THE ONGOING ISSUE OF CYBER INSECURITY: WHY CYBER INSURANCE SHOULD BE MANDATORY FOR CONSUMER COMPANIES

ALLYSON PATTERSON

INTRODUCTION

In 2014, a survey by the Online Trust Alliance of 500 data breaches showed that 90% of the breaches could have been prevented with easily implemented security measures.[1] Companies are not adequately protecting customer data. Though the Security and Exchange Commission (SEC) enforces certain procedures for companies to follow when a data breach occurs and customer information is stolen,[2] companies are still left without adequate incentives to implement robust cybersecurity systems.[3] There are many misaligned incentives that arise from the current cybersecurity regulation that steer companies

1. ONLINE TRUST ALLIANCE, SECURITY AND PRIVACY ENHANCING BEST PRACTICES 1 (2015).

2. *See generally* Securities Act of 1933, 15 U.S.C. §§ 77a-77aa.

3. Lauren Miller, *Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity*, 7 J.L. & CYBER WARFARE 147, 158-59 (2019).

in the direction of careless cybersecurity systems instead of adequate systems.[4] A cyber insurance mandate for all companies that serve public customers is necessary to add an additional safeguard for protecting customer data.

Though the focus of this proposal is cybersecurity regulations on the federal level, states are looking at these issues as well. In fact, the vast majority of states have enacted legislation regarding the requirements for consumer notification after breaches that include personal information.[5] California led this trend of state disclosure laws when it adopted a law in 2003 that required companies and state agencies to give notice to the affected individuals after a data breach.[6] This law was the first state law that handled the importance of disclosures, and it increased awareness of this ongoing issue.[7] Unfortunately, the data security problem has gotten much worse since 2003.

There are a multitude of reasons why the number of data breaches is consistently rising.[8] First, the increasing use of the internet has resulted in Americans transmitting their personal data to online sources substantially more than in past decades.[9] Additionally, the rise in recent years of smart devices has expanded the privacy issues from personal computers and cell phones to cars, speakers, appliances, TVs, and many other products.[10] The rise in smart devices and internet related services certainly has benefits, such as personally tailored products.[11] However, once their personal information is obtained by the companies, customers often have no control over or knowledge regarding how the information is being handled.[12] Often, it is easy to trust that a large, successful company is devoting a reasonable amount of attention and resources to ensure the safety of their "cherished" customers' data. However, the rapid evolution of technology is being used for malicious purposes as well, and not all companies are taking adequate security measures to combat this.

In 2019, the business sector in the U.S. had 1,473 data breaches, ending the year with a 17% increase from the previous year.[13] Reports from mid-2020 listed the yearly breaches as being down 33% so far in

4. *Id.*

5. RITA TEHAN, CONG. RSCH. SERV., RL33199, DATA SECURITY BREACHES: CONTEXT AND INCIDENT SUMMARIES 3 (2007).

6. *Id.*

7. *Id.*

8. STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 1-2 (2019).

9. *Id.*

10. *Id.*

11. *Id.* at 2.

12. *Id.*

13. IDENTITY THEFT RES. CTR., 2019 END OF YEAR DATA BREACH REPORT 1 (2020) (noting that 2018 saw 1,257 data breaches).

comparison to mid-2019.[14] By June of 2020, there were only 540 publicly reported breaches.[15] The president and CEO of the Identity Theft Resource Center accredits the drop in data breaches to organizations being on higher alert due to mass amounts of employees working from home as a result of COVID-19.[16] The president believes that since working remotely causes all of the data to be at higher risk of interception, companies are paying attention to cybersecurity more than usual.[17] If this is truly the reason why data breaches are down as of mid-2020, it shows that companies are capable of being significantly more diligent in instituting preventative measures than they have been in recent years. The case law discussed in later sections surrounding corporate cyber breaches and the lack of adequate effort in preventing the unauthorized access of customers' personal data illustrates the massive impact some breaches have. A cyber insurance mandate for consumer companies is exactly what is needed to increase diligence regarding the protection of customer data.

Section I will dive into the current regulations regarding what the SEC expects of companies in cybersecurity systems and disclosures. This section will also detail three SEC actions that arose out of failures to meet the SEC standards in these areas. Section II will focus on the current incentives that companies have to avoid data breaches that arise out of cost and reputation damage after a breach occurs. Additionally, this section will list the misaligned incentives that seem to deter companies from implementing adequate systems and worsen the problem of customer data carelessness. This section will also briefly discuss four large data breaches and how these breaches affected the companies financially. Section III will outline the basic principles of cyber insurance and the current market. Section IV will explain how a cyber insurance mandate would assist with protecting customer data, limit negligent cyber procedures by companies, and assist companies in meeting the existing obligations under SEC standards. The final section will conclude the analysis.

