Bloomberg Law

bloombergbna.com

INSIGHT: Parallels in the SEC's Approach to Cybersecurity for Market Intermediaries and Issuers

BY VINCE MARTINEZ AND MCNAIR NICHOLS

Introduction

When it comes to cybersecurity, the Securities and Exchange Commission (SEC) has a limited regulatory hand. First, for virtually all of its registrants, the SEC has no regulation that articulates specific cybersecurity requirements (with the possible exception of Regulation SCI, which applies to a very limited number of SEC registrants). Second, SEC regulatory processes move more slowly than the pace of technological change. Accordingly, any regulation mandating specific technological measures runs the risk of being obsolete on arrival. Despite these issues, the SEC has a relatively clear and discernable approach to cybersecurity. This article discusses how the SEC has crafted staff and interpretive guidance in lieu of regulation mandating prescriptive technological requirements in order to fashion a uniform approach to cybersecurity that is thematically consistent across its registrants, from market intermediaries (such as broker-dealers, investment advisers, and investment companies) to issuers (public reporting companies).

SEC Regulations Applicable to Market Intermediaries Rule 30 of Regulation S-P, known as the ''Safeguards Rule,'' requires firms to implement policies and procedures to: insure the security and confidentiality of customer records and information; protect against anticipated threats; and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to a customer. *See* 17 C.F.R. § 248.30 (2004). To date, the SEC has brought most of its cybersecurity-related enforcement actions as violations of Rule 30, including most recently *R.T. Jones Capital Equities Management, Inc.*, Investment Advisers Act Rel. No. 4204 (Sept. 22, 2015); *Craig Scott Capital*, Securities Exchange Act Rel. No. 77595 (Apr. 12, 2016); and *Morgan Stanley Smith Barney LLC*, Securities Exchange Act Rel. No. 78021, Investment Advisers Act Rel. No. 4415 (June 8, 2016).

However, Rule 30 is limited in two important ways. First, its information protection requirements apply to the information of ''customers'' and ''consumers,'' the latter of which is defined as ''an *individual* who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.'' 17 C.F.R. § 248.3(g)(1) (2009) (emphasis added). Second, the rule specifies no means for accomplishing its objectives. Instead, it requires registrants to create ''reasonably designed'' policies and procedures. In other words, Rule 30 merely articulates a principles-based standard. However, a registrant must act at least negligently to violate Rule 30. *See NEXT Financial Group, Inc.*, Admin. Proc. File No. 3-12738, at 23 (June 18, 2008). To illustrate the SEC's difficulty in creating specific technological measures in its regulations, the SEC has tried without success to amend Regulation S-P three times.

Other applicable regulations are less specific. Rule 206(4)-7 under the Investment Advisers Act of 1940 requires registered investment advisers to adopt and implement policies and procedures ''reasonably designed'' to prevent securities law violations, to conduct an annual review, and to designate a Chief Compliance Officer to administer compliance policies. Likewise, Rule 38a-1 under the Investment Company Act of 1940 imposes a similar policies and procedures requirement on registered investment companies. The only indication that these rules encompass cybersecurity is that cybersecurity-related concepts##8213;such as ''[s]afeguards for the privacy protection of client records and information'' and ''[b]usiness continuity plans''##8213;are mentioned among the considerations that registrants are expected to address in the preamble to the final rule. Advisers Act Rel. No. 2204 (Dec. 17, 2003). Otherwise, the mandate of these rules is a simple direction to ensure that the registrant is adhering to its obligations under the federal securities laws.

Nonetheless, it is through these broad prescriptions that the SEC staff has pursued the agency's basic approach to integrating cybersecurity into the business processes of market intermediaries. In April 2015, the SEC's Division of Investment Management (IM) issued a ''Cybersecurity Guidance Update,'' which described measures that ''funds and advisers may wish to consider'' regarding their cybersecurity. SEC Division of Investment Management, *Guidance Update: Cybersecurity Guidance*, No. 2015-02 (Apr. 2015). Most instructive is the following passage:

In the staff's view, funds and advisers should identify their respective compliance obligations under the federal securities laws and take into account these obliga-

tions when assessing their ability to prevent, detect and respond to cyber attacks. Funds and advisers could also mitigate exposure to any compliance risk associated with cyber threats through compliance policies and procedures that are reasonably designed to prevent violations of the federal securities laws.

