HONING IN ON HARDWARE: DATA SECURITY CONCERNS OF LARGE COMPANIES

*Nicholas Bartlett**

INTRODUCTION

Imagine for a moment that you are interested in computers, and you purchase a couple of old used servers from a company. Once you get home and access the servers, you notice that one of them is completely full of sensitive consumer information. This includes names, addresses, contact information, etc. A few questions should circle your mind at that point. "What do I do now? How did this happen?" Well, in 2006, this actually occurred.[1] Mark Morris, self-described used computer dealer, claimed to have found sensitive data on servers from Ernst & Young.[2] Morris wanted to be paid to remove the data which should have been wiped before he came into possession of the servers, but Ernst & Young simply wanted the servers returned to them. This conflict unsurprisingly resulted in legal proceedings.[3]

This event raises a significant issue: hardware security. Much of the news today revolves around data breaches that occur from hackers or people intruding networks remotely. The general public does not hear much about events like the scenario described above, where someone discovers a server that was not properly disposed of by the company. There are a few possibilities for why this is rarely known, but it is still an important aspect of data security that should be handled with competence. Failure to competently secure company data on hard drives may result in liability either from federal or state securities laws or common law fiduciary duties. The aftereffects of incompetence can be just as destructive as a remote security breach. Hefty fines can be issued if the information was required by law or industry standard to have been retained by the company. Further, the information may end up in the wrong hands. Morris was allegedly receiving offers to purchase the information on the purchased servers for up to $1.2 million.[4] It

* Nicholas William Bartlett is a recent graduate of The University of Toledo College of Law. He wishes to thank Professor Eric Chaffee for supervising his note. He also would like to thank his Note and Comment Editor, Erin Kelly, and past Editor in Chief, Lindsey Self for their guidance through the writing process. Finally, and perhaps most importantly, the author would like to thank his family and close friends for their unwavering support.

1. Ellen Messmer, *Ernst & Young Accused by Canadian Used Computer Dealer of Data Breach*, NETWORKWORLD (Sept. 9, 2014, 2:18 PM), https://www.networkworld.com/article/2604411/ernst-and-young-accused-by-canadian-used-computer-dealer-of-data-breach.html.

2. *Id.*

3. *Id.*

4. *Id.*

would not be at all shocking for a court to be harsher on a company who negligently handles their hardware when the entity has complete, direct control over the process as opposed to a data hack by an outsider.

While most of the focus in the cybersecurity context today revolves around protecting the intangible data, directors need to pay equal attention to the physical devices this data is stored on. The Securities Exchange Commission (SEC) should be issuing further guidance specifying this need. This guidance should look similar to state statutes that require companies to develop comprehensive data security practices and procedures.

While many legal scholars have recently focused on liability resulting from data breaches, this note focuses exclusively on hardware and what the SEC should be doing to guide corporations. Specifically, this note will provide a more nuanced look at how large companies should be treating their physical hardware, i.e., servers, hard drives, and the like.

This note will examine what cybersecurity is and the related issues facing companies today. It will then transition to an elaboration on fiduciary duties and their relation to cybersecurity incidents and hardware concerns. A discussion of current federal and state laws will follow, along with examples of guidance from other organizations. Finally, the conclusion will provide a recommendation of how hardware security should be emphasized and what may be missing from federal guidance from the SEC. Specifically, the SEC should issue further guidance and potentially adopt a statute that is designed to meet the concerns related to physical data breaches.[5]

I. BACKGROUND

a. Cybersecurity and Potential Liability

A cyberattack is a willful breach of a company's computer systems and networks.[6] Code[7] is often used to disrupt the normal operations that can compromise sensitive data and result in consequences such as identity and information theft.[8] Cyber threats are constantly changing and require an expenditure of resources to continually update data security departments within corporations.[9] Cybersecurity can be defined as "the protection of investor and firm information from compromise through the use – in whole or in part – of electronic

5. Physical data breaches are exactly as they sound and occur when hardware is lost or stolen. Ciaran Walsh, *Data Breaches – It's Not Just Digital, Physical Data Breaches Matter Too*, INFO. AGE (Jan. 15, 2019), https://www.information-age.com/physical-data-breaches-123478185/.

6. *What is a Cyber Attack?*, IBM SERVS. (Dec. 1, 2020), https://www.ibm.com/services/business-continuity/cyber-attack.

7. Code is the language computers run on. It tells a computer what to do and how to operate. In the cyber-attack context, attackers use their own code to alter the normal operations of a network giving the attacker control and access to data. *See What is Coding?*, COMPUT. SCI. DEGREE HUB, https://www.computersciencedegreehub.com/faq/what-is-coding/ (last visited Jan. 4, 2019).

8. Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L. J. SCI. & TECH. 23, 32 (2018).

9. *Id.* at 33.

digital media."[10] The phrase "data has been compromised" refers to loss of confidentiality, integrity, or availability of that data.[11] Specifically, a loss of confidentiality indicates disclosure of information, a loss of integrity means the destruction of information, and a loss of availability is the interruption of access to information.[12]

The probability of cyber incidents occurring combined with their impact is referred to as Cyber Risk.[13] Cyberattacks may be carried out in a variety of ways, such as by third parties or company insiders using complex techniques or through traditional social engineering.[14] Attacks can come remotely in a more stereotypical sense similar to what is seen on television or they can come through more personal means by directly interacting with people and gaining information needed to conduct the cyber-attack.[15] There can be many costs and negative consequences associated with a data breach:

- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
- Increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
- Increased insurance premiums;
- Reputational damage that adversely affects customer or investor confidence; and
- Damage to the company's competitiveness, stock price, and long-term shareholder value.[16]

While there are numerous benefits to innovation and the internet, the risks of data breaches often increase in relation, and sensitive data is unintentionally disclosed.[17] As the electronic nature of information keeps growing, cybersecurity issues will as well. Media reports of incidents relating to cybersecurity have

10. FINRA, REPORT ON CYBERSECURITY PRACTICES, 3 (Feb. 2015), https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.

11. *Id.*

12. Dynkin & Dynkin, *supra* note 8, at 32.

13. Cyber Task Force Final Report, OICU-IOSCO, 3 n.3 (June 2019).

14. SEC CF Disclosure Guidance: Topic No. 2 – Cybersecurity, 1 (October 13, 2011).

15. *See What is a Cyber Attack*?, *supra* note 6.

16. SEC Release Nos. 33-10459; 34-82746 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 3-4 (Feb. 26, 2018).

17. Luis J. Diaz, Maria C. Anderson, John T. Wolak, & David Opderbeck, *The Risks and Liability of Governing Board Members to Address Cyber Security Risks in Higher Education*, 43 J.C. & U.L. 49 (2017).

become as common as the weather forecast.[18] The U.S. Federal Bureau of Investigations reported that it had informed 3,000 companies, including banks, retailers, and defense contractors, that they were victims of breaches in 2013.[19]

Cybersecurity concerns span the globe. In the United Kingdom, a supermarket chain was hacked by a company insider who stole bank account information of 100,000 employees and published the stolen information online.[20] In South Korea, 105 million payment card accounts were uncovered in a breach, and in Germany 18 million e-mail addresses, passwords, and other information was stolen.[21] In addition, $45 million from ATM accounts of two banks in the Middle East was also taken by cyber criminals.[22]

Large companies in the U.S. have also fallen victim to data breaches. In 2013, Target reported a massive breach that affected around 40,000 of their card devices at stores.[23] It was initially believed to have exposed the credit card information of forty million customers.[24] At the time, it was the second largest[25] retail data breach in history.[26] In 2014, The Home Depot suffered a breach between April and September where the financial data of fifty-six million customers was stolen.[27] One year after the breach, the cost to The Home Depot was $152 million, with the total cost having been estimated to eventually reach $10 billion.[28] Wyndham Worldwide Corporation, a large hotel company, was also the victim of a breach on three occasions in 2008 and 2009.[29] Hackers stole personal information of hundreds of thousands of customers leading to over $10.6 million in fraudulent charges.[30] Other than direct loss, secondary effects such as a company's profits and its relationships with investors may be negatively impacted by data breaches.[31] Other large

18. PWC Global, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD, KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SURVEY 2015, 1 (Sept. 30, 2014) [hereinafter *Managing Cyber Risks*].

