GOVERNING CYBERSECURITY: THE SEC ENTERS THE RING

INTRODUCTION

Modern businesses and securities trading systems rely on high-speed digital communication technologies. One of these digital technologies, electronic information storage, has become a source of great liability. Electronic information storage is standard for most industries because it is a highly efficient method of storing and accessing large volumes of information.\(^1\) Even sensitive data, such as medical records and financial information, is increasingly stored electronically.\(^2\)

With increased reliance comes increased vulnerability. The more businesses and securities traders increase their use of electronic information storage, the more susceptible they become to cybersecurity breaches called “cyberattacks.” A cyberattack is a “deliberate [action] to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.”\(^3\) Cybersecurity breaches affect the entire economy because breaches impact both consumer confidence in businesses and the integrity of trading systems. The frequency of cyberattacks has increased over the past decade and will likely continue to increase as hackers become more advanced.\(^4\) This trend has not gone unnoticed by the Federal Trade Commission (“FTC”) or the Securities and Exchange Commission (“SEC”).

This Perspective will seek to explain how the FTC and SEC can regulate cybersecurity measures without redundancy and to suggest compliance strategies for regulated entities. To accomplish these goals, this Perspective

---


will explain how the FTC and SEC began regulating cybersecurity measures, compare the SEC’s and FTC’s involvement in cybersecurity regulation, and ultimately discuss how the agencies’ increasing focus on cybersecurity will impact corporate governance and accountability.

I. THE FEDERAL TRADE COMMISSION

Since 1996, the Federal Trade Commission has been interested in regulating companies’ cybersecurity measures. The FTC sees itself as a law enforcement agency that protects consumers by educating businesses and consumers about privacy and security issues.

The FTC draws its cybersecurity enforcement power from Section 5 of the Federal Trade Commission Act (“Section 5”) which prohibits unfair or deceptive business practices. In order to protect consumer privacy, the FTC takes measures to ensure that companies protect any consumer information they gather. The FTC promulgated its first rules on cybersecurity measures in 2000 and has been issuing rules as well as offering workshops on cybersecurity ever since. The rules, such as the Privacy of Consumer Financial Information Rule, generally require institutions to provide consumers with notice of their privacy policies.

Since 2002, the FTC has brought over fifty enforcement actions under Section 5 based on failure to implement “reasonable” data security systems. These cases include cases against Snapchat, Inc., Atlanta Falcons Football Club, LLC, and Verizon, Inc. Because the FTC is consumer focused, its primary goal is to protect personal information and build consumer confidence in the market place. To achieve this goal, the FTC’s enforcement actions generally require companies to take comprehensive measures to increase security and repair any harm done to their customers. The FTC primarily

6 Id.
8 FED. TRADE COMM’N, supra note 5.
10 FED. TRADE COMM’N, supra note 5.
11 Id.
12 Id.
13 FED. TRADE COMM’N, supra note 5.
focuses on institutions that collect sensitive data about consumers, such as medical and financial institutions. The agency investigates companies’ cybersecurity measures to determine whether they are adequate enough to protect sensitive consumer information. Unfortunately for businesses seeking clear guidelines, the FTC has maintained a flexible definition of what constitutes “reasonable” security safeguards. However, by not clearly defining a checklist of technologies required by businesses to be in compliance with FTC standards, the FTC has been able to quickly adapt its regulations to new, advancing threats. On the whole, the FTC goes to great lengths to be proactive about enforcement. In addition to its rules, the FTC regularly maintains blogs and workshops that educate and alert both businesses and consumers to cybersecurity threats. Companies interested in keeping up with FTC’s evolving industry guidance can easily access these blogs and workshops through the FTC’s website.

II. THE SECURITIES AND EXCHANGE COMMISSION

Although the SEC has only recently become interested in cybersecurity, it has made protecting registered investment companies’ (“RIC”) customer’s electronic information a priority. These RICs include publicly traded corporations and the investment companies that broker their shares. As a result, the definition of ‘customer’ has a narrower meaning for the SEC than it does for the FTC. Unlike the FTC, which focuses on protecting the common consumers’ information, the SEC seeks to protect stockholders’ sensitive information. By forcing RICs to disclose cybersecurity risk information in addition to actual breaches, the SEC seeks to ensure that stockholders are being properly informed.