Id. at 2. In effect, IM is stating that although cybersecurity is not a regulatory requirement itself, it is necessary in this day and age to ensure that a registrant is able to meets its obligations under the federal securities laws. More simply put, the SEC is bootstrapping cybersecurity onto other regulatory requirements.

SEC Cybersecurity Guidance for Issuers This same bootstrapping concept informs the agency's approach to issuers, for whom the regulatory ties to cybersecurity are more limited. Unlike market intermediaries, the SEC does not regulate the businesses of issuers. Instead, the regulation of public reporting companies is limited to imposing standards on the quality of disclosures, books and records, and internal controls. Accordingly, the agency's ability to integrate cybersecurity into the conduct of issuers is much less substantial.

In February 2018, the SEC issued a ''Statement and Guidance on Public Company Cybersecurity Disclosures.'' Securities Exchange Act Rel. No. 82756 (Feb. 21, 2018). Although, like staff guidance, it does not have the force of law or regulation, it does represent the agency's considered views on the place of cybersecurity in issuer disclosure practices. Further, like the April 2015 IM Guidance discussed above, it creates a linkage between cybersecurity and an issuer's regulatory obligations##8213;in this case disclosure controls. The February 2018 Interpretation largely reiterated guidance issued by the staff of the SEC's Division of Corporation Finance (CorpFin) in October 2011, but added a new section on disclosure controls and procedures. Most instructive is the following passage:

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications . . . . When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents. Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness. These rules define ''disclosure controls and procedures'' as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) ''recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms,'' and (2) ''accumulated and communicated to the company's management . . . as appropriate to allow timely decisions regarding required disclosure.''

Id. at 18-20. Again, the agency's approach is not to impose cybersecurity requirements directly. Nor does it seek to define specific technological measures. Instead, the February 2018 Interpretation makes the case that cybersecurity is a necessary part of a public reporting company's ability to ensure that it is detecting disclosure-worthy cyber events, and making timely and appropriate disclosures.

Coincidentally enough, the SEC drove these points home shortly after issuing the interpretation by bringing an enforcement action for a failure to disclose a data breach. On April 24, 2018, the SEC announced a settlement under which Altaba (formerly Yahoo! Inc.) agreed to pay a $35 million penalty in response to charges that it failed to disclose a significant data breach of personal information from user accounts. *See Altaba Inc., f/d/b/a Yahoo! Inc.*, Securities Act Rel. No. 10485 (Apr. 24, 2018). According to the SEC's order, members of the company's senior management and legal department were informed of the breach, but the company nevertheless failed to ''properly assess the scope, business impact, or legal implications of the breach.'' *Id.* at 6. In short, this is an instance of an asserted failure to properly implement controls reasonably designed to ensure that material information is timely and effectively disclosed. That fact was made clear by Jina Choi, Director of the SEC's San Francisco Regional Office, who stated in the accompanying press release that ''Yahoo's failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors.'' SEC Press Release, *Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million* (Apr. 24, 2018).

How Will the SEC's Approach to Cybersecurity Unfold over Time? It is difficult to predict how a regulatory approach grounded in staff and interpretive guidance coupled with the indirect application of principles-based regulations will manifest itself. Still, recent SEC staff practices offer some important clues.

