Public Statement

Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures

Commissioner Kara M. Stein

Feb. 21, 2018

Yesterday, the Commission attempted to tackle an increasingly important issue: How should a public company tell its investors about its cybersecurity risks and incidents?[1]

Undeniably, the high-profile data losses and security breaches that have occurred across the public and private sectors show that no company or organization is immune from cyberattack. Unfortunately, one only need look back to the past eight years to see example after example of these attacks. In 2010, a sophisticated cyberattack affected more than 75,000 computer systems at nearly 2,500 companies in the United States and around the world.[2] In 2014, hackers broke into the computer systems of a major Hollywood studio, stealing confidential documents and exposing these documents and other personal information to potential cybercriminals.[3] And last year, we learned that a major cybersecurity breach at a public company may have potentially affected half of the U.S. population.[4] When the magnitude of the breach was revealed publicly, the company's stock price plummeted, losing over $5 billion in

market value.[5]

Unfortunately, the risks and costs of cyberattacks appear to be growing. And the consequences of such attacks could have devastating and long-lasting collateral effects. Cybercriminals are only becoming more cunning and sophisticated. It is estimated that cybercrime will cost businesses approximately $6 trillion per year on average through 2021.[6] Globally, the average cost of cybercrime has increased 62% over the last five years.[7] In addition, the cost of unintentional data loss—the most expensive component of a cyberattack—has risen nearly ten percent over the last three years alone.[8] Not surprisingly, public companies, investors, and other market participants increasingly view confronting and mitigating cyberrisk as a major priority.

So, what has the Commission done in response? In 2011, the staff of the Division of Corporation Finance attempted to address cyberrisks from a disclosure perspective. The staff issued disclosure guidance that discussed how public companies should disclose cyberrisks and their related impact within the existing disclosure framework.[9]

Unfortunately, despite the staff's best efforts to develop guidance that elicits robust disclosure to investors, meaningful disclosure has remained elusive. In fact, a 2014 study noted that the staff guidance "resulted in a series of disclosures that rarely provide differentiated or actionable information for investors."[10] That same year, the Commission hosted a roundtable in order to discuss the cybersecurity issues faced by various market participants, including public companies.[11] As one participant pointed out during the roundtable, a public company's disclosures are supposed to allow investors to understand a company's particular risks to better determine how a company's risk profile may differ from another company's risk profile.[12] Nevertheless, other roundtable participants observed that public company disclosures regarding cybersecurity risks and incidents were far from robust and, instead, largely consisted of boilerplate language that failed to provide meaningful information for investors.[13] Just a few months ago, the SEC's Investor Advisory Committee noted that public company disclosures regarding cybersecurity risks and incidents have not improved.[14] This is the case despite the very real increase in the number and sophistication of, and damaged caused by, cyberattacks on public companies in recent years. Members of Congress also have repeatedly called for the Commission do to more to help public companies, investors, and other market participants address cyberrisks.[15]

And so, when the Chairman put cybersecurity on the Commission's agenda, I was very supportive. Unfortunately, I am disappointed with the Commission's limited action.

Yesterday, the Commission issued interpretive guidance to assist

public companies in preparing disclosures about cybersecurity risks and incidents. This guidance reminds companies that they should consider cybersecurity risks and incidents when preparing documents that they file with the Commission, as the federal securities laws require them to disclose information about material cybersecurity risks and incidents. As this guidance describes, disclosure may be required in the context of a public company's existing reporting obligations—such as the company's risk factors, management's discussion and analysis, or financial statements. This guidance also reminds companies of the importance of maintaining comprehensive policies and procedures—including effective disclosure controls and procedures—that address cybersecurity risks and incidents. In addition, it reminds company insiders that trading securities while in possession of non-public information about cybersecurity incidents may violate the federal securities laws.

To be sure, these are all valuable reminders and raising them to the Commission level indicates a level of significance the staff guidance from seven years ago simply does not. The problem, however, is that many of these reminders were offered by the staff back in 2011. If our staff has already provided guidance regarding cyber-related disclosures, the question, then, is what we, as the Commission, should be doing to add value given seven additional years of insight and experience. Should we be, in effect, re-issuing staff guidance solely to lend it a Commission imprimatur? Will companies, their general counsels, and their boards suddenly take notice of their cyber-related disclosure obligations because of the Commission's new endorsement? Or will law firms simply produce a host of client alerts reaffirming their alerts from years past?

