University of Georgia Law

Journal of Intellectual Property Law

Volume 25 | Issue 2 Article 4

October 2018

Cybersecurity, Shareholders, and the Boardroom: An Analysis of Current and Proposed Measures for Protecting Corporate Intellectual Property

Kathryn V. Wymer
University of Georgia School of Law

CYBERSECURITY, SHAREHOLDERS, AND THE BOARDROOM: AN ANALYSIS OF CURRENT AND PROPOSED MEASURES FOR PROTECTING CORPORATE INTELLECTUAL PROPERTY

Kathryn V. Wymer[*]

[*]J.D. Candidate, 2019

I. INTRODUCTION

The zeitgeist of the digital era is so pervasive that it renders explicit observation of corporate technological dependence redundant: it is universally true that large corporations electronically store an overwhelmingly large amount of valuable data on internet-connected computer networks.[1] Electronically-stored intellectual property (IP) and intangible assets relating to sales, planning, research and development, finance, and clientele each comprise a significant portion of corporate assets.[2] Studies and common sense both dictate that this paradigm of electronically-based business is only strengthening. A recent analysis of S&P 500 companies revealed that 83% of corporate market value was comprised of tangible assets in 1975.[3] By 1995, this figure fell to 32%; by 2015, 16%.[4] A corporation in any industry, whether traditionally IP-intensive or not, will likely owe its success to any or all types of IP: trademarks, design rights, copyrights, patents, trade secrets, and information stored in confidential databases.[5] Both derivative of and influential on these traditional corporate intellectual properties are a corporation's goodwill and reputational capital, the portion of excess market value attributed to the perception of a firm as a responsible corporate citizen.[6] This goodwill and reputational capital create brand appeal that is often as important to sales as quality or price in determining ultimate success; a favorably-recognized brand is one of the most valuable assets a company can own.[7] This asset is particularly valuable for corporations whose products or services lack sophisticated technology that can be protected through patents or copyrights as well as corporations that operate in industries with relatively low barriers to entry.[8] For example, the reputational capital of CocaCola has been estimated at $52 billion, Gillette at $12 billion, and

[1] Sam Young, Note, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 660 (2013).

[2] *Id.*

[3] Shilpa Andalkar, *Finding the 84% of Stock Market Value that Most Investors Ignore*, EQUITIES.COM: NEWS, (Apr. 17, 2015), https://www.equities.com/news/finding-the-84-of-stock-market-value-that-most-investors-ignore.

[4] *Id.*

[5] KEITH WITEK, *Intellectual Property Strategy: Creation and protection of the corporate identity,* 2 INTERNET LAW AND PRACTICE § 21:2 I (2017).

[6] Joseph A. Petrick & John F. Quinn, *The Integrity Capacity Construct and Moral Progress in Business*, 23 J. BUS. ETHICS 3, 15(2000).

[7] *Brands – Reputation and Image in the Global Marketplace* (World Intell. Prop. Rep. (2013), http://www.wipo.int/edocs/pubdocs/en/intproperty/944/wipo_pub_944_2013.pdf.

[8] WITEK, *supra* note 5.

Campbell's at $9 billion, illustrating the immense value and importance corporations should and do place on promoting and protecting their public perception.[9]

Given the vast amount of corporate value stored electronically, it is unsurprising that cybersecurity incidents that compromise corporate data are increasingly damaging and frequent.[10] James Comey, former Director of the Federal Bureau of Investigation, recently observed there were two types of companies: those who have been hacked and those who do not know they have been hacked.[11] Though this observation may be a slight exaggeration, it is not far removed from reality: Comey proceeded to very seriously posit that the cybersecurity threat to the United States will soon surpass that posed by international and domestic terrorism.[12]

These infamous and increasingly frequent cybersecurity attacks directly impact the corporate reputational capital, which devalues corporate intellectual property.[13] In a recent study of sixty-five companies affected by cybersecurity hacks since 2013, two-thirds saw an adverse impact with an average long-term decline of 1.8% and at worst 15% in value.[14] This is particularly pertinent with retailers; a recent study revealed that after revelation of a cybersecurity breach, 12% of "loyal" customers no longer shop at the retailer and 36% shop there less frequently.[15] With corporate identity of goodwill and reputation carrying such a high economic value, it is unsurprising why companies both with and without traditional IP assets spend millions of dollars annually on cybersecurity protection.[16]

---

[9] *Id.*

[10] Roberta S. Karmel, *Disclosure Reform – The SEC is Riding Off in Two Directions at Once*, 71 BUS. L. 781, 810 (2016).