I. CURRENT FEDERAL REGULATIONS FOR CYBERSECURITY

Guidance from the SEC regarding cybersecurity has improved in recent years. Sections from the Securities Act of 1933 (Securities Act) and the Securities Exchange Act of 1934 (Exchange Act) have been

14. Megan Leonhardt, *The Number of Data Breaches is Actually Down 33% So Far This Year—Here's Why*, CNBC: MAKE IT (July 14, 2020, 7:02 AM), https://www.cnbc.com/2020/07/14/number-of-data-breaches-down-33-percent-in-first-half-of-2020.html [https://perma.cc/9EW8-YSTH].

15. *Id.*

16. *Id.*

17. *Id.*

applied to instances of cybersecurity, though cybersecurity is not explicitly mentioned in either.[18] Commission statements from the SEC offer some additional guidance,[19] but there is still currently no specific timeline for necessary disclosures to be released to the public after a cyberattack. The SEC seems to use a "reasonableness" standard to determine how long after a breach disclosures should be made as well as how adequate a company's cybersecurity system should be to avoid penalties in the event of a data breach.[20] The current regulation for cybersecurity is important to this discussion because current regulation has not prevented many of the recent large data breaches caused by company negligence.

A. Securities Act of 1933

Though cybersecurity is not explicitly mentioned, the Securities Act discusses disclosure requirements that are important for companies to consider for the purposes of cybersecurity disclosures.[21] The Securities Act was written to ensure "full and fair disclosure of the character of securities sold in interstate and foreign commerce[.]"[22] The Securities Act requires companies to provide periodic disclosures regarding "the issuer, its business operations, its financial condition, its corporate governance principles, its use of investor funds, and other appropriate matters[.]"[23] Periodic disclosures can be requested by the SEC at its discretion to be made available to investors and filed with the SEC.[24] The Securities Act lists the reasoning for the necessity of these periodic disclosures as the protection of public interest and investors.[25] The Securities Act also requires fully adequate disclosures be listed in the registration statements as well.[26]

Though not explicitly mentioned, it can be inferred that cybersecurity risks and incidents should be included in periodic disclosures. The main point of these periodic disclosures is to protect investors.[27] Clearly, if a company had just faced a huge cyberattack where company files or customer information was retrieved by an unauthorized user, this would be relevant information for investors. Cybersecurity

18. *See generally* Securities Act of 1933, 15 U.S.C. §§ 77a-77aa; Securities Exchange Act of 1934, 15 U.S.C. §§ 78a-78qq.

19. *DF Disclosure Guidance: Topic No. 2*, U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/Y2Z2-NQN2] [hereinafter 2011 COMMISSION STATEMENT].

20. *Id.*

21. 15 U.S.C. § 77c(b)(4).

22. Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74.

23. 15 U.S.C. § 77c(b)(4).

24. *Id.*

25. *Id.*

26. *Id.* § 77g.

27. *See id.* § 77b(b).

disclosures should be included in the "other appropriate matters" portion of this section in the Securities Act.[28] It would be arguably more useful if the Act explicitly included cybersecurity disclosures to clarify for reluctant companies that cyber disclosures do need to be included.

Additionally, Section 77q(a)(2) of the Securities Act states that companies cannot "obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading[.]"[29] This section can be applied to cybersecurity disclosures since customers are still paying for the goods or services that the company provides until a disclosure is made and the customer can decide otherwise. Failure to disclose a cyberattack or other cyber incident should be seen as an omission of material fact. To leave customers without knowledge that their personal data had been compromised would certainly be misleading, as the statute prohibits.

Section 77q(a)(3) of the Securities Act states that registrants may not "engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser."[30] This section is different than Section 77q(a)(2) because it focuses on deceit instead of omission. This section would prohibit a company from lying to potential buyers about the condition of the cybersecurity systems or related cyberattacks. Though less helpful to customers than the previous section, this section prevents companies from selling to unknowing buyers after a large data breach. Cybersecurity information is certainly material in the modern era, and Sections 77q(a)(2) and (3) address the importance of material disclosures.[31]

B. Securities Exchange Act of 1934

Cybersecurity was also not explicitly mentioned in the Exchange Act. However, the Act includes relevant regulations that should be applied to cybersecurity disclosures. Section 78l of the Exchange Act requires issuers to submit periodic and current reports to make sure there is "fair dealing in the security."[32] Cybersecurity disclosures should be included in these reports if there is a risk or incident that is relevant to shareholders. Even though cybersecurity is not mentioned, the Exchange Act was enacted to prevent unfair practices within the

28. *Id.* § 77c(b)(4).
29. *Id.* § 77q(a)(2).
30. *Id.* § 77q(a)(3).
31. *Id.* § 77q(a)(2)-(3).
32. 15 U.S.C. § 78l.

market.[33] These required reports under the Exchange Act should include relevant cybersecurity disclosures because it is clearly the type of information the Act was trying to make companies disclose.

