Privacy and Data Security Enforcement: The SEC is Getting in on the Action

Introduction

Given the increasing importance of data to organizations and the ever-increasing connectedness of our world, cybersecurity has become a major issue for companies today. While headlines tend to focus on the breaches of large retailers, all organizations have valuable information, and most will suffer some sort of data breach in the upcoming years.[1] When they do, they may suffer enormous costs: the average data breach (not including the mega breaches) costs the breached organization $3.5 million.[2]

The regulation of privacy and data security in the United States is a patchwork of laws enforced by a variety of government actors, and until recently, the Securities and Exchange Commission ("SEC") has taken a backseat to other regulators. To date, the entity claiming the lead in this space has been the Federal Trade Commission, who, under its statutory framework to monitor and bring enforcement actions to prevent unfair or deceptive trade practices, has entered into a series of consent settlements with companies whose cybersecurity practices allegedly have been inconsistent with those companies' stated protection practices or, in a few cases, have been so inadequate as to allegedly constitute an "unfair" practice in the FTC's eyes.[3] State Attorneys General have also entered into settlements with breached companies under state consumer protection statutes, while agencies like the Consumer Financial Protection Bureau and the Federal Communications Commission have played a role in policing privacy and data security among organizations under their respective jurisdictions.

Recently, the SEC has begun focusing on cybersecurity as well. In March 2014, the SEC sponsored a cybersecurity roundtable, and in her opening remarks, Chairwoman Mary Jo White highlighted the SEC's focus: "The SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information."[4] Based on the SEC's actions in the year since the roundtable, we predict that the SEC will use a three pronged approach in which it 1) gathers information from market participants; 2) brings enforcement actions against failures to safeguard customer data; and 3) scrutinizes public-company disclosures regarding cybersecurity.

SEC's OCIE Cybersecurity Examination Initiative

Less than a month after Chairwomen White's statement, on April 15, 2014, the SEC launched the Office of Compliance Inspections and Examinations ("OCIE") Cybersecurity Examination Initiative as part of its effort to "assess cybersecurity preparedness in the securities industry."[5] Under the initiative, the SEC sent questionnaires to, and conducted examinations of, certain registered broker-dealers and investment advisers, asking about their cybersecurity governance, risk management, and experiences with cybersecurity threats. The purpose of the initiative was to "help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats."[6] The questionnaire itself

---

[1] *See* Ponemon Institute, *Is Your Company Ready for a Big Data Breach?* (2014) at p. 1, *available here*, (finding approximately 43% of organizations have had a breach in the last year, alone, and that number is up from 33% in 2013).
[2] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis* (2014) at p.1, *available here*.
[3] *See* Federal Trade Commission, *Enforcing Privacy Promises*, (listing the FTC's privacy related enforcement actions).
[4] SEC Chairman Mary Jo White, *Opening Statement at SEC Roundtable on Cybersecurity* (March 26, 2014), *available here*.
[5] Risk Alert, Office of Compliance Inspections and Examinations, OCIE Cybersecurity Initiative (April 15, 2014), at p.1, *available here*.
[6] *Id.* at 2.

was "intended to empower compliance professionals in the industry with questions and tools they can use to assess their firms' level of preparedness, regardless of whether they are included in OCIE's examinations."[7]

For these initial exams, the SEC selected 57 broker-dealers and 49 registered investment advisers to get "perspectives from a cross-section of the financial services industry and to assess various firms' vulnerability to cyber-attacks."[8] The staff then "collected and analyzed information from the selected firms," "held interviews with key personnel," and "conducted limited testing of the accuracy of the responses and the extent to which firms' policies and procedures were implemented."[9] The exam staff did not review the technical sufficiency of the firms' programs.[10]

On February 3, 2015, the OCIE released a "Risk Alert" in which it reported the results of the examinations. Incredibly, 88% of broker-dealers and 74% of advisers revealed that they had experienced a cyber-attack directly or through one or more of their vendors.[11] Not surprisingly, these entities are actively grappling with the best approach to cybersecurity, and the firms vary broadly in how rigorously they approach the issue. Here are some of the summary observations from the examinations that the OCIE reported in its Risk Alert:

i. Appointment of a Chief Information Security Officer ("CISO") -- 68% of broker-dealers and 30% of advisers specifically designate an individual as a CISO, and advisers often direct their Chief Technology Officer to assume such responsibilities;
ii. Written information security policies -- 93% of examined broker-dealers and 83% of advisers have written information security policies, and 89% of broker-dealers and 57% of advisers conduct periodic compliance audits of these policies;
iii. Periodic risk assessments -- 93% of broker-dealers and 79% of advisers conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities and business consequences;
iv. Information gathering -- 47% of broker-dealers were members of industry groups, associations, or organizations (both formal and informal) that exist for the purpose of sharing information regarding cybersecurity, while advisers more frequently relied on discussions with peers and independent research;
v. Firm-wide inventorying of technology resources -- although it varied according to the resource, 91-96% of broker-dealers and 60-92% of advisers conducted firm-wide inventorying of technology resources;
vi. Cybersecurity risk policies relating to vendors -- 72% of broker-dealers and 24% of advisers incorporated cybersecurity risk into their contracts with vendors, while 51% of broker-dealers and 13% of advisers had policies and procedures related to information security training for vendors who access their network;
vii. Use of encryption -- 98% of broker-dealers and 91% of advisers made use of encryption in some form;