14 Id.
16 Fed. Trade Comm’n, supra note 5.
17 Id.
20 Compare Fed. Trade Comm’n, 2014 Privacy and Data Security Update (2014) (stating the FTC is charged with protecting consumers), with U.S. Sec. and Exch. Comm’n, Examination Priorities for 2015 (stating the SEC’s mission includes investor protection, capital formation, and maintaining fair markets).
The SEC’s entrance into cybersecurity regulation was in some ways a natural progression from prior SEC regulations. For example, in 2000 the SEC promulgated the Privacy of Consumer Financial Information Rule (“Regulation S-P”). Known as the “safeguards rule,” Regulation S-P requires regulated entities to “adopt written policies and procedures reasonably designed to protect customer records and information.” With the shift to electronic records, Regulation S-P evolved to require firms to adopt policies and procedures, namely cybersecurity measures, designed to protect electronic records. The SEC’s power over cybersecurity regulation grew after the Dodd-Frank Wall Street Reform and Consumer Protection Act (“DFA”) was passed in 2010. The DFA transferred some regulatory power from the FTC to the SEC by requiring covered entities to develop identity theft programs that would detect and analyze possible identity theft incidents. These requirements allowed the SEC to explore its authority to regulate the cybersecurity measures used by regulated entities. The agency’s first action was the issuance of cybersecurity disclosure guidelines in 2011. In the disclosure guidelines the SEC expanded the power it gained from the DFA. It noted that although no existing rule plainly mentioned cybersecurity, many of its rules could be interpreted to require registered investment companies to disclose cybersecurity risks and incidents. The SEC went on to suggest that RICs should disclose the risk of “cyber incidents” and review the adequacy of their disclosures on an ongoing basis. Although the idea of an agency boldly regulating where it had never regulated before is troubling, agencies must evolve to meet rapidly changing threats within their jurisdiction. The SEC seems to be within a reasonable interpretation of its jurisdiction and prior regulations, such as Regulation S-P, because investors would be unable to properly evaluate the risks associated with investing in a company without knowing about its cybersecurity measures.

---

21 Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. § 248 (2000).
23 Id.
24 Shubert et al., supra note 7, at 4.
25 Id.
28 Id.
The SEC has investigated many entities within its jurisdiction and officially made cybersecurity a priority for 2015 going forward. Early SEC comment letters suggested that the SEC was primarily interested in how companies disclose their cybersecurity measures. However, recent regulations and official comments have shown an interest in controlling the actual procedures companies take to protect customer information. Under recent regulations, such as the Fair Disclosure rule (Regulation FD), RICs must develop procedures to address administrative, technical, and physical safeguards reasonably designed to protect against unauthorized access to customer information. In November 2014, the SEC promulgated the Systems Compliance and Integrity rule (“Regulation SCI”). Regulation SCI assessed the new problems presented by various new high-speed communication technologies being utilized by national securities exchanges. Regulation SCI also increased the SEC’s ability to oversee the cybersecurity measures of RICs by imposing an obligation on RICs to actively monitor their systems and prevent cyberattacks. The SEC has jurisdiction over an RIC’s cybersecurity measures because any unauthorized access to stockholder or customer information harms the financial well-being of RIC stockholders.

III. FTC vs. SEC

At first glance, it may seem redundant to have both the FTC and SEC regulating cybersecurity. Both agencies 1) require regulated entities to implement cybersecurity programs that contain administrative, technical, and physical safeguards, and 2) are concerned about the impact of cyberattacks. Additionally, the FTC has been regulating cybersecurity for much longer than the SEC and thus has much more experience on the subject. As a result, it may seem like a waste of resources for the SEC to take over a relatively small, albeit important, part of the cybersecurity realm when such an experienced agency exists to police cybersecurity. However, there are three important

29 U.S. SEC. AND EXCH. COMM’N, supra note 19, at 3.
30 Shubert et al., supra note 7, at 2.
31 Id. at 2.
32 Id. at 3.
33 Id. at 4.
34 Id.
35 Id.
36 Id. at 3.
37 Id. at 3; FED. TRADE COMM’N, supra note 5.
differences between the FTC and the SEC that justify the SEC’s entrance into cybersecurity regulation.

A. Different Focus

Although both the FTC and SEC are concerned about what companies do with consumer information, the FTC is focused on the impact to the individual consumer. On the other hand, the SEC is primarily focused on the manner companies disclose their cybersecurity measures to shareholders and the content of the disclosures. As discussed in Part II, the ‘customer’ that the agencies are concerned about is inherently different due to jurisdictional differences. Although the SEC has only recently began investigating the substance of cybersecurity measures, it has concentrated on controlling the methods with which companies determine and disclose material breaches. Much like the SEC’s definition of material information in Basic v. Levinson, the meaning of “material breach” is quite broad. Essentially, a cybersecurity breach is a “material breach” if it is substantial enough that an investor would want to know about it. The SEC does provide some guidance by giving examples of material breaches such as customer information or secret intellectual property being stolen during a cybersecurity breach. SEC rules are therefore immediately important to corporate governance because they require companies to have a system in place for determining whether a breach is a material breach and alerting shareholders if it is.

