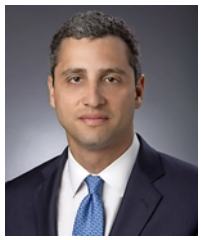
Bloomberg Law

Securities Regulation & Law Report™

CYBERSECURITY

The SEC's Relentless Focus on Cybersecurity: After WannaCry, Head of Enforcement Says Cybersecurity Is the Greatest Threat to the Industry


BY NICOLAS MORGAN, ROBERT SILVERS, AND ADAM M. REICH

According to Steven Peikin, the newly named co-director of the Division of Enforcement for the U.S. Securities and Exchange Commission (''SEC''), ''The greatest threat to our markets right now is the cyber threat.'' On June 8, 2017, Mr. Peikin's co-director, Stephanie Avakian, noted an ''uptick'' in cyber crime investigations by the SEC and also acknowledged concerns that ''the cyber threat'' to the nation's markets and investors ''will continue to emerge.''

Over the past several years, an increasing rhythm of enforcement actions, audits of cybersecurity controls, and issuance of risk alerts and other advisories from the U.S. Securities and Exchange Commission (''SEC'') has put regulated firms on notice that they may have to answer for the state of their organizations' cybersecurity. In an extraordinary interview, the SEC's new co-director for the Division of Enforcement, Steven Peikin, made clear just how seriously the Commission is taking this issue when he declared that ''the greatest threat to our markets right now is the cyber threat.''

Peikin's comments come on the heels of the unprecedented global spread last month of WannaCry, a ransomware strain that preys on a vulnerability in the nearly ubiquitous Microsoft Windows platform. WannaCry held hostage tens of thousands of networks and computing systems around the globe, including those belonging to companies, hospitals, utilities, and individuals.

The trend of the last several years is now confirmed: cybersecurity is a front-burner issue for the SEC. Regulated entities should expect more audits, regulatory inquiries, investor inquiries, and, ultimately, more enforcement actions from the SEC.

The May 17, 2017 Ransomware Alert

On May 17, 2017, the SEC's Office of Compliance Inspections and Examinations (''OCIE'') published a National Exam Program Risk Alert, Cybersecurity: Ransomware Alert. This Alert sets forth best practices for investment advisers, investment companies, and registered broker-dealers for protecting investors' private information.

The SEC describes OCIE's May 17, 2017 Ransomware Risk Alert as ''highlight[ing] the importance of conducting penetration tests and vulnerability scans on critical systems and implementing system upgrades on a timely basis.'' Unpacked, that description suggests that failure to timely and properly install system updates and patches when they are promoted by platform owners like Microsoft could spur enforcement proceedings and liability. Indeed, in the very first paragraph of the Alert, OCIE ''encourage[s]'' broker-dealers and investment management firms to ''(1) review the alert

published by the United States Department of Homeland Security's Computer Emergency Readiness Team — U.S. Cert Alert TA17-132A — and (2) evaluate whether applicable Microsoft Patches for Windows XP, Windows 8, and Windows Server 2003 operating systems are properly and timely installed.''

OCIE's May 17, 2017 Risk Alert was also significant in confirming that the SEC's active review and examination of cybersecurity practices of registered investment advisers, companies, and broker-dealers since before the WannaCry ransomware attack. Specifically, OCIE advises that it has examined 75 SEC-registered investment advisers, companies, and broker-dealers as part of a larger assessment of ''industry practices and legal, regulatory, and compliance issues associated with cybersecurity preparedness'' consistent with an OCIE Initiative announced in 2015. Based on this larger examination, OCIE has identified three specific practices that ''may be particularly relevant to smaller registrants'' in relation to WannaCry and future ransomware attacks: (1) periodic risk assessments of critical systems in order to identify cybersecurity threats, vulnerabilities, and potential business consequences; (2) penetration testing and vulnerability scans of critical systems; and (3) process design and enforcement relating to regular system maintenance, including installation of software patches to address security vulnerabilities.