[11] *See* James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct 6, 2014), www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (quoting then-FBI Director James Comey on CBS program *60 Minutes*, "[t]here are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.").

[12] *Homeland Threats and Agency Responses Hearing Before the S. Comm. n Homeland Security & Gov't Affairs*, 113th Cong. 59 (2013) (statement of Hon. James B. Comey, Jr., Former Director, Federal Bureau of Investigation).

[13] Deloitte, *Security Attacks: A Lead Driver of Reputation Risk*, WALL ST. S. RISK & COMPLIANCE J. (Jan. 21, 2015, 12:01am), deloitte.wsj.com/riskandcompliance/2015/01/21/security-attacks-a-lead-driver-of-reputation-risk/.

[14] Matthew Heller, *Cyber Attacks Can Cause Major Stock Drops*, http://www.CFO.COM (Apr. 12, 2017), http://ww2.cfo.com/ cyber-security-technology/2017/04/cyber-attacks-stock-drops/.

[15] Kate Vinton, *How Companies Can Rebuild Trust After a Security Breach*, FORBES (July 1, 2014, 9:29am),http://www.Forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/#48b40bc35e6c.

[16] Jonathan Vanian, *Here's How Much Business Worldwide Will Spend on Cybersecurity by 2020*, FORTUNE (Oct. 12, 2016), fortune.com/2016/10/12/cybersecurity-global-spending/.

Though cybersecurity breaches often result in devaluation of corporate assets, this value can often rebound quite rapidly if met with appropriate corporate responses.[17] Customers typically respond well to humility, transparency, and timely responses to breaches, which are corporate practices that can be provided for with sufficient foresight and preparation.[18] In some cases, a scintilla of corporate response can assist in a rebound. For example, the former Chief Executive Officer of Equifax recently testified before the House Energy and Commerce Committee on the credit reporting bureau's 2017 hack of nearly one hundred and fifty million Americans' sensitive data.[19] Though the corporation's stock declined dramatically upon the revelation of the breach, it saw its third-largest gain of 2017—3.9%, resulting in a market value increase of $500 million—by the end of the testimony.[20] Clearly, market value hinges on corporate response to cybersecurity breaches.

Our government officials, corporate leaders, and consumers are all concerned with the increasing threat of cybersecurity breaches. In the Equifax testimony, many Senators expressed incredulity over the corporation's executives' responses, with one Texas Senator Green comparing the continuing operation of Equifax to that of a restaurant with a failing health inspection remaining open.[21] In a recent study, Information Systems Audit and Control Association (ISACA), an international professional association focused on information technology (IT) governance, found that loss of enterprise intellectual property was the greatest concern amongst corporate leaders when asked of the top risks of a cybersecurity breach.[22] As previously explained, consumers respond to breaches with their wallets, directly impacting corporate value.[23]

All of these concerns are compounded and expanded upon in investor concern. After the September 2017 disclosure of a cyberattack on Equifax that harmed nearly 43% of the entire U.S. population, Equifax's stock fell by 18% as individuals both affected and unaffected lashed out against the corporation in anger—the very entity that was supposed to protect their identities had exposed them to the world.[24] Max Wolff, chief economist at Disruptive Technology Advisors, commented that because of the sensitive nature of this security breach,

---

[17] Vinton, *supra* note 15.

[18] *Id.*

[19] Jennifer Surane, *Equifax is Worth $500 Million More After Ex-CEO Faces Congress*, BLOOMBERG TECH. (Oct. 3, 2017, 2:26 pm), https://www.bloomberg.com/ news/ articles/ 2017-10-03/equifax-s-lashing-in-congress-ends-with-company-up-500-million

[20] *Id.*

[21] *Id.*

[22] Information Systems Audit and Control Association, *New Cobit 5 Guide Identifies Top Three Cybersecurity Game Changers*, 2013 WL 12090166 (2013).