19. *Id.*

20. Brandon Stosh, *UK Supermarket Chain Morrisons Hacked, 100,000 File Data Breach*, FREEDOM HACKER (Mar. 16, 2014), https://freedomhacker.net/2014-03-uk-supermarket-chain-morrisons-hacked-100000-file-data-breach/.

21. *Id.* at 2.

22. *Id.*

23. Robin Sidel, Danny Yadron & Sara Germano, *Target Hit by Breach of Credit Cards*, WALL ST. J. (Dec. 19, 2013, 7:29 AM), https://www.wsj.com/articles/target-hit-by-creditcard-breach-1387406300.

24. Peter Varlan, *The Growing Risk of Director Liability for Cyberattacks*, PROGRAM ON CORP. COMPLIANCE AND ENF'T AT NEW YORK UNIV. SCH. OF LAW (Sept. 4, 2017), https://wp.nyu.edu/compliance_enforcement/2017/09/04/the-growing-risk-of-director-liability-for-cyberattacks/.

25. For reference, the current holder of largest breach is Yahoo! from a hack in 2013 that affected over three billion accounts. They were also hacked a second time in 2014. Kenneth Kiesnoski, *5 of the Biggest Data Breaches Ever*, CNBC (July 30, 2019, 10:22 AM), https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html.

26. Complaint at 1, In re Target Corp., 2014 WL 497105 (D. Minn. 2014) (No. 14 CV 00261).

27. *In re* The Home Depot, Inc. S'holder Deriv., 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016).

28. *Id.*

29. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

30. *Id.*

31. Amanda Marie Payne, *What the Hack?! Reexamining the Duty of Oversight in an Age of Data Breaches*, 53 GA. L. REV. 727, 730 (2019).

companies who have experienced breaches include TJX Cos. (parent company of T.J. Maxx), Home Goods, J.C. Penny Co., 7-Eleven, Nasdaq OMX Group, and JetBlue Inc.[32] This list is certainly not exhaustive.

Even companies who often report news of cybersecurity events are not themselves adequately protected. Organizations such as The New York Times, The Financial Times, CNN, and Reuters have been compromised in the past.[33] Even the SEC had its Electronic Data Gathering, Analysis, and Retrieval (EDGAR) platform, which holds financial reports of publicly traded companies, hacked in 2016.[34]

Potential liability may lie in actions or inactions of the boards of directors of such organizations. As will be discussed shortly, directors have certain fiduciary duties they owe to their shareholders. Because cybersecurity and cyberattacks are more recent issues, there remains the question of how these issues apply to those fiduciary duties of board members. Unfortunately, there is no clear answer.[35]

Liability may also come from the federal securities realm. Congress passed the Securities Act of 1933 to enable more transparency in the securities area.[36] The Act created disclosure requirements for large companies who traded on the stock market.[37] Congress also created the SEC with the passing of the Securities Exchange Act of 1934.[38] The Act gave the SEC broad power and authority to regulate securities by implementing rules as well as providing for disciplinary actions.[39]

Another arm of the federal government tasked to protect consumers is the Federal Trade Commission (FTC). The FTC was created with the passing of the Federal Trade Commission Act.[40] Among other things, this act allowed the FTC to prevent unfair trading practices, seek relief for injured consumers, create rules describing acts that are unfair or deceptive, conduct investigations, and make reports to Congress and the public.[41] The FTC has initiated civil actions against companies who have failed to prevent breaches. Generally, these complaints allege violations of federal laws. Complaints also note the companies routinely collect information from customers in payment card purchases, and that the corporations

32. *See* Sidel, Yadrom, & Germano, *supra* note 24.

33. *See Managing Cyber Risks*, *supra* note 18, at 3.

34. Janet Burns, *SEC Reveals Its EDGAR Database Was Hacked, Maybe Used For Illegal Trades*, FORBES (Sept. 21, 2017, 3:39 AM), https://www.forbes.com/sites/janetwburns/2017/09/21/sec-reveals-that-hackers-may-have-used-edgar-data-for-illegal-trades/#313bddd21880.

35. *See generally* Varlan, *supra* note 25 (noting that courts have not yet found cybersecurity duties clear enough to form the basis for a claim).

36. *The Laws That Govern the Security Industry*, INVESTOR, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry (last visited Feb. 5, 2021).

37. *See* 15 U.S.C. § 77 (2018).

38. *Id.* § 78d.

39. *See id.* § 78.

40. *See id.* § 41.

41. *See id.* §§ 41-58.

failed to provide for adequate security, resulting in a breach.[42] These cases generally result in the FTC mandating companies to create improved security systems to prevent breaches in the future, and further require reporting to the FTC for a period of time.[43] As a result, directors need to be wary that their actions or inactions may result in violations of federal law.

b. Fiduciary Duties

Generally, in the law of corporations, boards of directors have fiduciary duties to the businesses they oversee.[44] They owe a duty to save their beneficiaries, or stockholders, from a loss. [45] The directors of corporations are said to have a triad of duties: due care, loyalty, and good faith.[46] They do not operate intermittently and directors are required to discharge all duties at the same time.[47] A shareholder attempting to hold a director liable for breach of a duty must show the duty breached was a duty owed to the stockholder and that the action can proceed without injury to the company.[48] For the purposes of this note, the fiduciary duties will be discussed as background information, but the central focus will be on the SEC and what guidance they should give regarding hardware.

i. Duty to Disclose

As a preliminary matter, directors owe a fiduciary duty to fully disclose all facts within their knowledge that are material to a stockholder action.[49] The materiality of facts is assessed from the view of a "reasonable" stockholder, being an objective standard and not from a director's perspective.[50] A fact will be material if disclosure of an omitted fact would have altered the "total mix" of information available to the investor.[51] That is, among all the information a potential investor would need to consider when investing, whether an additional fact would lead the investor to change their mind or have doubts. Directors owe disclosures in "complete candor."[52] Simply put, directors should be transparent and honest. Disclosure requirements would apply to cybersecurity issues as well, but

42. *In re* Dave & Busters, Inc., 149 F.T.C. 1449, 2010 WL 9434816, at *2 (May 20, 2010).

43. *See generally In re* Dave & Busters, Inc., 149 F.T.C. 2010 WL 943816 (May 20, 2010); *In re* Acranet, Inc., 152 F.T.C. 367, 2011 WL 1179855 (Aug. 17, 2011); *In re* Fajilan and Assocs., Inc., 152 F.T.C. 389, 2011 WL 11798456 (Aug. 17, 2011) (orders from FTC requiring implementation of improved security remaining active for twenty years from date of order).