Taken as a whole, the Risk Alert, and its references to prior guidance and initiatives published by OCIE, the SEC's Division of Investment Management (''DIM''), and the Financial Industry Regulatory Authority (''FINRA''), establishes a baseline for SEC expectations and investment adviser compliance. Cybersecurity has indeed been a focus of the SEC since at least 2014, when OCIE's National Examination Program identified ''information leakage and cyber security'' as a ''core risk'' common to registrants' businesses ''likely to continue for the foreseeable future.'' In the years since this pronouncement, OCIE has conducted further examinations to identify cybersecurity risks and assess cybersecurity preparedness in the securities industry, and continued to identify cybersecurity as an Examination Priority every year up to and including the present. And, increasingly, the SEC is holding regulated firms to account for its expectations by bringing enforcement actions.

SEC Cybsersecurity Enforcement Is Trending Upward

Since 2015, the SEC has pursued several high profile cybersecurity-related regulatory enforcement actions. For example, on September 22, 2015, the SEC announced a settlement relating to charges that the registered investment adviser ''failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients.'' Specifically, the SEC charged the Investment Adviser with violating Rule 30(a) of Regulation S-P under the Securities Act of 1933 (the ''Safeguards Rule''), because it had not adopted any written policies and procedures to ensure security and confidentiality of investors' PII, and to protect against anticipated threats or unauthorized access.

Several months later, in 2016, the SEC similarly charged a registered broker dealer and its principals with violating Regulation S-P's requirements that broker-dealers adopt written policies and procedures to protect customer information and records and to keep and maintain copies of all business communications. Specifically, the SEC alleged that the broker-dealer or its principals had not adequately protected investor PII by using personal email addresses for business matters, including to receive faxes and not having adequate written supervisory procedures to protect PII. The matter was resolved by an administrative settlement that cost the Respondents $150,000 in collective penalties.

Taken as a whole, the Risk Alert, and its references to prior guidance and initiatives published by OCIE, the SEC's Division of Investment Management, and the Financial Industry Regulatory Authority, establishes a baseline for SEC expectations and investment adviser compliance.

Shortly thereafter in 2016, the SEC issued a settled administrative order finding that a well-known investment advisory firm had violated the Safeguards Rule because two of the company's internal web ''portals,'' which allowed its employees to access investor PII, did not have effective authorization modules restricting employee access to investor data based on legitimate business needs, and because the firm did not audit or test relevant authorization modules, nor monitor or analyze access to and use of the portals. In the absence of appropriate oversight, a firm employee accessed and PII from approximately 730,000 investor accounts to his personal server, which was subsequently hacked. The charges were resolved with an unprecedented $1,000,000 penalty.

Conclusion: Takeaway Lessons for Investment Advisers

The SEC's prompt and prescriptive response to the WannaCry ransomware attack, combined with Director Peikin's recent comments, is yet further evidence that the SEC's vigilance regarding cybersecurity will continue and escalate.

Between escalating enforcement actions and proliferating OCIE advisories, the SEC has now articulated a landscape of regulatory expectation to which it expects investment advisers to adhere when it comes to cybersecurity. It is no longer sufficient for regulated entities to ''have a plan'' and hope that the SEC finds it sufficient.

Instead, the most sophisticated firms are now mapping their cybersecurity programs against the elements that the SEC has expressly stated that it expects to see. This includes, of course, time-tested basics like periodic risk assessments of critical systems, penetration testing

  SRLR ISSN 0037-0665

and vulnerability scans, regular system maintenance, and formulation and exercising of incident response and recovery plans. After WannaCry, it now also includes regular data back-up protocols, regular consultation of the Department of Homeland Security's US-CERT alerts, prompt installation of software patches and updates, and having a response plan specific to ransomware.

* * * * *

Nicolas Morgan is a partner in the Investigations and White Collar Defense practice at Paul Hastings and based in the firm's Los Angeles office. He focuses his practice on complex securities litigation in state and federal courts and representations involving government investigations and white-collar crime allegations levied against individuals and businesses.

Robert Silvers is a partner in the White Collar Investigations and Privacy and Cybersecurity practices of Paul Hastings and is based in the firm's Washington, D.C. office. His practice focuses on cybersecurity and data privacy, internal investigations and enforcement proceedings, government security review of foreign investments, and civil litigation at the intersection of law and national security. He previously served as Assistant Secretary for Cyber Policy at the U.S. Department of Homeland Security.

Adam Reich is an associate in the Litigation practice of Paul Hastings and is based in the firm's Los Angeles office. His practice is principally concentrated in complex commercial litigation matters, and includes counseling relating to cybersecurity and general contract issues.