[23] Vinton, *supra* note 15.

[24] Surane, *supra* note 19.

this breach in particular will dramatically impact how investors feel about cybersecurity and disclosure.[25] As cybersecurity incidents become more prevalent, the trend is shifting away from investors' concern being sparked by an incident and towards a proactive concern upon making an investment in a corporation.[26] Cybersecurity vulnerabilities and threats, as well as corporate policies relating to prevention and response of attacks, are becoming key questions for today's investors.[27] Currently, shareholders lack sufficient information on cybersecurity incidents and "tools to measure their impact."[28] In fact, the declines in corporate value we see after a cybersecurity breach actually dramatically underestimate the harm done to the value of the company. This is largely because the long-term effects of a data breach are difficult to quantify: lost intellectual property, sensitive data, and customer confidence are all highly likely to occur but difficult to capture in a stock price.[29] As such, shareholder reactions to cybersecurity breaches up until recently have largely consisted of knee-jerk reactions to dramatic breaking news of the breach and direct impact on business operations that immediately affect a corporation's known property.[30] Because of a lack of information (and sometimes misinformation), it is almost impossible for shareholders to assess the very real implications of a cybersecurity breach.[31]

The prominence and severity of cybersecurity breaches and resulting financial risks have increasingly pervaded conversations on corporate governance and securities regulation for the past decade.[32] Today's corporate environment has become increasingly compliance-focused, highlighting the need of effective disclosure and regulation to detect, monitor, and fix systemic corporate problems.[33] The United States is particularly and notoriously susceptible to cyberattacks because of the high number of insufficient networks and the presence of immensely valuable intellectual property.[34] Despite this, relatively little has been done to increase required disclosure of cybersecurity threats and regulate the response to them. The Dodd-Frank Wall Street Reform and

25 Rebecca Ungarino, *The Equifax breach aftermath could cause all investors to ask tough new questions* (CNBC, Sept. 12, 2017, 6:22pm), https://www.cnbc.com/2017/09/12/equifax-breach-may-push-investors-to-ask-tough-cybersecurity-questions.html.

26 *Id.*

27 *Id.*

28 Elena Kvochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV. (2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

29 *Id.*

30 *Id.*

31 *Id.*

32 Karmel, *supra* note 10.

33 Jennifer M. Pacella, Note, *The Cybersecurity Threat: Compliance and the Role of Whistleblowers*, 11 BROOK. J. CORP. FIN. & COM. L. 39, 40 (2016).

34 Scott J. Shackleford, *Protecting Intellectual Property and Privacy in the Digital Age: the Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAP. L. REV. 445, 446 (2016).

Consumer Protection Act, the most sweeping piece of legislation in securities regulation in recent times, did not contemplate cybersecurity disclosures because it was not until the bill became law in 2010 that these issues took center stage. Cybersecurity simply became an issue too late to be fully contemplated by the bill's authors.[35] As such, the current environment mandates a second look at corporate securities regulation as it relates to the greatest threat to corporations today.

II. BACKGROUND

A. DISCLOSURE FRAMEWORK

The U.S. Securities and Exchange Commission's (SEC) mission is "to protect investors; maintain fair, orderly, and efficient markets: and facilitate capital formation."[36] Primarily, the SEC "strives to promote a market environment that is worthy of the public's trust."[37] To fulfill this mission, the agency requires companies seeking investors in their securities to disclose certain information on their business, the securities they sell, and the risks involved in buying those securities.[38]

Two acts are of central importance in the regulation of securities. The Securities Act of 1933 (Securities Act) requires any corporation to make full disclosure of its business and affairs prior to offering a security for sale.[39] The Securities Act, passed in response to the 1929 stock market crash, provided corporations with a specified list of disclosure items.[40] The Securities Act of 1934 (Exchange Act) initially required companies under the Securities Act to make annual and periodic disclosures to encourage continued disclosure to investors.[41] Later amendments expanded its jurisdiction to all corporations, whether they were in the purview of the Securities Act or not, with $1 million in assets and five hundred shareholders.[42] This was later expanded yet again, and

[35] *See* Karmel, *supra* note 10.