---

[7] *Id.* The questionnaire was based on the National institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework"). The NIST Framework is widely used in cybersecurity, and breaks down an organization's cybersecurity into five activities: identification, protection, detection, response, and recovery. National Institute of Standards & Technology, Framework for Improving Critical Infrastructure Cybersecurity, (Ver. 1.0, Feb. 12, 2014), *available here*.
[8] Risk Alert, Office of Compliance Inspections and Examinations, Cybersecurity Examination Sweep Summary (February 3, 2015), at p.1, *available here*.
[9] *Id.*
[10] *Id.*
[11] *Id.* at 2-3.

viii. Suggestions for customer protection of data -- all broker-dealers and 75% of advisers who allow their retail customers online access to their accounts provide their customers with some form of information about reducing cybersecurity risks in conducting transactions with the firm; and

ix. Use of cybersecurity insurance -- 58% of broker-dealers and 21% of advisers maintain cybersecurity insurance, but only one broker-dealer and adviser had actually filed claims under such insurance.

The OCIE provided no commentary when it reported these results, simply noting that the staff was "still reviewing the information" and that OCIE "will continue to focus on cybersecurity using risk-based examinations."[12] Nevertheless, OCIE's observations suggest emerging industry practices and the SEC's potential expectations on how prevalent those practices should be, and broker-dealers, investment advisers and other companies should use the survey findings to evaluate their own approach to cybersecurity. The SEC has not announced what it plans to do as a follow-up to this initiative, but it has stated that it plans to continue "assessing cybersecurity controls across a range of industry participants."[13]

SEC's Ongoing Monitoring and Enforcement

We predict that the second prong of the SEC's strategy is enforcement and many expect that the SEC will follow up the OCIE Cybersecurity Examination Initiative and future examinations with cybersecurity enforcement actions. The initiative and past enforcement actions suggest that the SEC will focus on companies' policies for safeguarding customer data, and that such actions will be brought against registered broker-dealers and investment advisers under Rule 30 of Regulation S-P, known as the "Safeguard Rule."[14] The Safeguard Rule provides that:

> Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:
>
> a. Insure the security and confidentiality of customer records and information;
> b. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
> c. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The SEC has relied on the Safeguard Rule in the past (i.e., before the OCIE sweep) to scrutinize the policies and procedures of broker-dealers and investment advisers and to bring enforcement actions when it believes that a firm's policies and procedures are not "reasonably designed" to meet the goals of the Rule. The SEC has taken the position that this includes having procedures in place to safeguard against reasonably foreseeable risks.

---

[12] *Id.* This was in sharp contrast to the Financial Industry Regulatory Authority Report, issued at around the same time, which laid out detailed suggested approaches to information security. *See* Financial Industry Regulatory Authority, *Report on Cybersecurity Practices* (February 2015), *available here*. The FINRA report, like the SEC report, however, did "not create any new legal requirements or change any existing regulatory obligations." *Id.* at 2.

[13] Press Release, Securities and Exchange Commission, SEC Announces 2015 Examination Priorities (January 13, 2015), *available here*.

[14] SEC Regulation S-P, 17 C.F.R. § 248.30(a) (2014). FINRA also has jurisdiction to bring actions under Regulation S-P. *See, e.g.*, D.A. Davidson & Co., FINRA Letter of Acceptance, Waiver and Consent, No. 20080152998 (Apr. 9, 2010) (announcing a settlement for $375,000 for inadequate cybersecurity that allowed an intruder to obtain customer's personal information).