Additionally, Exchange Act Rule 13a-15(a) requires companies to maintain internal control over finances.[34] This rule is meant to keep confidential details inside the company to prevent unauthorized access to customer information.[35] Specifically, Sections 78m(b)(2)(B)(i) and (iii) of the Exchange Act require certain issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization; . . . [and that] (iii) access to assets is permitted only in accordance with management's general or specific authorization[.]"[36] This regulation ensures that financial data is being kept on specific servers instead of being frequently transferred and put at risk.

C. 2011 Commission Statement

The 2011 Commission Statement references the existing federal securities laws and how they require the disclosure of "information about risks and events that a reasonable investor would consider important to an investment decision."[37] Though the requirements only generally mention cybersecurity, the obligation of disclosure still arises under existing regulation regarding cybersecurity risks and incidents.[38] The statement mentions that companies should also disclose the risk of potential cyber incidents if necessary.[39] To determine if the disclosure is necessary, the SEC statement recommends that companies evaluate the frequency and severity of prior cyber incidents.[40] These suggestions are not very specific and do not address the many intricate problems that arise under cybersecurity disclosures. Specifically, the 2011 statement does not address any preventative actions companies should take to keep files safe. The lack of guidance in this area is not helpful to the protection of customer data. Perhaps if the SEC would outline more specific guidelines in its commission statements or regulations, companies would be more interested in cybersecurity.

33. Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881.
34. 17 C.F.R. § 240.13a-15(a) (2020).
35. *See id.*
36. 15 U.S.C. § 78m(b)(2)(B)(i)-(iii).
37. 2011 COMMISSION STATEMENT, *supra* note 19.
38. *Id.*
39. *Id.*
40. *Id.*

D. 2018 Commission Statement

The 2018 Commission Statement provides more guidance on the suggested handling of cybersecurity matters.[41] The statement addresses two areas not formally addressed in the 2011 statement, which were "the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context."[42] The statement addressed the time aspect of disclosures by stating that public companies need to inform investors of cybersecurity risks and other material incidents in a timely fashion.[43] Though this is more guidance than the 2011 statement, "timely fashion" is not very specific and is completely open to interpretation.[44] The statement encourages companies to educate relevant constituents about risks and prior cybersecurity incidents in order to develop effective disclosure procedures.[45] The 2018 statement establishes the requirement of companies to create "effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events[.]"[46]

In relation to the insider trading issue, the statement addresses the need to "refrain from making selective disclosures of material nonpublic information" in regard to cybersecurity risks and incidents.[47] Next, the statement lists examples of forms where registrants should include relevant risks and incidents such as periodic reports, Securities Act and Exchange Act registration statements, and current reports.[48] The statement warns companies that are making cybersecurity disclosures to refrain from disclosing "roadmap[s]" that would compromise their cybersecurity efforts by providing too much detail on the technicalities.[49] Overall, the 2018 statement does provide more detail regarding the necessity of cybersecurity disclosures and adequate procedures, but it fails to address the exact disclosure timeline that companies need to follow to avoid liability.

E. Federal Regulation 17 C.F.R. § 248.30

While there is no shortage of vague language in the previously mentioned regulations and statements, Federal Regulation 17 C.F.R. § 248.30 provides some much needed clarity regarding disclosures for

41. *See* U.S. SEC. & EXCH. COMM'N, 17 CFR PARTS 229 & 249: COMMISSION STATEMENT AND GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES (2018) [hereinafter 2018 COMMISSION STATEMENT].

42. *Id.* at 6.

43. *Id.* at 4.

44. *Id.*

45. *Id.* at 4-5.

46. *Id.* at 6-7.

47. *Id.* at 7.

48. *Id.* at 8-10.

49. *Id.* at 11.

cyber incidents and attacks.[50] This regulation provides that companies must "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[51] The regulation goes on to require those mentioned policies to insure confidentially of customer information, protect against any threats to security, and eliminate the unauthorized access of customer records that may cause harm or inconvenience to the customer.[52] This regulation applies to brokers, investment companies, investment advisors, and dealers registered with the SEC.[53] This regulation explicitly addresses the issue at hand: the obligations a company has regarding cybersecurity systems.[54]

F. SEC Investigations and Penalties

While discussion of the relevant regulation of cybersecurity is very important, it is equally important to see these regulations at work through prosecution by the SEC. The Division of Enforcement under the SEC investigates and prosecutes companies registered with the SEC for violating applicable federal laws, which include those regarding cybersecurity.[55] The SEC prosecutes violators of federal regulations in civil actions.[56] In some cases, companies in violation of cybersecurity regulations will come to a settlement agreement with the SEC.[57] The Division of Enforcement investigates, charges, and prosecutes all violators to ensure investors and customers are protected from corporate wrongdoing.[58]

1. SEC Action Against Yahoo

For example, in 2018, the SEC reached a settlement with formally Yahoo! Inc. (Yahoo), which was the first public company that the SEC prosecuted for failure to disclose a data breach.[59] In 2014, Yahoo learned that it was involved in a massive data breach and failed to disclose the breach until almost two years later.[60] The personal data of

50. 17 C.F.R. § 248.30 (2020).

