C. Cir. 1998) (government cannot deprive citizens of the opportunity to practice their profession without revealing the standard they have been found to be violating).

[6] See, e.g., Staff Legal Bulletin No. 20 (June 30, 2014) (addressing the availability of exemptions to the federal proxy rules for advisory firms), https://www.sec.gov/interps/legal/cfslb20.htm); Staff Legal Bulletin No. 18 (Mar. 15, 2010) (addressing the use of Exchange Act Rule 12h-3 to suspend reporting obligations under Section 15(d) of the Exchange Act), https://www.sec.gov/interps/legal/cfslb18.htm.

[7] National Exam Program Risk Alert, OCIE Launching Cybersecurity Preparedness Initiative (April 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

[8] See, e.g., 12 C.F.R. Pt. 30, App. B (Office of the Comptroller of the Currency) (requiring, among other things, the use of risk assessments and incident response plans and "consider[ation]" of whether encryption is "appropriate" for a particular firm); 12 C.F.R. Pt. 255 App. F (Federal Reserve Board); 12 C.F.R. Pt. 364 App. B (Federal Deposit Insurance Corp.). Notably, the federal banking regulators' guidance interprets the same statute that provides the basis for the SEC's Reg. S-P.

[9] See, e.g., Final Rule: Privacy of Consumer Financial Information (Regulation S-P), SEC Release IA-1883 17 C.F.R. 248 (June 22, 2000) (effective date of 17 CFR Parts 248 November 13, 2000, nearly five months after publication of final rule); Final Rule: Rules Implementing Amendments to the Investment Advisers Act of 1940, SEC Release IA-3221 (June 22, 2011) (effective date of 17 CFR Parts 275 and 279 September 19, 2011, nearly three months after publication of the final rule, with later "compliance dates" for certain requirements of the new rule).

[10] See, e.g., FINRA's Report on Cybersecurity Practices (Feb. 2015), https://www.finra.org/newsroom/2015/finra-issues-report-cybersecurity-practices-cybersecurity-investor-alert.

All Content © 2003-2015, Portfolio Media, Inc.