[36] U.S. SECURITIES AND EXCHANGE COMMISSION: *About the SEC* (Last Modified Dec. 26, 2017), https://www.sec.gov/about.shtml.

[37] *Id.*

[38] *The Role of the SEC*, INVESTOR.GOV, https:/ /www.investor.gov/introduction-investing/basics/role-sec (last visited Apr. 25, 2018).

[39] 15 U.S.C. § 77a(1933). *See also Federal regulation of publicly traded companies*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, https://www.rcfp.org/sunshine-inc/federal-regulation-publicly-traded-companies (last visited Apr. 25, 2018)

[40] *Federal regulation of publicly traded companies, supra* note 39.

[41] 15 U.S.C. § 78a(1934). *See also Federal regulation of publicly traded companies, supra* note 39.

[42] *Federal regulation of publicly traded companies,* supra note 39; Karmel, *supra* note 10, at 784.

currently stands at companies with $10 million in assets and either 2,000 shareholders or 500 shareholders who are not accredited investors.[43]

Regulation S-K, under the Securities Act, provides public companies with the substantive disclosures they must make regarding their businesses, operations, and governance structures.[44] The standard for disclosure is "materiality"; this has been defined by case law as that information which (1) has a substantial likelihood that a reasonable investor would attach importance to the information in determining how to vote and (2) alters the "total mix" of information on the security.[45] Line-item disclosures required by the S-K, however, "are mandated and do not depend on an independent judgment by registrants as to their materiality" to shareholders.[46] Instead of limiting the information that must be provided on the S-K, the materiality standard increases the burden of the S-K by requiring that the corporation go beyond its requirements, providing material information "as may be necessary to make the required statements, in light of the circumstances . . . not misleading."[47] The tests of materiality have been defined as "a substantial likelihood that a reasonable shareholder would consider it important " and that a reasonable shareholder would "consider it important in deciding how to vote."[48]

The SEC traditionally "interpreted materiality to mean economic materiality, but sometimes more qualitative measures have crept into SEC standards," creating a much stronger regulatory environment.[49] One important example of this trend is the SEC's view regarding disclosure of corporate governance. In *Franchard Corp.*, the SEC, acting under its adjudicatory powers, found disclosure of "management integrity" to be material to shareholders.[50] As a result, the SEC required full disclosure on the composition of the individuals serving on corporate boards, including details on the independence of each of the corporate directors sitting on the board.[51] The Sarbanes-Oxley Act codified and expanded upon these requirements, including a mandatory code of ethics and executive and external accountant attestations of financial statements and internal controls.[52] These attestation requirements "remain in force for large public" corporations.[53]

---

43 *Id.*

44 17 C.F.R. § 229 (2017).

45 *See* Karmel, *supra* note 10, at 785-88.

46 *Id.* At 786

47 17 C.F.R. §§ 230.408, 240.12b-20 (2015).

48 TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976)

49 *See* Karmel, *supra* note 10, at 786.

50 *Franchard Corp.*, 42 S.E.C. 163, 170 (July 31, 1964).

51 *Id.*

52 Sarbanes-Oxley, 15 U.S.C. 7262 (2012).

53 *See* Karmel, *supra* note 10.

Current disclosure requirements are very complicated due to "changing business realities and new capital market practices."[54] S-K and S-X primarily embody the disclosure regime, but disclosure policies are "scattered throughout SEC forms, interpretive releases, no-action letters, and comment letters."[55]

The current regulatory trend of SEC disclosure requirements features a bifurcated trend of some calling for deregulation and simplification of over-burdensome disclosures while others call for more extensive disclosures to ensure a more efficient, fair market.[56] Those who support increased reform typically seek to reform corporate conduct and practice and prevent past failures by forcing corporations to reveal more information to investors.[57] Proponents of this school of thought believe that when issues are placed squarely in front of the board they will be more efficiently and adequately addressed due to the risk of losing potential investors who are displeased rather than leaving them to the discretion of corporate boards who may decide to avoid certain issues in hopes of investor indifference or ignorance.[58] On the other hand, opponents view these measures as costly and unnecessary, flooding largely passive, uneducated investors with superfluous information while costing corporations enormous amounts of money that do not justify the marginal benefits.[59] While these arguments raise valid concerns, the prevailing school of thought in the regulatory environment endorses increased disclosure of cybersecurity threats and responses, given its prevalence in the news.