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. *About the Division of Enforcement*, U.S. SEC. EXCH. COMM'N (Aug. 2, 2007), https://www.sec.gov/enforce/Article/enforce-about.html [https://perma.cc/BD8N-SQKJ].

56. *Id.*

57. *See* Altaba Inc., Exch. Act Release No. 83096 (Apr. 24, 2018).

58. *About the Division of Enforcement*, *supra* note 55.

59. Derek Kearl, *SEC Issues First Ever Enforcement Action For Failure to Disclose a Data Breach, Obtaining $35 Million Penalty*, HOLLAND & HART (May 18, 2018), https://www.hollandhart.com/sec-issues-first-ever-enforcement-action-for-failure-to-disclose-a-data-breach-obtaining-35-million-penalty [https://perma.cc/X77A-HBKL].

60. Altaba Inc., Exch. Act Release No. 83096, at 2 (Apr. 24, 2018).

Yahoo's customers was stolen during the breach. Therefore, the breach was a material event that should have been disclosed to customers in a reasonable time.[61] The SEC charged Yahoo with violating Section 13(a) of the Exchange Act and Sections 17(a)(2) and 17(a)(3) of the Securities Act, along with multiple other SEC rules.[62] Yahoo agreed to settle the action with the SEC for $35 million.[63] This action illustrates that the SEC is not tolerant of public companies failing to disclose cyberattacks or other incidents within a reasonable about of time.

2. SEC Action Against R.T. Jones Capital Equities Management

In addition to instances where the company fails to disclose a cyber breach in a timely fashion to customers, the SEC also prosecutes companies for failing to set up adequate policies and procedures under 17 C.F.R. § 248.30.[64] In 2015, the SEC settled with R.T. Jones Capital Equities Management (R.T. Jones), an investment advisor, which was charged with failing to comply with 17 C.F.R. § 248.30.[65] R.T. Jones failed to adopt adequate procedures to protect customer data from unauthorized access.[66] A data breach of R.T. Jones' system occurred in 2013 where hackers accessed the personal information of 100,000 individuals.[67] Though R.T. Jones did disclose the breach to the affected customers, the SEC brought the action because R.T. Jones did not implement the cybersecurity policies and procedures that are required.[68] R.T. Jones settled with the SEC for $75,000.[69]

3. SEC Action Against Morgan Stanley Smith Barney LLC

Additionally, a similar situation occurred in the SEC action against Morgan Stanley Smith Barney LLC.[70] From 2011-2014, Morgan Stanley Smith Barney LLC had a security breach where customer information was retrieved and sold online due to a lack of adequate cybersecurity.[71] The breach occurred because a then-employee of the firm, Galen Marsh, transferred 730,000 accounts to his personal server,

61. *Id.*

62. *Id.*

63. *Id.* at 9.

64. *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach*, U.S. SEC. EXCH. COMM'N (Sept. 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html [https://perma.cc/H5QF-LEQJ].

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

70. *SEC: Morgan Stanley Failed to Safeguard Customer Data*, U.S. SEC. EXCH. COMM'N (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html [https://perma.cc/8MLF-6BWK].

71. *Id.*

where the information was accessed by a third party.[72] The reason the firm was prosecuted was that it failed to implement the necessary policies that would have prohibited such careless movement of data to unprotected servers.[73] The company agreed to pay a $1 million penalty in a settlement for failing to protect customer information.[74] Also, Marsh was criminally convicted and received thirty-six months of probation.[75] Both the R.T. Jones and Morgan Stanley Smith Barney LLC actions show that the SEC is not tolerant of companies failing to ensure adequate policies and procedures for potential data breaches.

II. INCENTIVES AND MISALIGNED INCENTIVES FOR ADEQUATE CYBERSECURITY

This discussion of protecting customer data requires the evaluation of current incentives for companies to ensure adequate cybersecurity. The 2018 SEC Commission Statement mentions many of the costs that companies face when they fall victim to cyberattacks or other cyber incidents.[76] According to a 2017 survey by Ponemon Institute and IBM Security, the average cost for a company after a data breach was $7.35 million.[77] These costs should act as a deterrent for careless cybersecurity policies. The important question is whether these costs outweigh the costs of adequate cybersecurity measures.

There are many different factors that make up the total cost of a data breach. The first factor that should act as an incentive for companies to avoid cyberattacks is remediation costs.[78] Remediation costs include the company's liability for the information that was stolen, customer incentives, and system repair.[79] Though there is minimal regulation regarding how companies should compensate customers after a data breach, companies are still motivated to provide incentives in hopes of maintaining the relationship.[80] This same motivation may cause the company to provide similar incentives to business partners.[81] Additionally, remediation costs may include any ransom payments to perpetrators of ransomware attacks.[82] Remediation is just one of the measures that companies must take after a cyber breach.