These questions serve to demonstrate only part of the problem. The more significant question is whether this rebranded guidance will actually help companies provide investors with comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents. I fear it will not.

I would like to highlight just a few examples of what we could have achieved in the context of disclosure:

- We could have examined what the staff has learned since the release of its 2011 guidance and provided new guidance that capitalized on these findings. After all, the staff of the Division of Corporation Finance reviews hundreds of public company filings every year. The staff also reviews hundreds of shareholder proposals each year, many of which have been increasingly calling on companies to provide more effective cyber-related disclosure.
- We could have discussed the various advances in technology used in cyberattacks since 2011, and how such advances could affect a company's disclosure

regarding company-specific risks.

- We could have considered the suggestions from some of our leading commenters, including academics and practitioners. We could have, for example, considered some of the recent Investor Advisory Committee Subcommittee's preliminary suggestions,[16] and discussed the value to investors of disclosure relating to:
    - a company's protocols relating to, or efforts to minimize, cybersecurity risks and its capacity, and any measures taken, to respond to cybersecurity incidents;
    - whether a particular cybersecurity incident is likely to occur or recur; or
    - how a company is prioritizing cybersecurity risks, incidents, and defense.
- We could have discussed the value to investors of disclosure regarding whether any member of a company's board of directors has experience, education, expertise, or familiarity with cybersecurity matters or risks. And, if not, why the company believes that board-level resources are not necessary for the company to adequately manage its cybersecurity risks.

The list goes on. In effect, we could have helped companies formulate more meaningful disclosure for investors. Instead, yesterday's guidance provides only modest changes to the 2011 staff guidance.

Some would say that the Commission is confined in what it can do in the context of guidance, without engaging in a formal rulemaking. I agree. I believe it is important for the Commission to be mindful of the guidance it or its staff produces that may be tantamount to rulemaking.[17]

That is why, as I have remarked before, it is imperative that the Commission do more.[18] As we have heard from a variety of commenters since the 2011 staff guidance, guidance, alone, is plainly not enough. This makes it all the more confusing that the Commission more or less reissued that very guidance. Simply put, seven years since the staff guidance was released, despite dramatic increases in cyberattacks and their related costs, there have been almost imperceptible changes in companies' disclosures. This to me strongly suggests that guidance alone is inadequate.

Yet, the Commission has ignored pleas from issuers, investors, market participants, and members of Congress to do more. And we could have done so much more. For example:

- We could have sought notice and comment on proposed rules that address improvements to the board's risk

management framework related to cyberrisks and threats. Too many companies currently fail to consider cybersecurity as a business risk and, thus, do not incorporate it within the risk management framework overseen by their boards. These proposed rules could address current weaknesses in the nature, timing, and extent of disclosure to investors.

- We could have sought notice and comment on whether the Commission should establish minimum standards to protect the personally identifiable information of investors and whether such standards should be required for key market participants, such as broker-dealers, investment advisers, and transfer agents.[19]
- We could have sought notice and comment on proposed rules that would require a public company to provide notice to investors (*e.g.*, a Current Report on Form 8-K) in an appropriate time frame following a cyberattack and to provide disclosure that is useful to investors, without harming the company competitively.
- We could have sought notice and comment on whether the Commission should issue rules that are more programmatic and that would require a public company to develop and implement cybersecurity-related policies and procedures beyond just disclosure.

I recognize that in our current Digital Age, these matters are complicated. But this cannot be the reason we do not engage. We should proceed, and engage investors, market participants, and pubic companies through notice and comment rulemaking in order to get their best thoughts.[20]

In conclusion, it is hard to disagree with the Commission emphasizing the importance of the disclosure of cybersecurity risks and incidents. As a result, I supported the Commission's guidance, but not without reservation. While it may have the potential of providing both companies and investors with incremental benefit, the guidance does not sufficiently advance the ball—even in the context of disclosure guidance. Even more, it may provide investors a false sense of comfort that we, at the Commission, have done something more than we have.

