Bloomberg BNA

Securities Regulation & Law Report™

Reproduced with permission from Securities Regulation & Law Report, 47 SRLR 2241, 11/23/15. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

CYBERSECURITY

Upping the Ante: Cybersecurity, the SEC and the Perils of Being Unprepared

BY CRAIG A. NEWMAN

The U.S. Securities and Exchange Commission is finally getting serious about cybersecurity – and for good reason. If the ever-growing business and headline risks aren't enough to scare investment advisers and broker-dealers into action, they now have added motivation to make cybersecurity a top priority – impending regulatory examinations and enforcement proceedings.

Cybersecurity has been on the SEC's radar for the past few years but only recently has the agency intensified its scrutiny of firms' data security and governance protocols. And, in a series of bold public statements, the SEC is even promising to hold chief compliance officers accountable if they look the other way when it comes to implementing meaningful cybersecurity plans – including incident response protocols – to guard against and remediate when cybercriminals and hackers burst through a firm's firewalls even when it's the fault of a hapless employee or outside vendor.

It's no surprise that the SEC is clamping down. Cyber-attacks on major financial institutions, broker-dealers and even hedge funds are already yesterday's news. Indeed, the SEC's own cybersecurity sweep exam conducted in 2013-2014 revealed that, of the more than 100 firms examined, 88% of the broker-dealers and 74% of the investment advisers had experienced a cyber-attack, either directly or through a third-party vendor. These statistics don't bode well for the future. (http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf)

And just two months ago, the SEC threw down the proverbial gauntlet. In September 2015, the SEC's Office of Compliance Inspections and Examination issued a Risk Alert announcing a new cybersecurity examination initiative. The initiative provides the Commission's regulatory expectations for this round of examinations of broker-dealers and investment advisers. The SEC's expectations are, to be sure, not ''check the box'' compliance measures but a series of significant steps toward creating a broad platform of cybersecurity compliance that touches upon key areas of a firm's business operations. Aside from identifying specific areas of focus for regulated firms including governance and risk assessment, IT and network access rights and controls, data loss prevention, third-party vendor management and safeguards, training and incident response, the five-page, single-spaced appendix to the Risk Alert sets forth a detailed list of information requests firms can expect to face from SEC examiners ''that should not be considered inclusive.'' (http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf)

On top of all this, recent public statements by senior SEC officials make it clear that the agency won't tolerate a ball drop when it comes to these new measures. In a speech in October, SEC Chief of Staff Andrew J. Donohue set off alarm bells when he said that the Commission ''has brought, and will continue to bring, enforcement actions against compliance officers when appropriate.'' Donohue challenged chief compliance officers (CCOs) to be ''proactive'' in their work and noted three recent SEC enforcement actions against CCOs on the grounds that they did not implement programs that were reasonably tailored to the needs of their firms. ''We don't bring cases based on second guessing compliance officers' good faith judgments, but rather when their actions or inactions cross a clear line that deserve

Craig A. Newman is a partner with Patterson Belknap Webb & Tyler LLP, and chair of the firm's Privacy and Data Security practice group.

sanction,'' he said in his comments. (http://www.sec.gov/news/speech/donohue-nrs-30th-annual.htm)

Two days later, SEC Chair Mary Jo White announced that ''[w]hile cybersecurity attacks cannot be entirely eliminated, it is incumbent upon private fund advisers to employ robust, state-of-the-art plans to prevent, detect, and respond to such intrusions.'' (http://www.sec.gov/news/speech/donohue-nrs-30th-annual.html)

But on November 4th, SEC Enforcement Director Andrew Ceresney, in a speech to the National Society of Compliance Professionals, sought to calm the waters and clarify the circumstances in which CCOs would find themselves in the agency's cross-hairs, emphasizing that ''[w]e look hard at the facts and fairness concerns in each case. The overwhelming majority of cases we bring involve CCOs who crossed a clear line by engaging in affirmative misconduct or obstructing regulators, or who wore multiple hats.'' (http://www.mondovisione.com/media-and-resources/news/2015-national-society-of-compliance-professionals-national-conference-keynot/)

The SEC's remarks come in the aftermath of the agency's first cybersecurity enforcement action – a largely symbolic shot across the bow – against R.T. Jones Capital Equities Management, Inc., a small St. Louis-based registered investment adviser, for failing to establish cybersecurity policies and procedures in advance of a breach that compromised personally identifiable information (PII) including social security numbers for 100,000 individuals. (https://www.sec.gov/litigation/admin/2015/ia-4204.pdf) The facts in this case are particularly telling. RT Jones stored PII on a third-party hosted web server, which was compromised in a cyber-attack. After the attack, RT Jones took remedial steps which included retention of a forensics consulting firm that traced the hacker to China, and notification of each person whose information was compromised. There is no indication – at least yet – that any RT Jones client suffered financial harm as a result of the attack.

The SEC, however, determined that RT Jones willfully violated Rule 30(a) of Regulation S-P, the ''Safeguards Rule'' that applies to investment advisers and broker-dealers, and requires written policies and procedures to ensure information security. The Commission noted that RT Jones did not have such written safeguards in place in advance of the cyber-attack and issued a $75,000 fine.

If the RT Jones case is any indication, the SEC's message to investment advisers and broker-dealers couldn't be clearer: cybersecurity is not just an IT issue and it's time to get your house in order and implement a thoughtful and detailed cybersecurity plan *before* the hackers strike. But equally clear is the fact that there's no ''one size fits all solution.'' Yes, stronger firewalls are part of the mandate but it's also about the intelligent design of an overall cybersecurity program including governance that makes sense for a particular organization. While the SEC's September 2015 Risk Alert establishes a framework and key elements for cyber preparedness, each organization will need to assess their own vulnerabilities and design a plan to address those risks. Specific considerations might include whether a firm has an outward-facing website and the vulnerabilities that might create, or whether penetration testing, often called ''pentesting'' for short, makes sense to determine if a network is vulnerable to an outside attack.

With so much at stake, investment advisers and broker-dealers that don't answer the SEC's call for cybersecurity preparedness will be operating at their own peril with the weight of both the Commission, and the business-crippling impact of a hacking ready to come down hard.

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0037-0665