With respect to market intermediaries, the SEC has been signaling its expectations for a little over four years. Beginning on April 15, 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a ''Risk Alert'' announcing its first ''Cybersecurity Initiative,'' the results of which it announced publicly on February 3, 2015 in a subsequent Risk Alert. OCIE issued another Risk Alert to announce a second ''Cybersecurity Examination Initiative'' on September 15, 2015, which also led to published results on August 7, 2017. All of these Risk Alerts can be found on the SEC's

website. Attached to the Risk Alerts announcing each initiative was an Appendix which listed specific questions and topics that firms could expect to encounter in an OCIE examination that included a cybersecurity component. These Appendices were based in part on the February 12, 2014 ''Framework for Improving Critical Infrastructure Cybersecurity,'' issued by the National Institute of Standards and Technology. Both Appendices were offered by OCIE with the stated purposes to ''empower'' and ''assist'' firms in evaluating their own cybersecurity preparedness. Significantly, the guidance articulated in the Appendices became more precise and prescriptive over time, venturing from general questions about policies and procedures to specific questions about controls and documentation.

While OCIE's guidance is a laudable effort to help firms increase their cybersecurity preparedness, it carries potential risks; namely, it can create *de facto* standards with respect to policies, procedures and technological measures that firms must become familiar with, and upon which they may be judged. In other words, these staff-created measures may well become the standards by which ''reasonably designed'' policies and procedures are evaluated.

Certainly, recent enforcement actions for violations of the Rule 30 of Regulation S-P reflect an intention to define ''reasonable design'' in light of failures to apply specific technological measures including encryption, access restrictions and monitoring controls. *See R.T. Jones* at 3; *Morgan Stanley* at 5-6. It is fair to predict both that cybersecurity examination components will become more frequent and detailed, that enforcement actions will not be limited to firms that have been attacked (e.g., *Craig Scott*), and that OCIE and the Division of Enforcement will find deficiencies and violations based on concepts articulated in staff guidance.

With respect to issuers, the picture is less clear, but again past practice may give some clues as to how things will proceed. When CorpFin first issued its cybersecurity guidance in 2011, it spawned a raft of comment letter practice in which the staff evaluated cybersecurity disclosures from various issuers. *See*, *e.g.*, *SEC Staff Comment Letter to Prosper Marketplace, Inc.* (Jun. 29, 2012); *SEC Comment Letter to Hilton Worldwide Holdings Inc.* (Oct. 10, 2013). While the tendency to seek more tailored disclosures was evident, the letters did not collectively identify further guidance on the quality of disclosures.

The February 2018 Interpretation, however, is potentially quite different. Because it includes a new section on the relationship between cybersecurity and effective disclosure controls, we may see comment letters requesting disclosures on the effectiveness of a company's disclosure controls. Further, to the extent that it becomes accepted that robust cybersecurity is necessary to ensure effective disclosures, then a company's cybersecurity policies and procedures could themselves become the subject of audits, and their absence or inadequacy could be cited as weaknesses.

With respect to enforcement actions emanating from cybersecurity disclosures, the picture is still less clear. The *Altaba* case involved an alleged failure to disclose a material breach that was significant enough to bring an antifraud charge. Most disclosure issues will not be so remarkable. To the extent that a company can resolve disclosure questions raised by CorpFin during a filing review, it would be rare for that interaction to result in an enforcement referral. Fraudulent disclosures aside, the most likely outcomes of the February 2018 Interpretation will be a growing focus on the integration of cybersecurity into a company's policies and procedures and, in certain cases, a growing insistence on disclosures that reflect a company's efforts to ensure that its disclosure controls surrounding cyber events are effective.

Vince Martinez is a partner in K&L Gates' Washington, D.C. office, where he focuses his practice on counseling and defending financial services firms, companies, and individuals facing government examinations, investigations, and charges. He has a distinguished history of leadership at the Securities and Exchange Commission and the Commodity Futures Trading Commission.

McNair Nichols is an associate in K&L Gates' Washington, D.C. office, where he focuses on the defense of companies and individuals subject to government investigations, enforcement, and other regulatory actions. He has assisted in the representation of individuals and financial institutions before the SEC and the Financial Industry Regulatory Authority.