Ultimately, the step the Commission took with respect to cybersecurity risks and incidents should only be its first. There is so much more we can and should do. I hope we will proceed accordingly for the good of investors, public companies, and our capital markets.

---

[1] As we all know, fundamental to the federal securities laws is the principle that public companies disclose information to allow investors to make informed investment decisions. This means

that public companies must disclose, among other things, risks and events that a reasonable investor would consider important. And depending on the company and its particular facts and circumstances, this could mean disclosure relating to cyber risks.

[2] *See* Ellen Nakashima, "More than 75,000 computer systems hacked in one of largest cyberattacks, security firm says," *The Washington Post* (Feb. 18, 2010), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html .

[3] *See* Andrea Peterson, "The Sony Pictures hack, explained," *The Washington Post* (Dec. 18, 2014), *available at* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.5b8531b2bf8f .

[4] *See* Victor Reklaitis, "Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap," *MarketWatch* (Sept. 14, 2017), *available at* https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14 .

[5] *Id.*

[6] *See* Nick Eubanks, "The True Cost Of Cybercrime For Businesses," *Forbes* (Jul. 13, 2017), *available at* https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#6c0453c44947

[7] *See* Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference, Accenture (2017), *available at* https://www.accenture.com/t00010101T000000Z__w__/fr-fr/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf .

[8] *See* Path to cyber resilience: Sense, resist, react, EY's 19th Global Information Security Survey 2016-17, Ernst & Young LLP, *available at* http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf .

[9] CF Disclosure Guidance: Topic No. 2, Cybersecurity, Division of Corporation Finance (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[10] *See* What investors need to know about cybersecurity: How to evaluate investment risks, Investor Responsibility Research Center Institute (Jun. 2014), *available at* https://irrcinstitute.org/wp-content/uploads/2015/09/cybersecurity-july-20141.pdf .

[11] *See* Cybersecurity Roundtable, U.S. Securities and Exchange Commission (Mar. 26, 2014), *available at*

https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[12] *See* Transcript, Cybersecurity Roundtable, U.S. Securities and Exchange Commission (Mar. 26, 2014), *available at* https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

[13] *Id.*

[14] *See* "Discussion Draft Re: Cybersecurity and Risk Disclosure," Investor as Owner Subcommittee, SEC Investor Advisory Committee (Dec. 2017) ("IAC Discussion Draft"), *available at* https://www.sec.gov/spotlight/investor-advisory-committee-2012/discussion-draft-cybersecurity-disclosure-iac-120717.pdf.

[15] *See, e.g.*, Letter from Congressmen Jim Langevin and Jim Himes, Members, Committee on Homeland Security, Cybersecurity, Infrastructure Protection, and Security Technologies, to Mary Jo White, Chair, U.S. Securities and Exchange Commission (Jun. 17, 2015), *available at* http://langevin.house.gov/sites/langevin.house.gov/files/documents/06-17-15_Langevin_Himes_Letter_to_SEC.pdf.

[16] *See* IAC Discussion Draft.

[17] *See, e.g.*, Commissioner Kara M. Stein, Statement on the Staff's No-Action Relief Regarding MiFID II (Oct. 26, 2017), *available at* https://www.sec.gov/news/public-statement/statement-stein-2017-10-26.

[18] *See* Commissioner Kara M. Stein, "Mutualism: Reimagining the Role of Shareholders in Modern Corporate Governance," Remarks at Stanford University (Feb. 13, 2018), *available at* https://www.sec.gov/news/speech/speech-stein-021318.

[19] *See* Chair Mary Jo White, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014), *available at* https://www.sec.gov/news/public-statement/spch112014mjw ("I have directed the staff to prepare recommendations for the Commission's consideration as to whether an SCI-like framework should be developed for other key market participants, such as broker-dealers and transfer agents.")

[20] *See* Steven T. Mnuchin & Craig S. Phillips, U.S. Dep't of the Treasury, A Financial System That Creates Economic Opportunities: Capital Markets 219 (Oct. 2017), *available at* https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-Capital-Markets-FINAL-FINAL.pdf ("Treasury recommends that the CFTC and the SEC take steps to ensure that guidance is not being used excessively or unjustifiably to make substantive changes to rules without going through the notice and comment process.").