44. Bodell v. General Gas & Elec. Corp., 132 A. 442, 446 (Del. Ch. 1926).

45. *Id.* at 447.

46. Emerald Partners v. Berlin, 787 A.2d 85, 90 (Del. 2001).

47. *Id.*

48. *In re* J.P. Morgan Chase & Co. S'holder Litig., 906 A.2d 808, 817 (Del. Ch. 2005).

49. Arnold v. Society for Sav. Bancorp, Inc., 650 A.2d 1270, 1276 (Del. 1994).

50. *Id.* at 1277.

51. *Id.*

52. Smith v. Van Gorkom, 488 A.2d 858, 890 (Del. 1984).

shareholders still need to identify what was misleading or false.[53] Disclosure may not be required solely because it is relevant or of interest.[54]

ii. Duty of Loyalty

The duty of loyalty prevents directors from using their position to further their own private interests at the expense of the corporation's beneficiaries.[55] The law of corporations demands unselfish and undivided loyalty to the company.[56] If an opportunity comes to a director in his individual capacity as a private citizen and does not affect the corporation he represents, then the opportunity is his own and he has not violated this duty.[57] But if an opportunity comes in conflict with the corporation the director represents, "the law will not permit him to seize the opportunity for himself."[58] The obligation to the company does not tolerate self-dealing by the director.[59] This duty can be simplified to mean that a director cannot steal from the corporation he represents. The duty of loyalty is not a huge issue to cybersecurity and will not be a focal point of this note, but it does exist. It could be relevant if a director stole consumer information himself, but this is rare, if it happens at all.[60] For example, with regard to hardware, this duty would be violated by a director stealing a hard drive or server.

iii. Duty of Care

Company directors have a fiduciary duty to manage their businesses with due care, and this duty is owed to the corporation's stockholders.[61] There are generally two scenarios where a director may be liable involving this duty. The first is for a decision that results in a loss that may have been negligent or ill-advised; the second being for "an unconsidered failure of the board to act" in such circumstances where action would have prevented a loss.[62] Even unconsidered inaction could be the basis for liability because ordinary business decisions by officers deeper within the company can hurt the company and subject it to criminal penalties.[63] Management can fulfill this duty by gathering opinions of experts to design policies and procedures to be able to protect their companies from unauthorized access.[64]

---

53. *In re* Home Depot, Inc. S'holder Deriv. Litig., 223 F. Supp. 3d 1317, 1330 (N.D. Ga. 2016).
54. *Id.*
55. Guth v. Loft, 5 A.2d 503, 510 (Del. 1939).
56. *Id.*
57. *Id.*
58. *Id.* at 511.
59. Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1984).
60. *See* Federated It v. Anthony, No. 1:18cv1484 (LMB/JFA), 2020 U.S. Dist. LEXIS 150555 at *7 (E.D. Va. May 12, 2020) (though involving a breach of the duty loyalty arising from agency law, rather than corporate law).
61. 2 Data Sec. & Privacy Law § 10:8 (2019).
62. *In re* Caremark Int'l, Inc. Deriv. Litig., 698 A.2d 959, 967 (Del. Ch. 1996).
63. McCall v. Scott, 239 F.3d 808, 817 (6th Cir. 2001).
64. 2 Data Sec. & Privacy Law § 10:8 (2019).

The duty of care has not been much of an issue for corporations in recent years. Delaware, one of the more popular jurisdictions for businesses to incorporate, has allowed a waiver of the duty of care in their certificate of incorporation.[65] This is an exculpatory provision. It does not eliminate liability for the duty of loyalty, acts of bad faith, or decisions where a director obtained an improper benefit.[66] Directors can only be held liable if they act with a disloyal state of mind in regard to their obligations to the company.[67] Thus, complaints alleging omissions not in good faith and intentional misconduct in violation of law fall outside exculpation and will not be disposed of at the pleading stage of litigation.[68]

Directors can also escape liability for this duty through the business judgment rule. This rule is based on a presumption that directorial decisions are made in good faith and with an honest belief that the action was in the best interest of the corporation.[69] It is irrelevant if a judge or jury concludes that the decision was "stupid" or they would have come to a different conclusion; a board's action will be sustained so long as there was a good faith effort to advance the corporation's interests.[70] The purpose of this rule is to take judges out of the position of evaluating business decisions.[71] Therefore, the duty of care is satisfied when a director "in fact exercises a good faith effort to be informed and to exercise appropriate judgment."[72] There will be no liability for loss unless the facts show that no person could authorize such a transaction if they were actually trying to meet their duty in good faith.[73] A court may only overrule a director's business judgment in the rare case that the decision on its face is so egregious.[74] A shareholder will need to overcome this good faith presumption to pursue a claim.[75] If a plaintiff shareholder does rebut the presumption of business judgment, then the burden will shift to the defendant directors to prove "entire fairness" of the transaction.[76] This means the director will need to show the transaction was fair to the shareholder.[77]

The duty of care would be violated if a director did not have any policies or procedures regarding hardware security.[78] It may also be violated if there are policies, but they are negligent or ill-advised.[79] For example, if a company had a

65. DEL. CODE. ANN. tit. 8, § 102(b)(7) (2020).

66. *Id.*

67. Desimone v. Barrows, 924 A.2d 908, 933 (Del. Ch. 2007).

68. *In re* Abbott Labs. Deriv. S'holders Litig., 325 F.3d 795, 811 (7th Cir. 2003).

69. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984).

70. In re Caremark Int'l, Inc. Deriv. Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

71. Joseph K. Leahy, *A Decade After Disney: A Primer on Good and Bad Faith*, 83 U. CIN. L. REV. 859, 860 (2015).

72. *In re Caremark*, 698 A.2d at 968.

73. Gagliardi v. Trifoods Int'l, Inc., 683 A.2d 1049, 1053 (Del. Ch. 1996).

74. Brehm v. Eisner, 746 A.2d 244, 260 (Del. 2000).

75. Rales v. Blasband, 634 A.2d 927, 933 (Del. 1993).

76. McMullin v. Beran, 765 A.2d 910, 917 (Del. 1999).

77. Emerald Partners v. Berlin, 787 A.2d 85, 91 (Del. 2001).

78. Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. & CYBER WARFARE 109, 123 (2014).

79. *Id.*

policy that allowed lower level employees access to secure hardware devices containing consumer information, and that policy was deemed insufficient and resulted in a loss for the company because an employee lost or stole the device, directors may be held liable. Of course, these hypothetical situations may not result in liability if the business is incorporated in a state that allows for waiver of the duty of care, like Delaware.

iv. Duty to Monitor

The duty to monitor, also known as the duty of oversight, is a sub-division of the duty of care.[80] It was first articulated in *In re Caremark International Inc.* (*Caremark*).[81] In *Caremark*, shareholders engaged in a derivative suit against directors.[82] The claim was for breach of fiduciary duties because physicians were allegedly receiving "kick-backs" for referring patients to certain facilities within the network.[83] The court, in reviewing a settlement agreement, elaborated that a director has a duty to make sure a reporting system merely exists, and failure to do so may theoretically result in liability.[84] "[O]nly a sustained or systematic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability."[85] This certainly seems to be a low standard for directors and the court acknowledged this fact. "Such a test of liability . . . is quite high."[86] It would be easier to plead a failure to monitor compliance with law as opposed to a failure to monitor the normal course of business.[87] The court upheld the settlement agreement as reasonable, found that the directors did not lack good faith, and found that the directors did not consciously violate the law.[88]

The next case to elaborate on the rule from *Caremark* was *In re Walt Disney Co. Derivative Litigation* (*Disney*).[89] In *Disney*, the board approved the hire of Michael Ovitz to serve as president for a five-year term, and ended up terminating his employment without cause only fourteen months into his contract.[90] The termination included a severance of $130 million.[91] Plaintiff shareholders alleged breach of fiduciary duties against the board claiming the board failed to act with due care and in good faith by approving the employment contract with the no fault

80. Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill their Monitoring Role*, 15 U.C. DAVIS BUS. L.J. 201, 204 (2015).