For example, in 2011 the SEC brought an action against the Chief Compliance Officer ("CCO") of a Florida-based brokerage firm for willfully violating the Safeguard Rule.[15] The CCO was responsible for implementing, maintaining, and reviewing the adequacy of his firm's policies and procedures, and he failed to revise the policies after the theft of three laptop computers and a registered representative's computer password credentials. Though there was no evidence that customer information was misused, the SEC found that the incidents exposed foreseeable risks and criticized the CCO for not revising his firm's policies, which they found to be "general and vague." The SEC noted that the policies must "instruct the firm's supervisors and registered representatives how to comply with the Safeguard Rule."[16]

In a similar 2009 action, the SEC fined a Massachusetts-based broker-dealer and investment adviser firm $100,000 for willfully violating the Safeguard Rule.[17] In this matter, an unauthorized party using malware entered the firm's intranet site, obtained customer information, and attempted to execute trades. Within ten minutes of the rogue trades, the firm detected the intruder, blocked him from further trading, and reversed the trades that had been made, eventually absorbing $8,000 in losses. Although none of the impacted consumers suffered financial harm from the incident, their personal information had been compromised. The SEC here too found that the firm's written policies were inadequate. The SEC noted that the firm recognized the need for antivirus software, but merely recommended, as opposed to required, that its registered representatives maintain antivirus software on their computers, leaving customer information vulnerable to unauthorized access.

These and similar actions are telling because they show the degree to which the SEC may scrutinize and second-guess, often with the benefit of hindsight, broker-dealers' or investment advisers' cybersecurity policies and procedures. Broker-dealers and investment advisers are wise to be mindful of the SEC's oversight and to consider instituting detailed and specific cybersecurity policies that account for foreseeable risks.

SEC's Review of Company Cybersecurity-Related Disclosures

The final prong to the SEC's approach on cybersecurity, addresses company disclosures.

In 2011, the Division of Corporation Finance at the SEC issued guidance regarding disclosure obligations related to cybersecurity (the "Guidance").[18] In the Guidance, the SEC indicated that companies may need to factor cybersecurity into multiple sections of a disclosure – not just as a general risk factor. For example, the SEC advised "[i]f one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should [also] provide disclosure in the

---

[15] In the Matter of Marc A. Ellis, No. 64220 at 2 (April 7, 2011) (fining the CCO $15,000).
[16] *Id.* ; *see also* In the Matter of David C. Levine, No. 64222 (April 7, 2011) (finding a violation of the Safeguard Rule when the company "knew that there was a reasonably foreseeable risk that its departing registered representatives would disclose customer nonpublic personal information to successor brokerage firms but nonetheless failed to adopt [or have in place] any written policies or procedures addressing the transfer and protection of such information"); In the Matter of J.P. Turner & Company, LLC, Rel. Initial Order No. 395 at 15 (May 19, 2010) *finalized in* In the Matter of J.P. Turner & Company, LLC, No. 62313 (June 17, 2010) (fining a broker-dealer $65,000 for having minimal guidelines that failed to include "a method for or steps describing how its registered representatives should safeguard their customers' information").
[17] In the Matter of Commonwealth Equity Services, LLP, No. 60733 (Sept. 29, 2009).
[18] Securities and Exchange Commission, Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (October 13, 2011),

registrant's 'Description of Business.'"[19] Similarly, the Guidance explained how cybersecurity risks might need to be included in disclosures regarding management's discussion and analysis of financial condition and results of operation as well as in descriptions of legal proceedings and financial statements.[20]

Similar to the view that the SEC takes when ensuring that financial institutions safeguard customer information, the SEC frames disclosure obligations based on "risks of potential incidents."[21] For example, the Guidance explains that "[r]egistrants should address cybersecurity *risks* and cyber incidents . . . if the costs . . . associated with one or more known incidents or *the risk of potential incidents* represent a material event . . . likely to have a material effect on the registrant's results of operations, liquidity, or financial condition . . . ," and "[i]n evaluating whether risk factor disclosure should be provided, registrants should also consider . . . risks to that security, *including threatened attacks of which they are aware*."[22] In other words, the SEC takes the view that a company should factor all known or potential risks of a cybersecurity incident into their disclosure decisions.

In this regard, when a public company experiences a data breach, the SEC may review the company's public filings to see whether the breached-entity properly considered its potential and known risk, and companies who have experienced a breach might have to answer questions from the SEC about whether the company knew or should have known about a risk that contributed to the attack and, if so, whether their prior disclosures adequately accounted for such risk. To assess foreseeability and thus the adequacy of earlier disclosures, the SEC may inquire about earlier breaches, help desk complaints, security audits, and other factors that could have alerted management to the potential risk.

Conclusion

At the March 2014 roundtable SEC Commissioner Luis A. Aguilar noted his concern about the risks that cyber-attacks pose to public companies and to the capital markets, concluding that: "There is no doubt that the SEC must play a role in this area. What is less clear is what that role should be."[23] A year later, the SEC is still grappling with its proper role in protecting investors and markets from cyber risks, but as it continues to gather information and experience in this space, the SEC will inevitably expand its enforcement footprint.

Laura Hoey
Jonathan Schmidt
Justin Van Etten
Lindsey Sullivan

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.* (emphasis added).
[23] SEC Commissioner Luis A. Aguilar, *The Commission's Role in Addressing the Growing Cyber-Threat*, (March 26, 2014), *available here*.