Another cost that should act as an incentive for companies to avoid cyberattacks is the cost of enhanced cybersecurity measures after an

72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. 2018 COMMISSION STATEMENT, *supra* note 41, at 3-4.
77. PONEMON INST., 2017 COST OF A DATA BREACH STUDY 5 (2017).
78. 2018 COMMISSION STATEMENT, *supra* note 41, at 3.
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.* at 3 n.6.

attack.[83] A reasonable company would work to increase protection of company and client information in the aftermath of a data breach. These costs may include hiring experts, retraining employees, new cybersecurity protection equipment, and the cost of other desired organizational changes.[84] If the breach was caused by outdated cybersecurity systems, the company will likely work to properly modernize its system, which will be costly. Lessons learned from cyberattacks will result in an increase in expenditures and company efforts to prevent similar events from reoccurring.

Other costs that companies face resulting from cyber breaches include failure to retain or attract customers, litigation costs, cyber insurance, reputational damage, and market value damage.[85] Legal costs can include any regulatory costs incurred from actions by state, federal, or non-U.S. authorities.[86] Many times, large security breaches will be featured on front line news channels, which hurts the company's public image. News coverage is especially damaging to the company's reputation if the company is found to have not adequately protected customer information. Though all of the costs mentioned seem like they should be adequate deterrence from handling cybersecurity procedures negligently, companies are still currently being prosecuted for careless behavior.

There are many expenses associated with creating a strong cybersecurity system that may outweigh the expenses of a potential data breach.[87] These factors working against the adequate protection of customer information are misaligned incentives. Security administration, updates, and oversight costs for adequate cybersecurity are extremely expensive to maintain for an indefinite period of time.[88] Additionally, obtaining information about the cyber industry and its best practices is costly as well.[89] Some larger companies invest in insurance and take advantage of the fact that the expense burden of a data breach would mostly fall on the insurance provider.[90] The problem is that often cyber insurance is more expensive than the prospective costs of a data breach.[91] This failing system of nonaccountability is putting consumers at risk of their personal information being easily retrieved.

83. *Id.* at 3.
84. *Id.*
85. *Id.* at 4.
86. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.0 (2017); 2016 O.J. (L 119) 1.
87. Miller, *supra* note 3, at 158.
88. *Id.*
89. *Id.*
90. *Id.* at 159.
91. Miller, *supra* note 3, at 180.

A. 2013 Target Data Breach

For example, in 2013, Target was hacked and the hackers stole the credit and debit card information of around forty million customers.[92] Along with the financial information of the forty million customers, the hackers also retrieved seventy million other customers' information, which included home addresses and phone numbers.[93] Target was sued by customers in 2014 for negligence regarding its cybersecurity procedures.[94] Specifically, customers believed that their data was able to be stolen from Target's servers because Target did not have sufficient cybersecurity to prevent the breach.[95] So, as a result of Target's alleged negligence within its cybersecurity systems and developments, the personal information of approximately 110 million people was accessed by hackers.

In 2017, Target ended up settling claims with customers in forty-seven states for $18.5 million.[96] After paying all related expenses, including the settlement amount, the data breach costed Target $252 million.[97] Target's insurance reimbursed Target for $90 million.[98] Another $57 million was deducted from the total net loss since cyber breach related expenses are tax deductible.[99] After everything was said and done, Target paid $105 million for the data breach that affected millions of its customers.[100] Though this seems like a hefty amount, $105 million was roughly 0.1% of Target's sales in 2014.[101] It could be argued that negligence in cybersecurity should inflict more damage than a loss of 0.1% earnings. This kind of low financial impact is part of the reason that expensive cybersecurity systems may not be in a company's best financial interest.

---

92. *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 484 (D. Minn. 2015).

93. Michael Kassner, *Data Breaches May Cost Less Than the Security to Prevent Them*, TECHREPUBLIC (Apr. 9, 2015, 12:45 PM), https://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/ [https://perma.cc/Q8Q6-BDMA].

94. *Target*, 309 F.R.D. at 485.

95. *Id.*

96. *Target Settles 2013 Hacked Customer Data Breach For $18.5 Million*, NBC NEWS (May 24, 2017, 10:49 AM), https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031 [https://perma.cc/Q997-EG8M].

97. Kassner, *supra* note 93.

98. *See id.*

99. *See id.*

100. *Id.*

101. *Id.*

B. 2013 Adobe Data Breach

In 2013, Adobe's systems were hacked, and the hackers accessed information from credit card transactions of thirty-eight million users.[102] Adobe failed to warn the affected customers or provide them with adequate credit monitoring services within a reasonable amount of time.[103] Additionally, Adobe misled customers to believe that its cybersecurity system was better than what it was, even though Adobe knew its systems were not up to par with the rest of the industry.[104] Adobe was sued by customers of multiple states and ended up paying $1.1 million for the plaintiffs' attorney fees.[105] The lawsuit also resulted in a mandatory audit of Adobe's cybersecurity systems to ensure that it had implemented new security measures that would adequately protect customer information.[106] However, Adobe's reported revenue from 2013 was $4.06 billion.[107] The settlement hardly put a dent in Adobe's cash flow.