81. *In re* Caremark Int'l, Inc. Deriv. Litig., 698 A.2d 959 (Del. Ch. 1996).

82. *Id.*

83. *Id.* at 962.

84. *Id.* at 970.

85. *Id.* at 971.

86. *Id.* at 971.

87. *In re* Facebook, Inc. Section 220 Litig., No. 2018-0661-JRS, 2019 WL 2320842, at *14, n.150 (Del. Ch. 2019).

88. *In re* Caremark Int'l, Inc. Deriv. Litig., 698 A.2d 959, 972 (Del. Ch. 1996).

89. *In re* Walt Disney Co. Deriv. Litig., 906 A.2d 27 (Del. 2006).

90. *Id.* at 35.

91. *Id.*

termination provision and the severance agreement.[92] Plaintiffs also alleged a breach of fiduciary duties of care and loyalty against Ovitz himself by negotiating and accepting that same agreement.[93] In determining what constitutes bad faith, the Delaware Supreme Court articulated three factual scenarios where bad faith can be found.[94] First is subjective bad faith, which is an actual motive to do harm; second is lack of due care or action that is taken negligently without intent or motive; the third situation falls between the first two and includes subjective bad intent and gross negligence.[95] The court upheld the Chancery Court's finding that the decisions of *Disney* were protected business judgments, and there were no fiduciary duty violations.[96]

The next decision to elaborate on these fiduciary duties was *Stone v. Ritter*.[97] In *Stone*, AmSouth Bank allowed two individuals to open up custodial trust accounts for investors of their business venture.[98] Unfortunately, this "business venture" was nothing more than a "Ponzi" scheme[99] and was not uncovered until two years after the initial opening of the accounts.[100] AmSouth Bank and its parent company AmSouth became subject to $40 million in fines and $10 million in civil penalties resulting from government investigation.[101] Dealing with a *Caremark* claim, the court further elaborated on the good faith standard. "[A] failure to act in good faith is not conduct that results, *ipso facto*, in the direct imposition of fiduciary liability."[102] The court noted that the good faith requirement is a subsidiary element of the duty of loyalty.[103]

> [T]he obligation to act in good faith does not establish an independent fiduciary duty that stands on the same footing as the duties of care and loyalty. Only the latter two duties, where violated, may directly result in liability, whereas a failure to act in good faith may do so, but indirectly.[104]

Directors are exposed to oversight liability when they actually knew they were not discharging their fiduciary obligations.[105] There has to be a showing that directors were consciously disregarding their duties.[106] Because an unwise business judgement with a bad outcome does not necessarily constitute bad faith,

92. *Id.* at 46.
93. *Id.* at 47.
94. *Id.* at 64-66.
95. *Id.*
96. *Id.* at 73.
97. *See generally* Stone v. Ritter, 911 A.2d 362 (Del. 2006).
98. *Id.* at 365.
99. A Ponzi scheme, named for Charles Ponzi, is where investments from new investors are used to satisfy older investors on their promised returns. They are illegal.
100. *Stone*, 911 A.2d at 365.
101. *Id.*
102. *Id.* at 369.
103. *Id.* at 370.
104. *Id.*
105. *Id.*
106. Guttman v. Huang, 823 A.2d 492, 506 (Del. Ch. 2003).

the court dismissed the action.[107] Oversight duties are not designed to hold directors liable for failing to predict the future.[108] "In the absence of red flags, good faith in the context of oversight must be measured by the directors' actions 'to assure a reasonable information and reporting system exists' and not by second-guessing after the occurrence of employee conduct that results in an unintended adverse outcome."[109] The court defined red flags in the context of the case as "facts showing that the board was aware that AmSouth's internal controls were inadequate, that these inadequacies would result in illegal activity, and that the board chose to do nothing about problems it allegedly knew existed."[110] Additionally, this evidence does not need to be direct as courts will allow circumstantial evidence to prove director knowledge and liability.[111]

Based on the preceding case law, one can argue that in the hardware setting, this duty will be violated if a director knows that hardware is not secure and does nothing. There would need to be a showing that the director completely failed to oversee the operations of her respective corporation. The obvious issue is that such complete failure is incredibly difficult to prove, as can be seen by the previously mentioned cases that were dismissed for lack of evidence. In general, it appears that claims alleging breach of fiduciary duty will not make it far before they are dismissed or settled.

c. Securities Regulation

i. Federal Regulation

1. The Securities Exchange Commission

Two major pieces of federal legislation set the stage for the regulation of securities: the Securities Act of 1933 and the Securities Exchange Act of 1934.[112] The Securities Act sought to regulate securities[113] and provide disclosure requirements to companies that planned to offer shares.[114] There were two main goals with this Act: Congress wanted (1) investors to have financial information about securities available and (2) to prohibit fraud, deceit, and misrepresentations within the sale of securities.[115] The disclosures should enable potential investors to perform their due diligence when purchasing shares.[116] One example is that companies are required to register securities they offer. The reason for this is so

107. *Stone*, 911 A.2d at 373.

108. *In re* Citigroup Inc. S'holder Deriv. Litig., 964 A.2d 106, 131 (Del. Ch. 2009).

109. *Stone*, 911 A.2d at 373 (quoting In re Caremark Int'l Inc. Deriv. Litig., 698 A.2d at 968).

110. *Id.* at 370.

111. *In re* Pfizer Inc. S'holder Deriv. Litig., 722 F. Supp. 2d 453, 461-62 (S.D.N.Y. 2010).

112. 15 U.S.C. § 77 (1933); 15 U.S.C. § 78 (1934).

113. A "security" is a business investment.

114. 15 U.S.C. § 77g(c) (2010) (1933).

115. *The Laws that Govern the Securities Industry*, U.S. SEC. EXCH. COMM'N, https://www.sec.gov/answers/about-lawsshtml.html (last visited Nov. 7, 2019).