B. Different Jurisdictions

The FTC and SEC do not share the same jurisdiction. While the SEC has jurisdiction over publicly traded companies and other RICs, the FTC has jurisdiction over nearly every entity that conducts business in the United

---

38 Fed. Trade Comm’n, supra note 5.
39 Shubert et al., supra note 7, at 2.
40 U.S. SEC. AND EXCH. COMM’N, supra note 19, at 1.
41 Compare Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988) (Information is material if there is a “substantial likelihood” that a “reasonable investor” would find it important in making an investment decision or if the information would substantially alter the “total mix” of information available), with U.S. SEC. AND EXCH. COMM’N, CF Disclosure Guidance: Topic No. 2 (2011) (Cybersecurity disclosure requirements are designed to elicit information about risks and events that “a reasonable investor would consider important”).
42 U.S. SEC. AND EXCH. COMM’N, supra note 27.
43 Id.
States.\textsuperscript{44} Accordingly, a broad reading of Section 5 could give the FTC the power to regulate the security of stockholder information as well as general consumer information. However, when Congress passed the Exchange Act and created the SEC it took the regulation of securities-based issues from the FTC and placed it in the hands of the SEC. Through the Exchange Act, Congress granted the SEC a broader delegation of power to address securities-specific problems than the FTC possessed.\textsuperscript{45} Therefore, Section 5 does not likely give the FTC jurisdiction over issues that pose a threat to stockholders and securities trading, such as material breaches. These issues are reasonably within SEC jurisdiction because material breaches hurt stockholders’ investments. On the other hand, the FTC’s cybersecurity regulations will inevitably control publicly traded companies because they collect consumer information.

With a different focus and jurisdiction than the FTC, the SEC has plenty of room to fulfill a meaningful purpose in cybersecurity regulation. The SEC’s focus on cybersecurity measures of publicly traded companies will lead to more transparency in investment markets and may allow the FTC to focus its resources on monitoring cybersecurity measures used by companies outside the SEC’s jurisdiction.

C. Different Strategies

In action and in word, the FTC seeks to maintain “reasonableness” in its enforcement actions by considering a company’s reaction to a cybersecurity breach.\textsuperscript{46} The SEC may not be so forgiving. The Commission proved as much in its first cybersecurity enforcement action.\textsuperscript{47} Although there was no indication of financial harm to investors, the SEC censured and fined an investment firm $75,000 for violating the “safeguards rule.”\textsuperscript{48} By fining an RIC even when there was no indication of financial harm, the SEC believes it will incentivize firms to anticipate, rather than react, to cybersecurity breaches.\textsuperscript{49} Like the FTC, the SEC requires regulated entities to detect, prevent, and remediate cybersecurity faults. However, the SEC also obligates


\textsuperscript{46} Milicic & Blackburn, supra note 15.


\textsuperscript{48} U.S. SEC. AND EXCH. COMM’N, supra note 22.

\textsuperscript{49} Id.
RICs to make extensive disclosures whether a cyberattack occurred or not. An RIC’s obligation does not end with regular disclosures that outline its cybersecurity risk factors and disclosures following cyberattacks. The SEC mandates that RICs have a procedure for auditing previous disclosures to ensure their accuracy in the light of the most recent disclosure.\(^{50}\)

On balance, there are three important differences between the FTC and the SEC that make room for both of them to regulate cybersecurity. The agencies have different focuses, jurisdictions, and enforcement strategies. With both agencies regulating cybersecurity, more people are protected and consumers as well as investors will have more trust in the marketplace.

IV. ACCOUNTABILITY FOR CYBERSECURITY

The aforementioned distinctions present unique obstacles for corporations when developing internal governance procedures. Companies that fear damage to their reputation and worth by disclosing cybersecurity threats should weigh that risk against the heavy weight of the hammer awaiting those who do not comply. To comply with both FTC and SEC cybersecurity regulations, a corporation must focus on adopting a corporate structure that facilitates accuracy, accountability, and communication. Both the FTC and SEC require regulated entities to implement cybersecurity programs that contain administrative, technical, and physical safeguards.\(^{51}\) However, the agencies’ divergent focuses and enforcement techniques broaden the range of a regulated corporation’s liabilities. One breach may expose corporations to dual liability. Following a breach, the FTC might examine a company’s cybersecurity measures to determine if they were reasonably adequate. At the same time, the SEC might compare the impact of the breach with how a corporation has represented its cybersecurity measures in past and present disclosures.

A corporate governance model that creates high-speed communication avenues for alerting management to cybersecurity threats and breaches is essential to meeting SEC and FTC requirements. This model must contain a structure for monitoring cybersecurity measures and determining which breaches are material breaches. It is important that the officers who certify disclosures are adequately informed because any downplaying of cybersecurity attacks is possible grounds for a SEC enforcement action. Such a model has

\(^{50}\) Shubert et al., supra note 7, at 1.

\(^{51}\) Id.; Fed. Trade Comm’n, supra note 5.
two advantages for corporations. By increasing internal accountability, a corporation incentivizes management to stay apprised of cybersecurity measures. Additionally, as a result of customers and investors perceiving that the market is safer, revenues and stock prices may rise. Thus, the cost of such a corporate model may be offset by the returns from the sense of security it gives customers and investors.

FORREST E. LIND III*