B. CURRENT STATUS OF CYBERSECURITY IN DISCLOSURE REQUIREMENTS

Many companies already disclose cybersecurity-related matters , even though current line-item disclosures do not explicitly require it, because they believe it prudent to do so..[60] The materiality standard of required disclosures holds that companies must disclose information that a reasonable investor would find necessary to vote, and change the "total mix" of information. Oftentimes corporations in industries very sensitive to cybersecurity threats, like those in IP-intensive industries or who store the vast majority of their assets digitally, will feel shareholders are entitled to full disclosure under this standard.[61]

In recent years, the SEC has centered its cybersecurity focus on "(1) governance and risk assessment; (2) access rights and controls; (3) data loss

54 *Id.*

55 *Id.*

56 *Id.* at 790.

57 *Id.*

58 *See generally* Karmel, *supra* note 10.

59 *See id. at 810-813*

60 *Id.*

61 *See id.* at 787, 810-813

prevention; (4) data management; (5) training; and (6) incident response."[62] In so doing, the commission has made it abundantly clear that cybersecurity risks, preventative measures, and response strategies should, in most circumstances, be disclosed to investors, but has not explicitly required any line-item disclosures.[63] In related disclosure guidance most recently promulgated in 2011, the SEC provided corporations with various recommendations for disclosing cybersecurity risk factors, management discussion and analysis, description of business, legal proceedings, and financial statement disclosures.[64] These guidelines seek to balance the need for accurate information and fully informed investors with the barrage of unnecessary and overwhelming information that could result if investors are provided with every technical cybersecurity fact that they likely will not understand.[65] Many corporations remain confused on what exactly to disclose to investors, often simply looking to other, similarly-situated companies in their industry to ascertain how much detail their peers provide in complying with this "industry standard," essentially establishing a "first mover" standard for adequate disclosure.[66] As cybersecurity threats become more prevalent, damaging, and varied across all industries, these disclosure requirements need to be solidified and clarified.

If past practice is an indicator, however, "the SEC will resist both efforts to increase or decrease the disclosure burden of public companies unless new laws force it to do so"; the cost of imposing new regulations is high and can generate significant resistance and outrage amongst entities subject to the new regulation.[67] As cybersecurity threats become an increasing risk, new laws from Congress must force the SEC's hand in underscoring the importance of full disclosure of cybersecurity-related matters to investors.

---

[62] *Observations from Cybersecurity Examinations* OFFICE OF COMPLIANCE INSEPCTIONS AND EXAMINATIONS (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[63] Amy Terry Sheehan, *Meeting Expectations for SEC Disclosures of Cybersecurity Risks and Incidents*, 1 CYBERSECURITY LAW REPORT 10, (Aug. 12, 2015), https://www.davispolk.com/files/agesser.Cybersecurity.Law_.Report.aug15.pdf

[64] U.S. SECURITIES & EXCHANGE COMMISSION: *Division of Corporate Finance Disclosure Guidance: Topic No.2: Cybersecurity*, (Oct. 13, 2011), https:// www.sec.gov/ divisions/ corpfin/ guidance/cfguidance-topic2.htm.

[65] *See* Sheehan, *supra* note 63 at 1.

[66] *Id.* ("It is also prudent practice to stay in line with the disclosures of similarly situated companies in the same industry").

[67] Karmel, *supra* note 10, at 783.