116. 15 U.S.C. § 77g(c)(2)(B) (1933).

investors can view all available information in order to make a sound decision.[117] Generally, the information to include when registering a security includes a description of the business, a description of the security, information about management of the business, and financial statements certified by independent accountants.[118]

The Securities Exchange Act, among other things, created the SEC.[119] Congress noted that the regulation of securities is important and necessary because prices on markets and exchanges are susceptible to manipulation, and the spread of this information results in unfair practices.[120] Importantly, the Act requires companies with over $10 million in assets, and with securities held by more than 500 owners to file annual and other periodic reports.[121] Both Acts include measures to prevent insider trading[122] and disciplinary actions for violations.[123]

Federal regulations also dictate how a securities firm must store consumer information. The SEC requires firms to retain information in the course of their business.[124] Records that are required to be retained may be produced on "electronic storage media."[125] This storage media must: (1) preserve information in a non-rewriteable, non-erasable format; (2) verify the quality and accuracy; (3) serialize the original and any duplicates; and (4) have the capacity to download the records.[126] Companies registered with the SEC are required to adopt written policies that encompass safeguards to protect consumer information.[127] These policies must be designed to ensure the confidentiality and safety of customer records, provide protection against threats, and protect against unauthorized access or use of that information.[128]

Specifically, the SEC provides guidance for the creation of Identity Theft Prevention Programs.[129] The Commission requires that these programs identify red flags and provide responses to possible threats.[130] The program must be regularly updated,[131] and administration of the program must involve a board of directors with effective oversight.[132] This duty is similar to the fiduciary duty of oversight but differs because the Commission requires more than the simple appearance of a program. They provide further information about how a corporation can design

117. *The Laws that Govern the Securities Industry*, *supra* note 117.

118. *Id.*

119. 15 U.S.C. § 78d (1934).

120. 15 U.S.C. § 78b(3) (1934).

121. *The Laws that Govern the Securities Industry*, *supra* note 117.

122. Insider trading is illegal and occurs when a person trades a security while in possession of material, nonpublic information.

123. *The Laws that Govern the Securities Industry*, *supra* note 117.

124. *See* 17 C.F.R. § 240.17a-3 (2020).

125. 17 C.F.R. § 270.31a-2(f)(1)(ii) (2018).

126. 17 C.F.R. § 270.31a-2(f)(3)(i)-(iii) (2018) .

127. 17 C.F.R. § 248.30(a) (2005).

128. 17 C.F.R. § 248.30(a)(1)-(3) (2005).

129. 17 C.F.R. § 248.201(d) (2013).

130. 17 C.F.R. § 248.201(d)(2)(i)-(iii) (2013).

131. 17 C.F.R. § 248.201(d)(2)(iv) (2013).

132. 17 C.F.R. § 248.201(e)(2), (4) (2013).

its programs including what a company may include in the program, what red flags to look for, and how to respond to them. The Commission also supplies information regarding how the program should operate in order to prevent and mitigate identity theft of consumers.[133]

SEC regulation also provides guidance for disposal. Companies registered with the Commission that maintain consumer information "must properly dispose of the information by taking reasonable measures to protect against unauthorized access or use of the information in connection with its disposal."[134]

2. The Federal Trade Commission

The FTC regulates companies through the Federal Trade Commission Act,[135] and was established to prevent unfair methods of competition or deceptive acts affecting commerce. [136] The FTC brings action against companies for violations of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLB) to name a few.[137] Specifically, the GLB Safeguards Rule requires financial institutions to protect the security, confidentiality, and integrity of consumer information by creating a comprehensive security program.[138] The FCRA requires consumer reporting agencies to limit the furnishing of consumer reports.[139] The FTC also defined not providing an adequate security system as an unfair act or practice in violation of the FTC Act.[140]

The FTC brought an action against Wyndham as a result of their breaches in 2008 and 2009.[141] The FTC alleged that Wyndham failed to use "readily available security measures" and allowed third parties to access the network multiple times in direct contravention of their own privacy policy as an unfair practice or act.[142] The hackers allegedly stole credit card information of over 619,000 consumers resulting in at least $10.6 million in fraud loss.[143] Wyndham attempted to dismiss the complaint arguing the conduct did not amount to "unfair,"[144] and offered a dictionary definition that a practice is only unfair if it is "not equitable" or is "marked by injustice, partiality, or deception."[145] The court disagreed, but otherwise noted "[a] company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes

133. 17 C.F.R. § Pt. 248, Subpt. C, App. A. (2013).
134. 17 C.F.R. § 248.30(b)(2)(i) (2005).
135. 15 U.S.C. § 41. (2020).
136. 15 U.S.C. § 45. (2006).
137. *See* In re Acranet, Inc., 152 F.T.C. 367 (2011).
138. *Id.* at *3.
139. *Id.* at *4.
140. *Id.*
141. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
142. *Id.* at 241.
143. *Id.* at 242.
144. *Id.* at 244.
145. *Id.* at 245.

its unsuspecting customers to substantial financial injury, and retains the profits of their business."[146]

Another issue presented concerns whether Wyndham had fair notice of the meaning of the FTC Act. The court determined they did[147] by comparing the *Wyndham* complaint to another complaint the FTC had filed previously and noting the similarities.[148] This ruling is quite contrary to the shareholder complaint.[149]

ii. State Regulation

This section will analyze different laws in twenty-four states discussing how entities in the private sector are to handle data security for consumers' information,[150] specifically examining as to what extent they provide for hardware security. Even where laws may not specifically apply to business entities, they are still worth looking at in terms of how they could apply to large companies. Generally, the following statutes can be broken down into two categories: flexible and comprehensive.

The "flexible" statutes mainly require reasonable security measures without much specificity. Presumably, this is to allow corporations to come up with their own industry procedures. It follows, then, that reasonableness must be examined in this context. Although there are limited court opinions that elaborate on the reasonableness requirement in this area, it has been noted that the standard is reasonable because data security, and consequently what is reasonable, is an evolving area.[151]

Examining an individual data security plan's reasonableness will also depend on context.[152] In an administrative decision, the Federal Communications Commission (FCC) articulated four factors for the reasonableness standard: (1) "the nature and scope of [a corporation's] activities; (2) the sensitivity of the data it collects; (3) its size; and (4) technical feasibility."[153] In this context, reasonableness may depend on guidance issued directly from the state. For example, in California, the Attorney General identified twenty data controls as a baseline and failure to meet those controls constituted a lack of reasonable

146. *Id.*

147. *Id.* at 255.

148. *Id.* at 258.

149. *See* Palkon v. Holmes, No. 2:14CV-01234, (SRC), 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (dismissing shareholder complaint due to pleading issues and business judgment rule).

150. *Data Security Laws – Private Sector*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 29, 2019)), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

151. *In re* Protecting the Privacy of Customers of Broadband and Other Telecomms. Servs., 31 FCC Rcd. 13911, 14006 (Oct. 27, 2016).

152. *Id*. at 14009.

153. *Id.*

security.[154] A few of the controls included in this list are inventorying, use of privileges in administration, incident response, etc.[155]

A comprehensive statute, as can be inferred, includes much more. Rather than a single paragraph stating reasonable security measures, a comprehensive statute includes more detailed requirements that are necessary if a business collects customer information. Similar to the FCC's four factors, a comprehensive statute also considers factors such as size of the business and the number of resources available.[156] Comprehensive statutes provide myriad, in-depth requirements, the most pertinent of which concern authentication protocols, access control, encryption, program oversight, identification of risks, prevention of terminated employees from access, post-incident review, and the catch-all "any other safeguards" a company feels necessary to include.[157]

1. Alabama

Alabama's statute only requires that companies maintain "reasonable security measures" to protect sensitive information against a breach.[158] The statute elaborates on some measures that meet this standard but does not mention hardware specifically. However, there is a portion of the bill that can be interpreted to imply hardware. In the section of the statute covering an assessment of the current security, one of the considerations is the amount of sensitive data and, among other things, how it is stored.[159]

2. Arkansas

In Arkansas, the applicable statute does not specifically reference hardware by name or how it should be handled. Rather, it prescribes for the proper method of destruction for personal information the company no longer needs. This statute merely mandates that a business implement reasonable security measures as appropriate for the type of information.[160]

154. Bret Cohen, Paul Otto, Nathan Salminen, & Morgan Perna, *California Consumer Privacy Act: The Challenge Ahead – The CCPA's "Reasonable" Security Requirement*, HOGAN LOVELLS (Feb. 7, 2019), https://www.hldataprotection.com/2019/02/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-ccpas-reasonable-security-requirement/.