C. 2014 Home Depot Data Breach

In 2014, Home Depot's system was breached, and the hackers stole the credit card information of around fifty-six million customers.[108] Banks from several states then sued Home Depot for damages.[109] Home Depot settled with the banks for $25 million.[110] All expenses from the breach, including the settlement, totaled to $43 million.[111] Home Depot's insurance reimbursed it for $15 million of that total, leaving the out of pocket cost for Home Depot at $28 million.[112] This total out of pocket cost for Home Depot equaled only .01% of its total sales in 2014.[113] This is yet another example of low financial impact for inadequate cybersecurity systems.

---

102. Jason Schossler, *Adobe Settles Data Breach Suit, Will Pay $1 Million in Legal Costs: In re* Adobe Sys. Priv. Litig., 33 No. 7 WESTLAW J. COMPUT. & INTERNET 8, 1 (2015).

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.* at 2.

107. *Adobe's Cloud Innovations Drive Strong Q4 and FY2013 Financial Results*, ADOBE (Dec. 12, 2013), https://www.adobe.com/content/dam/cc/en/investor-relations/pdfs/Q413Earnings.pdf [https://perma.cc/DWL3-G778].

108. *In re*: Home Depot, Inc. Customer Data Sec. Breach Litig., 65 F. Supp. 3d 1398, 1399 (J.P.M.L. 2014).

109. *Id.*

110. Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, FORTUNE (Mar. 9, 2017), https://fortune.com/2017/03/09/home-depot-data-breach-banks/ [https://perma.cc/4AF8-WEDB].

111. *See* Kassner, *supra* note 93.

112. *Id.*

113. *Id.*

D. 2014 Yahoo! Data Breach

Though already briefly mentioned, the Yahoo case is very important to this conversation about cyber insurance. Yahoo is a platform that customers use for email, photo storage, bank accounts, stock trading accounts, and medical information storage.[114] Some users, such as small businesses, provide Yahoo with their credit and debit card numbers as well.[115] Users of Yahoo's services sued Yahoo for punitive damages regarding three security breaches that occurred within a period of five years.[116] The users who were suing Yahoo claimed that Yahoo should have already been on notice of its data security issues.[117] In 2010, Google informed Yahoo that its network had been compromised and hackers were using Yahoo's systems to attempt to breach Google's system.[118] In 2012, Yahoo was breached during an SQL injection attack as well.[119] It would seem that after these cyberattacks, Yahoo would have been on notice regarding its inadequate cybersecurity. However, the three breaches in question in this lawsuit occurred because Yahoo had once again failed to adequately protect user data.

The first breach that the users sued over occurred in 2013.[120] In the process of the 2013 breach, hackers "stole users' Yahoo logins, country codes, recovery emails, dates of birth, hashed passwords, cell phone numbers, and zip codes."[121] This breach affected all three billion user accounts at Yahoo.[122] There is speculation that the breach was caused by Yahoo's use of outdated encryption technology.[123] Yahoo did not disclose the 2013 breach to the public until three years after it occurred.[124] Yahoo experienced another breach in 2014, where hackers stole the personal data of 500 million Yahoo users.[125] The stolen user information was then posted for sale on the dark web.[126] The 2014 breach was not publicly disclosed until two years after the breach occurred.[127]

---

114. *In re*: Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1120 (N.D. Cal. 2018).

115. *Id.*

116. *Id.* at 1121, 1129.

117. *Id.* at 1121.

118. *Id.* at 1121.

119. *Id.*

120. *In re*: Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1122 (N.D. Cal. 2018).

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *In re*: Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1122 (N.D. Cal. 2018).

127. *Id.* at 1123.

The final Yahoo data breach that users sued the company over occurred sometime in 2015-2016.[128] In the 2015-2016 breach, the same hackers from the 2014 breach used forged cookies to hack the accounts of even more Yahoo users.[129] Yahoo did not notify users about the 2015-2016 breach until 2017.[130] Some of the injuries that users suffered from the data breaches from 2013 to 2016 included stolen social security benefits, credit score damage, expenses for credit monitoring services, missed financial deadlines resulting in fees, fraudulent credit card charges, unsolicited requests, and many other fraudulent activities that affected the users' day to day lives.[131]

Yahoo settled with the users in this class action suit for $117.5 million.[132] Users who had a Yahoo account from January 1, 2012, to December 31, 2016 could join the class action and benefit from the settlement funds or receive free credit monitoring services.[133] Yahoo's revenue in the final quarter of 2017 was $1.33 billion.[134] Though this is the highest settlement discussed in this section by far, it is important to keep in mind that the settlement covered three main data breaches along with two others which affected a total of more than three billion users.[135] Though Yahoo had plenty of notice from the early 2000s that its cybersecurity systems were ineffective, three more large, successful data breaches harmed many users in the years that followed. Yahoo lacked incentive to improve its data security. It seems Yahoo did not update its cybersecurity systems, despite many cyber incidents, because it could easily pay the penalties and settlement amounts and move on.

