MORRISON | FOERSTER

Client Alert

April 22, 2014

Cybersecurity: SEC Is Starting to Scrutinize Registrants' Practices

By Daniel A. Nathan and Libby J. Greismann

The SEC plans to examine the cybersecurity practices of over 50 registered broker-dealers and investment advisers. The SEC announced its plan in an April 15, 2014 Risk Alert, which closely follows the March 26 Cybersecurity Roundtable at which Chair Mary Jo White underscored the importance of cybersecurity to market security and customer data protection. At the Roundtable, Chair White emphasized the "compelling need for stronger partnerships between the government and private sector" to address cyber threats.[1]

The Risk Alert included a comprehensive Appendix detailing the types of questions the SEC may be asking registrants in these exams, on such topics as cybersecurity governance, risks associated with remote customer access and risks associated with vendors and third parties. The sample questions include whether companies have discovered malware in their systems, suffered a network breach or found that computers used by customers and vendors to remotely access networks have been compromised since January 2013.[2]

The scope and detail of the sample questions reflect the SEC's commitment to assessing and encouraging cybersecurity readiness. In the past, the SEC has been fairly active in enforcing Rule 30 of its Regulation S-P (Privacy of Consumer Financial Information), the so-called Safeguards Rule, in the cybersecurity area. The SEC has imposed fines ranging from $100,000 to $275,000 for such deficiencies as the failure of a firm to have customer information policies and procedures for its employees designed to protect customer records and information, distribution of limited and insufficient written materials regarding safeguarding customer information and failure to implement adequate controls to safeguard customer information. FINRA has also been active in the area of cybersecurity, as discussed in our previous Client Alert. However, the increased attention, in the wake of several recent highly publicized intrusions, likely heralds additional enforcement actions and more serious scrutiny of companies' preparedness to respond to the growing threat presented by cyber hackers.

RESPONDING TO THE RISK ALERT

It is incumbent on companies to ensure that their practices are up to snuff when the scrutiny arrives. First, companies should use the SEC's questions themselves to gain insight into the regulators' thinking and adjust their own policies and processes accordingly. The questions are far more specific than anything previously issued by the SEC, and the level of detail is a valuable resource for those companies that are searching for guidance in updating their cybersecurity practices. Companies should ask themselves the questions provided in the Risk Alert

[1] Chair Mary Jo White, "Opening Statement at SEC Roundtable on CyberSecurity" (March 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

[2] The SEC is in a good position to offer such advice, having been the subject of a Government Accounting Office audit earlier this year that identified several ways that the SEC's own network, servers, applications and databases were open to cyberattack. "Without adequate access controls, unauthorized individuals, including intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or for personal gain," the auditors wrote.

to ensure that they are complying with the SEC's proposed cybersecurity framework. Among other things, the SEC will be requesting information about:

- The firm's cybersecurity governance, including:
  - the firm's practices for managing information security assets;
  - whether the firm conducts periodic risk assessments to identify cybersecurity and physical security threats; and
  - the firm's written information security policy, written business continuity plan to mitigate the effects of a cybersecurity incident and written documentation of cybersecurity roles and responsibilities.
- The firm's practices for protecting its networks and information, including:
  - employee training in information security and risks;
  - controls to prevent unauthorized escalation of user privileges and lateral movement among network resources;
  - processes for managing IT assets and ensuring regular system maintenance; and
  - the firm's information security policy, written data destruction policy and written cybersecurity incident response policy.
- The firm's practices for dealing with risks associated with remote customer access and funds transfer requests, including:
  - whether the firm provides customers with on-line account access;
  - the firm's procedures for verifying authenticity of email requests seeking to transfer customer funds; and
  - firm policies for addressing responsibility for losses associated with attacks impacting customers.
- The firm's practices regarding risks associated with vendors and other third parties, including whether the firm conducts cybersecurity risk assessments of vendors and business partners, and details about those assessments.
- The practices employed by the firm to assist in detecting unauthorized activity on its networks and devices, and details about those practices.
- Any previous cybersecurity breach, including any detected malware, unauthorized user breach, fraudulent activity or emails.
- Any incident in which customer information was stolen, lost or exposed, resulting either from deliberate wrongdoing, an accident or negligence.

If, in reviewing these questions, firms identify aspects of their cybersecurity policies and procedures that do not conform to the SEC's expectations, they should first consider whether their business model and size require such policies. A firm need not be expected to say "yes" or provide detail with respect to every single question asked, but it must be prepared to explain its answer if it appears insufficient. On the other hand, if the firm concludes that it should have a policy or procedure in place, it should immediately develop a plan for instituting the missing practice. A firm should identify an appropriate vendor for strengthening its security plans and lay out a clear timetable for implementing those plans. Such steps allow a firm to demonstrate a good faith effort to the SEC should the firm be examined or audited.

The non-binding nature of the SEC's Risk Alert and proposed questions suggest that the SEC is still working on its approach to cybersecurity issues. Right now, the SEC is focused on gaining information about the state of the industry and it may use that information to issue further guidelines or a more specific framework for improvement. The ability to be flexible and responsive to changing guidelines will serve firms well as the SEC clarifies its requirements and expectations.

Contact:

Hillel T. Cohn
(213) 892-5251
hcohn@mofo.com

Daniel A. Nathan
(202) 887-1687
dnathan@mofo.com

Nathan David Taylor
(202) 778-1644
ndtaylor@mofo.com

Libby J. Greismann
(202) 778-1607
lgreismann@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.