155. *The 20 CIS Controls & Resources*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-list/ (last visited Feb. 4, 2020).

156. CONN. GEN. STAT. ANN. § 38a-999b(b)(1) (West, Westlaw through 2020 Reg. Sess.) (repealed 2021).

157. CONN. GEN. STAT. ANN. § 38a-999b(b)(2)(A)-(L) (West, Westlaw through 2020 Reg. Sess.) (repealed 2021).

158. S.B. 318 § 3(a), 2018 Regular Leg. Sess. (Ala. 2018).

159. S.B. 318 § 3(c)(2).), 2018 Regular Leg. Sess. (Ala. 2018).

160. ARK. CODE ANN. § 4-110-104 (West, Westlaw through Acts 18, 20, 56, 60, 87, and 94 passed by the 2021 Reg. Sess. of the 93rd Ark. Gen. Assemb.).

3. California

California law provides legislative intent, and similar to others, only requires reasonable security measures.[161] Again, this law does not specifically provide for hardware. However, there is another potentially relevant statute in the same chapter regarding connected devices.[162] Connected devices are types of hardware that may be used in businesses. This statute may be beneficial for hardware security as it provides specifics for password use and authentication for access.[163] While it only applies to manufacturers in California, it could still be helpful as a framework for businesses.

4. Colorado

The pertinent Colorado law requires only "reasonable security procedures."[164] A different section of the law also provides for disposal of information which gives examples of what information the law refers to as needing protection such as a social security number, personal identification number, password, etc.[165] Nothing else in either of these sections provide specifically for hardware.[166]

5. Connecticut

The Connecticut statute requires companies storing customer data to adopt a comprehensive security program.[167] While some of the components do not apply to hardware specifically, a large company could utilize a similar framework in their business, especially with the care of hardware. Of particular importance is that this statute does provide guidelines for access control such as who should be allowed access, and how information should be stored.[168]

---

161. CAL. CIV. CODE § 1798.81.5 (West, Westlaw through ch. 2 of 2021 Reg. Sess.).

162. A "Connected Device" is a physical object that can connect with others over the internet. Common connected devices are laptops, desktops, smartphones, tablets, and the like. *Glossary: Connected Devices*, ARM, https://www.arm.com/glossary/connected-devices (last visited Jan. 19, 2020).

163. CAL. CIV. CODE § 1798.91.04(b)(1)-(2) (West, Westlaw through ch. 2 of 2021 Reg. Sess.).

164. COLO. REV. STAT. ANN. § 6-1-713.5 (West, Westlaw through ch. 7 of the 1st Reg. Sess. of the 73rd Gen. Assemb. (2021)).

165. COLO. REV. STAT. ANN. § 6-1-713(2)(b) (West, Westlaw through ch. 7 of the 1st Reg. Sess. of the 73rd Gen. Assemb. (2021)).

166. It might seem interesting to note that the disposal section does not require a recycling or disposal firm to verify that records were actually destroyed. COLO. REV. STAT. ANN. § 6-1-713(4) (West, Westlaw through ch. 7 of the 1st Reg. Sess. of the 73rd Gen. Assemb. (2021)).

167. CONN. GEN. STAT. ANN. § 38a-999b (West, Westlaw through 2020 Reg. Sess.) (repealed 2021).

168. CONN. GEN. STAT. ANN. § 38a-999b(b)(2)(B) (West, Westlaw through 2020 Reg. Sess.) (repealed 2021). (providing examples of access control measures such as limiting access to personal information to only those who need it); CONN. GEN. STAT. ANN. § 38a-999b(b)(2)(I) (West, Westlaw through 2020 Reg. Sess.) (repealed 2021). (noting storage of information in locked facilities).

Another statute providing for care of personal information by state contractors in Connecticut lists what actions a contractor should *not* do.[169] This provides helpful information for businesses to look at regarding their own information security, and hardware control. For example, it states that a contractor should not keep confidential information on stand-alone computers, external hard drives, flash drives, etc.[170] It is important that businesses follow similar protocols if they handle sensitive information.

6. Delaware

The relevant Delaware statute only requires reasonable procedures and practices to prevent the misappropriation of personal information.[171] Delaware's law is likely not as comprehensive as the Connecticut statute because Delaware is known for being attractive to businesses based on their courts, tax system, laws, and policies.[172]

7. Florida

Florida's statute also requires that reasonable measures be taken to protect and secure consumer data.[173] It does not mention hardware specifically, except to note that it is included in the statute's definition of "[d]ata in electronic form."[174]

8. Illinois

Similar to other states, Illinois only requires reasonable security measures.[175] The statute does not reference hardware with any specificity.

9. Indiana

Indiana's legislation mandates reasonable procedures to prevent unlawful use or disclosure of personal information.[176] The law does not specifically mention hardware, but it does provide for liability for disposing or abandoning records containing sensitive information without first having destroyed the information.[177] This could be useful for businesses as it is important to keep track of hardware

169. *See generally* CONN. GEN. STAT. ANN. § 4e-70(c) (West, Westlaw through 2020 Legs. Sess.).

170. § 4e-70(c)(1).

171. DEL. CODE ANN. tit. 6, § 12B-100 (West, Westlaw through ch. 292 of the 150th Gen. Assemb. (2019-2020)).

172. Suzanne Raga, *Why Are the Majority of U.S. Companies Incorporated in Delaware?*, MENTAL FLOSS (Mar. 11, 2016), https://www.mentalfloss.com/article/76951/why-are-so-many-us-companies-incorporated-delaware.

173. FLA. STAT. ANN. § 501.171(2) (West, Westlaw through ch. 184 of the 2020 Sess.).

174. § 501.171(1)(d).

175. 815 ILL. COMP. STAT ANN. 530 / 45(a) (West, Westlaw through P.A. 101-651).

176. IND. CODE ANN. § 24-4.9-3-3.5(c) (West, Westlaw through 121st Gen. Assemb.).

177. § 24-4.9-3-3.5(d).

marked for disposal if it contains personal information. This is the concern articulated in the Ernst & Young example in the introduction of this note.

10. Kansas

Kansas law also states that reasonable procedures and practices must be established.[178] This statute does not specifically mention hardware, but includes a provision allowing an affirmative defense to a claim against the business, and that burden of proof rests with the entity.[179] Requiring a business to prove that it should not be liable is much different than alleging breach of a fiduciary duty, where the burden is traditionally on the plaintiff to show that the business failed to carry out that duty.

11. Louisiana

Louisiana requires reasonable security practices to protect personal information.[180] Its law also provides for destruction of information, as well as disclosure requirements in the event of a breach,[181] but it does not specifically state how hardware should be managed.