C. CURRENT LEGISLATION REGARDING REGULATING CORPORATE CYBERSECURITY

Recent legislation has attempted to place the responsibility of cybersecurity with boards of directors.[68] The Cybersecurity Disclosure Act of 2017, introduced in the Senate on March 7, 2017, would require publicly-traded companies to disclose whether any member of their board has cybersecurity expertise. If no member does, the act requires the company to explain why this expertise is unnecessary due to other steps taken by the company.[69] Essentially, this means that every board must have a cybersecurity expert on it, and if it doesn't, it has to explain why it doesn't need one. The bill does not define cybersecurity expertise, but instead directs the SEC to do so.[70]

III. ANALYSIS

A. ADEQUACY OF CURRENT PROPOSAL

This legislation is a step in the right direction towards forcing corporations deal with cybersecurity issues by forcing the issues squarely into the boardroom, but its aim is off—or, at least, not properly centered. The bill demands "cybersecurity expertise," whatever that means, on the board, but essentially lets the corporation off the hook for thorough disclosure to shareholders of risks, incidents, responses, and preventative measures. This approach dismisses shareholder concern with a simple "we have an expert," thus requiring the shareholders to blindly trust the undefined "expertise" of just one individual on the board. Certainly, requiring board members to be aware of cybersecurity issues is important, but further regulation is necessary to ensure that the company as a whole adequately protects its intangible assets, and that shareholders are fully informed of the measures designed to do so. Merely forcing a corporation to change the composition of its board may enhance the board's quality, but it does not address the fundamental issue at hand: the need for corporations to allocate resources and attention to the risks they are facing.[71] This is because, ultimately, it is not the board's job to handle the daily management of cybersecurity; after all, board members do not necessarily need the expertise themselves in order to direct employees to take preventative measures or obtain third-party assessment

[68] Daniel B. Garrie, David Lawrence & Yoav M. Griver, *Cybersecurity Disclosure Act: A Misguided Attempt to Effectively Address Cyber Threats*, 20 NO. 5 WALLSTREETLAWYER.COM: SEC. ELECT. AGE NL 2 (2016).

[69] S. 536, 115th Cong. (2017–2018).

[70] *Id.*

[71] Garrie, Lawrence & Griver, *supra* note 68.

of their cybersecurity risks.[72] Of course, this is not to say enhanced knowledge of cybersecurity matters would not help the board and corporation in some ways, but it certainly will not certainly settle the issue if additional regulations are not required.[73]

B. PROPOSED INCREASED REGULATION OF CORPORATE CYBERSECURITY MATTERS

Cybersecurity threats are so important to full disclosure that they should be a separate line-item disclosure, not simply covered vaguely by the materiality standard. The increasing risks and severity of cybersecurity attacks require that they take a more prominent, distinct, and separate position in the securities regulation process. Investors in this era of pervasive digital dependence should be able to rest assured that they will be provided with information concerning the corporation's cybersecurity threats, preparedness, and response strategies, without having to request the information under the materiality standard or rely on a single individual on the board's expertise with the matter.

As such, the Cybersecurity Disclosure Act of 2017, if reintroduced in a similar form, should have additional requirements; the current bill could certainly be helpful in ensuring increased cybersecurity measures, but it is simply insufficient as-is to combat the current crisis on its own. First, the bill itself should define what is meant by "cybersecurity expertise," or at least promulgate guidance on the subject. To that end, it should be required that this expertise involves some past experience in handling risks, prevention, and responses to cybersecurity attacks, rather than simply allowing experience in a digital- or tech-based company to suffice. This will ensure that the board can put the "expertise" to effective use. It would also be very helpful for a board member to have the ability to delegate cybersecurity-related tasks to officers, coming from a place of experience with prevention and response, rather than merely having a working knowledge, for example, of how a cybersecurity attack would work.

Second, it would be helpful to require more than one board member to have the cybersecurity expertise. The law should require at least two board members to have cybersecurity expertise; or, in the alternative, the law could require a certain percentage of the board to have such expertise. The former would allow for some discussion between "experts" on the appropriate cybersecurity procedure to implement within the corporation, rather than just a single expert working in a silo and delegating instructions on how to best handle cybersecurity issues. The latter could also allow for this dialogue to take place in corporations

[72] *Id.*

[73] *Id.*

with larger boards, without overburdening a small board with having to fill all of its seats with so-called "cybersecurity experts."