III. CYBER INSURANCE OVERVIEW

Cyber insurance is insurance that companies can get in order to alleviate some of the out of pocket costs resulting from cyberattacks.[136] Cyber insurance covers damages and other claims against the insured

128. *Id.*

129. *Id.*

130. *Id.* at 1123-24.

131. *Id.* at 1125.

132. *Yahoo! Inc. Customer Data Security Breach Litigation Settlement*, YAHOO! INC., https://yahoodatabreachsettlement.com [https://perma.cc/A22U-CEBB] (last visited July 22, 2021).

133. *Id.*

134. Anita Balakrishnan, *In Last Hurrah, Yahoo Revenue Jumps 22% as Quarterly Earnings Smash Expectations*, CNBC (Apr. 18, 2017, 6:20 PM), https://www.cnbc.com/2017/04/18/yahoo-earnings-q1-2017.html [https://perma.cc/6GAZ-BAYB].

135. *In re*: Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1122 (N.D. Cal. 2018).

136. Judy Selby, *Removing the Mystery from Cyber Insurance: Insuring Against Digital Attacks Requires a New Form of Insurance that Most Firms Now Need to Protect Their Business*, L. PRAC. Jan./Feb. 2019, at 51.

company resulting from a cyber incident.[137] Though the sales of cyber insurance are gradually rising in the U.S., the market for cyber insurance is much different from that of other insurances.[138] Since cyber insurance is a relatively new concept, the current policy offerings are erratic.[139] In 2019, there were only approximately sixty carriers of cyber insurance.[140] There is no standard cyber insurance policy yet, and the existing polices constantly change with industry trends and as cyber risks evolve with technology.[141] Current cybersecurity insurance policies offer both first-party and third-party coverage.[142]

To obtain cyber insurance, companies typically have to answer questions about company size, volume of data handled, existing cybersecurity systems, previous cybersecurity incidents, financial information, and awareness of existing issues that may give rise to a claim.[143] There are several reasons why cyber insurance has not completely taken off in the market yet. First, large data breaches are a problem that has arisen in the modern era.[144] This newer problem of large cyberattacks has not generated a lot of case law yet.[145] The parameters of liability for companies that fall victim to these cyber breaches have not been completely dictated yet.[146] Due to these lack of parameters, injured parties have had to resort to filing creative claims in response to data breaches.[147] Until there is more of a precedent set for these kinds of cases, the fluctuating details of cyber insurance policies and the skepticism of their necessity will continue.

Since there is no standard cyber insurance policy for companies to adopt, shopping for cyber insurance is not an easy task for companies.[148] There are numerous varying policies covering different cyber risks offered by different insurers, making it difficult to get a grasp of the market.[149] This lack of a standard policy makes buying cyber insurance harder for companies than buying other types of insurance. It also creates a lack of standard pricing, which acts as a deterrent for getting the insurance in the first place.

---

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.*

142. *Id.* at 51-52.

143. *Id.* at 52.

144. Jes Alexander, *Anatomy of a Data Breach–What Cyber Policies Should Cover,* 13 J. TEX. INS. L. 5, 5 (2015).

145. *Id.*

146. *Id.*

147. *Id.*

148. *See id.*

149. *Id.*

IV. PROPOSAL

Cyber insurance should be mandatory for companies that sell goods or services to the public. The SEC needs to adopt a regulation that requires companies to set up cyber insurance policies immediately. This would decrease the careless handling of customer data. This mandate should not apply to organizations that only deal with other organizations and not the public. In this day and age, technology is advancing rapidly. The cases described in the preceding sections demonstrate the severity of this issue and how companies, even large reputable ones, are not taking adequate measures to protect customer data. The public is having credit card numbers accessed by unauthorized parties, credit scores destroyed, and fraudulent activity performed using its credentials.[150] The best way to help slow the devastating effects of cyberattacks on customers is to ensure that companies are doing everything in their power to protect customer information. Since case history shows that companies will not take these steps on their own, it is necessary to mandate that companies obtain cyber insurance.

There are many details of the structure of a cyber insurance mandate that must be addressed. Obviously, small local companies should not have the same premiums as large corporations. There would need to be a sliding scale, similar to other insurances, that would make premiums reasonably affordable for each company. This scale should be based on attributes similar to those that current cyber insurance providers look at, such as size of the company, previous cyber incidents, and magnitude of company data.[151] Each company would need to disclose pertinent information to the insurance provider so that it could do the proper screening to gauge the level of risk that the company poses. By mandating companies obtain cyber insurance, insurance providers would eventually develop a standard plan, similar to liability insurance for motor vehicles. The standard plan needs to include both first-party and third-party coverage to ensure both internal company mistakes and unauthorized breaches are covered. Then, if a company continues to show cybersecurity negligence regarding its procedures despite the implementation of cyber insurance, the consequence should be its premium rising substantially.