12. Maryland

Like Louisiana, Maryland only requires reasonable security procedures and practices.[182] The law also provides that third party security providers must meet the same standards as if the business were providing their own security.[183] This law does not specifically mention hardware.

13. Massachusetts

Massachusetts provides that the security procedures must meet the same requirements as the applicable federal regulation.[184] The law does not specifically mention hardware but discusses that the amount of stored data will be taken into account when creating a program.[185] This could foreseeably include physical hardware.

178. KAN. STAT. ANN. § 139b(b)(1) (West, Westlaw through Jul. 1, 2020 Legis. Sess.).
179. § 139b(c).
180. LA. STAT. ANN. § 51:3074(A) (West, Westlaw through 2020 Second Extraordinary Sess.).
181. § 51:3074(B)-(C).
182. MD. CODE ANN. COM. LAW § 14-3503(a) (West, Westlaw through 2020 Reg. Sess. of the Gen. Assemb.)
183. § 14-3503(b)(1).
184. MASS. GEN. LAWS. ANN. ch. 93H, § 2(a) (West, Westlaw through ch. 226 of the 2020 2nd Ann. Sess.).
185. *Id.*

14. Minnesota

Minnesota's law requires reasonable steps be taken to maintain the security of personally identifiable information.[186] The section does not reference hardware.

15. Nebraska

Nebraska's law requires reasonable security procedures and practices.[187] It does not specifically mention hardware.

16. Nevada

Nevada's statute requires reasonable security measures but does not specifically mention hardware.[188] Rather, it provides that a collector doing business in the state must not move data storage devices outside of actual physical control by the collector.[189] This may be helpful to businesses as a guideline to possibly prohibit the transfer of physical hardware beyond the building where the business operates.

17. New Mexico

New Mexico only requires reasonable security procedures and practices.[190] It does not reference hardware.

18. Ohio

Ohio's law is organized such that a business must meet the requirements to claim an affirmative defense in case of a breach.[191] Generally, a business must create a written program that has administrative, technical, and physical safeguards, and that program must conform to an applicable industry framework.[192] While the law does not specifically mention the security of hardware, it does reference physical safeguards, which can be inferred to include hardware.

186. MINN. STAT. ANN. § 325M.05 (West, Westlaw through 2021 Reg. Sess.).

187. NEB. REV. STAT. ANN. § 87-808(1) (West, Westlaw through 2nd Reg. Sess. of the 106th Leg (2020)).

188. NEV. REV. STAT. ANN. § 603A.210 (West, Westlaw through 31st & 32nd Spec. Sess. (2020)).

189. NEV. REV. STAT. ANN. § 603A.215(2)(b) (West, Westlaw through 31st & 32nd Spec. Sess. (2020)).

190. N.M. STAT. ANN. § 57-12C-4 (West, Westlaw through Second Reg. Sess., 1st & 2d Spec. Sess. of the 54th Leg. (2020)).

191. OHIO REV. CODE ANN. § 1354.02(A) (West, Westlaw through files 78, 79, 80, 81 through 94, 98 through 107, 109 through 113, and 115 of the 113rd Gen. Assemb. (2019-2020)).

192. § 1354.02(A)(1)).

19. Oregon

Oregon's statute requires reasonable safeguards to protect consumer information.[193] Their law necessitates, for example, physical safeguards which includes assessing the risk of storage and retention of information.[194] While the law does not specifically reference hardware, coverage can be inferred under this section. Oregon's law is more thorough than most and is comparable to Connecticut's.

20. Rhode Island

Rhode Island requires a "risk-based" information security program.[195] The purposes of the law are the same as most states referenced here, but it does not specifically address hardware.

21. South Carolina

South Carolina's law applies to insurance data, but can still be helpful for other businesses. Similar to other states with more thorough legislative guidance, South Carolina requires a comprehensive written security program based on a risk assessment.[196] Specifically, the law requires access control to limited individuals.[197] In terms of hardware, it also necessitates encryption of laptops and portable storage devices.[198]

22. Texas

Texas law requires businesses to maintain reasonable procedures to protect sensitive personal information.[199] It also outlines how a firm may destroy such information.[200] However, this law does not reference hardware specifically.

23. Utah

Utah law is similar to most and only requires reasonable procedures to protect information.[201] It does not specifically mention hardware.

193. OR. REV. STAT. ANN. § 646A.622(1) (West, Westlaw through 2020 Reg. Sess. of the 80th Leg. Assemb.).

194. § 646A.622(d)(C)(i).

195. Tit. 11 R.I. GEN. LAWS ANN. § 11-49.3-2(a) (West, Westlaw through ch. 79 of the 2020 2d Reg. Sess.).

196. S.C. CODE ANN. § 38-99-20(A) (West, Westlaw through 2020 sess.).

197. § 38-99-20(D)(2)(c)).

198. § 38-99-20(D)(2)(d)).

199. TEX. BUS. & COM. CODE ANN. § 521.052(a) (West, Westlaw through 2019 Reg. Sess. of the 86th Leg.).

200. § 521.052(b).

201. UTAH CODE ANN. § 13-44-201(1) (West, Westlaw through 2020 Sixth Spec. Sess.).

24. Vermont

Vermont's statute is among those that require a comprehensive system.[202] Some important aspects to note are that the law is concerned with restrictions on access of stored data and how that data is stored. It requires reasonable restriction on physical access[203] and encryption for portable hardware and storage devices.[204]

II. PROPOSAL

a. Hardware Security Should be Emphasized by the SEC

The SEC should issue additional guidance, specifically regarding the need to secure hardware. It should provide guidelines for large businesses to follow, so that hardware does not become an afterthought. The SEC commits itself to helping people and businesses in regard to cyber threats and is already regularly providing guidance.[205] In a speech posted to the Commission's website, the director of the Office of Compliance Inspections and Examinations spoke directly about the need to secure hardware.

> [T]hese devices may [] contain sensitive customer information or other data that could be utilized to compromise the integrity of a firm's technology systems. Firms should assess their policies and procedures for inventorying, deactivating, and removing physical devices on their networks . . . Inadequate policies and procedures could result in harm to investors or the firm, and could be deficient under the federal securities laws.[206]

Yet, the SEC has not released guidance with specificity concerning the importance of hardware security. It should adopt a comprehensive approach with features similar to those implemented by states such as Connecticut, Oregon, South Carolina, and Vermont.[207] Specifically, the Commission should have an approach that outlines the importance of access control, physical location, encryption, and others. Additional requirements such as what not to do, and a statement noting that liability may be diminished for following the protocol, may be especially helpful.

---

202. VT. STAT. ANN. tit. 9, § 2447(a)(1) (West, Westlaw through Acts 1-180, M-1-M-12 of the Adjourned Sess. of the 2019-2020 Vt. Gen. Assemb. (2020)).

203. § 2447(b)(7)).

204. § 2447(c)(5)).

205. *Cybersecurity*, U.S. SEC. EXCH. COMM'N, https://www.sec.gov/spotlight/cybersecurity (last visited Feb. 9, 2021).

206. Peter Driscoll, *Remarks at the SIFMA Operations Conference & Exhibition: Staying Vigilant to Protect Investors*, U.S. SEC. EXCH. COMM'N (May 8, 2019), https://www.sec.gov/news/speech/driscoll-remarks-sifma-operations-conference-050819.