Finally, and of greatest importance, is the external auditing of cybersecurity issues. This is a necessary step to assure investors that the corporation has taken the appropriate steps to secure its digital assets and has appropriate steps in place to respond to a potential threat, without publicly divulging too much information on exactly what steps it has taken. Clearly, a major risk in the disclosure of cybersecurity-related matters is over-exposure of details that may, in turn, lead to an increased risk of a threat. A corporation cannot be expected to divulge all of its perceived risks, measures, and response practices to its investors without also divulging it to individuals who will seek to use it to implement the very attack the company is trying to prevent.

As such, corporations should be required to undergo auditing of cybersecurity practices by a third party, independent auditor, in the same manner required for corporate financials by the Sarbanes-Oxley Act.[74] Just like auditors under Sarbanes-Oxley, these auditors should be overseen by the Public Company Accounting Oversight Board (PCAOB), which was established by the Act to ensure the independency and adequacy of the auditors, outline specific procedures and processes for compliance with audits, inspect and police the audit, and enforce compliance with the specific requirements of the Act.[75] This organization should be augmented, by statute, to explicitly include cybersecurity audit procedures and oversee the process of the public corporations it currently regulates.

C. LIKELY CORPORATE RESPONSE

New line-item disclosure, increased board make-up requirements, and additional auditing requirements will inevitably met with some hostility from industry actors: all of these proposals will undoubtedly cost corporations large sums of money to comply. By analogy, suggestions to require disclosure of certain trending social responsibility issues (i.e., sustainability, fair labor practices abroad, etc.), for example, have been met with an uproar from corporations about the heavy burden they impose on the industry.[76] Cybersecurity, however, fits much more squarely within the traditional investor protection concerns.[77] Unlike other required disclosures, which are often SEC responses to pressure to "do something" about a hot-button problem in corporate governance, disclosure

[74] Mark S. Bergman, *Congress Passes Accounting Reform and Corporate Governance Legislation*, 8 NO. 20 ANDREWS DERIVATIVES LITIG. REP. 10, 2002.

[75] *About the PCAOB,* PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD, https://pcaobus.org (last visited Apr. 25, 2018).

[76] *See generally* Karmel, *supra* note 10.

[77] *Id.* at 810-813.

of cybersecurity measures is key to full disclosure, given the seriousness and increasing prevalence of breaches. This is not a "trendy" problem that will solve itself; it must be met swiftly and effectively.

IV. CONCLUSION

One cannot visit any news website today without finding a breaking story on cybersecurity. Whether it is consumer outcry over a recent breach, corporate outcry over the impossibility of solving the problem, or the government clamoring for a fix, the conversation pervades today's business and national security concerns. Though the topic of cybersecurity as an element of securities regulation has been thoroughly discussed in these settings, and many suggestions have been posed as to how to solve the problem, it seems that we are currently placated by puttering around discussing possible solutions rather than implementing one. These discussions point us in the right direction, i.e. towards increasing the importance of cybersecurity disclosure, but they need to go even further in requiring corporations to deal with the issue as quickly and effectively as possible.

Current proposals, such as the Cybersecurity Disclosure Act of 2017, are beneficial in that they bring the conversation of the corporate cybersecurity crisis into Congress. However, these attempts fall short of what is actually demanded by the situation. Instead of forcing corporations to appropriately allocate resources to their individual and unique cybersecurity needs, the Act merely changes board composition, allowing a corporation to avoid all other disclosure by having an ill-defined "expert" on the board. This is beneficial in that it places the issue in the boardroom for immediate attention, but in practice would not be an effective way at solving the issues immediately and imminently facing corporate America.

Instead, corporations must be forced to deal with the issues by legislation requiring a more Sarbanes-Oxley-esque required disclosure of their cybersecurity issues. Public corporations should be required to disclose cybersecurity as a separate line-item on disclosures statements, rather than being given the option to disclose it under a materiality standard; legislation should require clear definitions of "cybersecurity expertise" that involve true experience with risk prevention and damage control, and require more than one board member have this expertise; and corporations should be required to enlist in the aid of an external, federally-regulated auditor to ensure the corporation is aware of the risks it faces, that appropriate measures are in place to prevent an attack, and that the company is prepared to respond appropriately should one occur. Though there will undoubtedly be corporate pushback, the benefits that will come from a more carefully regulated economy regarding cybersecurity will dramatically outweigh the costs, encouraging investment and national security.