207. CONN. GEN. STAT. ANN. § 38a-999(b) (West, Westlaw through 2020 Reg. Sess.) (repealed 2021); OR. REV. STAT. ANN. § 646A.622(1) (West, Westlaw through 2020 Reg. Sess. of the 80th Leg. Assemb.); S.C. CODE ANN. § 38-99-20(A) (West, Westlaw through 2020 Sess.); Vt. Stat. Ann. tit. 9, § 2447(a)(1) (West, Westlaw through Acts 1-180, M-1-M-12 of the Adjourned Sess. of the 2019-2020 Vt. Gen. Assemb. (2020)).

Further guidance from the Commission would help companies adopt stronger policies, thus making misappropriation of consumer data less likely. For example, the Hong Kong Registration and Electoral Office reportedly lost two laptops, which resulted in the information of 3.7 million people being compromised.[208] Companies need to be reminded to take care of their physical hardware. Criminals can still gain access to restricted or privileged data through social engineering.[209]

Ultimately, giving this guidance is necessary and beneficial for information security. In fact, the FTC already mentions hardware in its guidance. The FTC guidance notes that the same considerations for network security can apply to physical media, and it provides helpful examples of how to store physical data.[210] Similar to some state laws, the FTC guidance also notes the importance of portable devices. A phone is not "just" a phone" and can cause harm if it is accessed by the wrong hands.[211] The FTC also discusses disposal and how more regulation is needed than simply clicking "delete."[212]

In addition, other organizations also mention hardware. The International Organization of Securities Commissions (IOSCO) issued a cyber report that contained a question set for companies to see if they met their standards. One of those questions asks if "the organization maintains an inventory of its software, *hardware*, applications, and vendors[.]"[213] The Financial Industry Regulatory Authority (FINRA) issued a report on cybersecurity practices that gave options for technical controls for a company. Of particular relevance are practices such as encryption standards for laptops, desktops, servers, mobile devices, and the like.[214] The report also notes the importance of developing physical security protocols for devices and creating processes for secured disposal of information and hardware.[215]

Because the concern of hardware security relates to physical breaches, it is important to note some common examples. These may include rogue employees, a lack of accountability, unattended devices, relaxing protocol by employees, and even eavesdropping.[216] Using the knowledge and guidance from preceding sources, a statute can be crafted such that the SEC could adopt outright or use as they see fit for purposes of issuing its own guidance:

---

208. Ciaran Walsh, *Data Breaches – It's Not Just Digital, Physical Data Breaches Matter Too*, INFO. AGE (Jan. 15, 2019), https://www.information-age.com/physical-data-breaches-123478185/.

209. *Id.*

210. *Start With Security: A Guide for Businesses*, FTC 13, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 20, 2020).

211. Thomas B. Pahl, *Stick with Security: Secure Paper, Physical Media, and Devices*, FED. TRADE COMM'N (Sept. 29, 2017, 12:21 PM), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-secure-paper-physical-media-devices.

212. *Id.*

213. CYBER TASK FORCE: FINAL REPORT, IOSCO, 19 (2019) (emphasis added).

214. FINRA, REPORT ON SELECTED CYBERSECURITY PRACTICES – 2018, 4 (2018) https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

215. *Id.*

216. Bernhard Mehl, *Types of Physical Security Threats You Should Know*, KISIBLOG (June 29, 2018), https://www.getkisi.com/blog/types-of-physical-security-threats.

A. Corporations registered with the Commission shall implement a comprehensive data security program designed for the protection of firm hardware. Such a program shall include:

1. Inventory of all hardware devices (desktops, servers, hard drives, laptops, etc.)
2. Encryption of devices to prevent unauthorized access
3. Access control program designed to confirm that only employees are allowed on grounds of any company property
4. Only allow access to authorized employees in which devices to be used shall be checked out and promptly returned when finished
5. These devices shall be placed in locked storage areas when not in use
6. Prompt rescission of employee access upon employee termination
7. Secured disposal of devices that are no longer needed, and actual disposal must be confirmed
8. Disciplinary review for employees who violate any provision
9. Yearly review of procedures included in this statute
10. Any other security program the company feels necessary to accomplish this purpose
11. If a company installs all procedures listed herein, it shall constitute an affirmative defense to an action arising from a physical breach

The list above covers some of the basic necessities mentioned in regard to hardware security. Specifically, the sections regarding access rescission of terminated employees and access control are aimed at satisfying the rogue employee concern. The access control provisions are also meant to cover the eavesdropping concern by controlling who can be in the vicinity of various devices, which will reduce the risk of employees seeing or hearing passwords entered. The disciplinary review section addresses accountability and relaxes protocol concerns. Finally, the affirmative defense provision provides an extra incentive to corporations to actually comply. Of course, the SEC and any business may expand on any individual section as it sees fit. This type of statute could be more effective than a flexible statute because it does not leave the requirements open for interpretation by businesses. Further, with the catch-all provision businesses can still incorporate any other method that is consistent with its industry practices.

Some may argue that this is unnecessary because hardware security is something that businesses are already addressing. If that is the case, then these types of security measures are not being taken care of well enough across the board. In a study of data breaches in California from 2012, 27% of total breaches were a result of physical failures that affected 58% of the total victims.[217]

Scholars and business professionals may argue that a comprehensive program is too expensive to implement. While there will be costs associated with implementing certain controls, the benefits are enough to outweigh them. The

217. *Data Breach Report 2012*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf (last visited Jan. 20, 2020).

average cost of a breach was $7.35 million in 2016,[218] and there are plenty of indirect losses tied to a breach such as stock prices and public image. If a company does as much as they can to avoid a breach in the first place, then the costs resulting from a breach are avoided. Having a comprehensive data security plan as a result of guidance from the SEC would establish greater confidence in both customers who do business with a particular company as well as that company's own shareholders. In addition, reputation may also be a persuasive justification for implementing a comprehensive program. In the aftermath of the Target breach, it was noted that the corporation had largely recovered, "[b]ut no matter how grand its remediation efforts were, Target will forever be associated with the data breach and its lasting repercussions."[219] A comprehensive program may help to avoid a breach in the first place, thereby avoiding the costs of a negative reputation.

Some may also argue that comprehensive programs are also too costly for small businesses and not feasible for them. This can be a concern, and while the focus of this note is on large companies, small businesses are still important to address. More guidance from the SEC is needed regarding hardware, not law, meaning there will be no liability if a firm cannot afford what is being suggested here. Also, the guidance can be scaled back for smaller businesses that might not have the funds to meet requirements. This would be similar to guidance offered by FINRA who specifically has a checklist for smaller businesses.[220]

III. CONCLUSION

The SEC should issue further guidance specifying the need to secure physical hardware in businesses. Adopting an approach similar to state laws in Connecticut, Oregon, South Carolina, Vermont, or the new statute proposed in this note will remind businesses of that need and hopefully lead to more adequately secured hardware and less physical breaches.

218. U.S. SECURITIES AND EXCHANGE COMMISSION, *COMMISSION STATEMENT AND GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES* 3 n. 5 (2018).

219. Natalie Gagliordi, *The Target Breach, Two Years breach, two years later*, ZDNET (Nov. 27, 2015), https://www.zdnet.com/article/the-target-breach-two-years-later/.

220. *Small Firm Cybersecurity Checklist*, FINRA, https://www.finra.org/rules-guidance/key-topics/cybersecurity#overview (last visited Jan. 20, 2020).