Mandating cyber insurance would solve many of the problems currently preventing voluntary, widespread purchase of cyber insurance. Smaller companies are unlikely to purchase cyber insurance without a mandate because of high premium rates caused by minimal participation in the market. The lack of revenue in the current cybersecurity insurance pool causes less effective policies and higher premiums. Re-

150. *E.g.*, *In re*: Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1125 (N.D. Cal. 2018).

151. Selby, *supra* note 136, at 52.

quiring all companies, even smaller and seemingly lower-risk companies, to buy cyber insurance would balance out the scale and help ensure that all customer data is being reasonably protected. Though it may seem unfair to have small, low-cyber-risk companies share this burden that falls mostly on large companies, this is how many insurance systems work. In the ideal system, the premium rates for small, low-earning companies would be manageable for their budgets. This is the best system to ensure that customer data is being adequately protected with the smallest burden imposed on each individual company.

Mandatory cyber insurance would increase cyber accountability for companies. Currently, with no mandate, some companies are acting negligently with customer data and overall cybersecurity procedures because the costs of a possible cyber breach are less than that of cyber insurance or expensive, high-class cybersecurity systems.[152] A cyber insurance mandate would require companies to pay a premium as well as a significant deductible in the event of a cyberattack. This would ideally motivate companies to keep cybersecurity procedures up to date and give employees adequate cybersecurity training. Additionally, the insurance providers may develop policies with procedures for lowering premiums if companies invest in additional security measures that would increase overall cybersecurity. This idea is similar to how car insurance providers take into account the car's existing safety measures as well as the driver's history. This type of policy would motivate companies to invest in extra security measures to lower their premiums. The accountability that cyber insurance providers could provide for companies by regularly checking in on cybersecurity systems to ensure adequate protections is crucial in this quest to protect customer data.

A new SEC regulation that requires companies to adopt cyber insurance would help companies fulfill the already existing obligations under federal securities acts. Information regarding the cyber insurance policy, such as cyber insurance claims, would need to be disclosed in the periodic disclosures that the Securities Act requires.[153] Additionally, obtaining cyber insurance would help companies avoid violating Section 77q(a)(2) of the Securities Act, which prohibits companies from making a profit through providing misleading or false information.[154] Cyber insurance would create an accountability dynamic that would make it more difficult for companies to hide inadequacies in cyber protection systems and mislead investors.

Mandatory cyber insurance would help achieve one of the main goals of the Securities Act: to protect the public interest and investors'

152. *See* Miller, *supra* note 3, at 158, 180.

153. 15 U.S.C. § 77c(b)(4).

154. *Id.* at § 77q(a)(2).

rights.[155] Additionally, mandatory cyber insurance would help the SEC avoid making specific determinations about the exact timeline in which disclosures should be made after a breach. Many of the SEC's vague suggestions and comments could finally be put to rest since companies would now have the insurance provider to answer to. In a way, cyber insurance providers would work as a sort of gatekeeper for unethical and illegal behavior involving cybersecurity. If all companies that deal with the public were required to have cyber insurance, there would be a third party constantly concerned about the wellbeing of companies' cybersecurity.

In addition to the implications that mandatory cyber insurance would have on the obligations arising out of the Securities Act, mandatory cyber insurance would also assist companies in complying with Federal Regulation 17 C.F.R. § 248.30.[156] By obtaining mandatory cyber insurance, companies would be doing exactly what is required in this regulation, which is to adopt policies and procedures to protect customer information.[157] Cyber insurance would help protect customer information because it would cause companies to adopt any additional cybersecurity measures that the insurance provider suggests, motivate companies to avoid breaches of customer data to avoid costly policy increases, and ensure that companies are taking the issue seriously once they realize that the SEC will no longer tolerate carelessness.

This proposal is certainly not without drawbacks. First, the moral hazard problem exists in any insurance dynamic. The cyber insurance provider is unable to monitor the company every day to ensure no cybersecurity negligence is occurring. The idea is that the deductible will be enough motivation for companies to use due care, but not all companies will take the system seriously. Though there is no way to fully monitor the cybersecurity of every single company to ensure no breach ever occurs, this system will improve the current system by adding an extra layer of accountability. Another issue with this proposal is that large companies may still act negligently with cybersecurity even while they are insured since they can easily afford to pay any deductible. This issue would hopefully be resolved by frequent monitoring by the insurance provider as well as increasing deductibles and premiums with each cyber incident that occurs. Eventually, careless companies would be paying a very high price for coverage if there is a repetition of incidents.

An additional issue with this proposal is that mandating cyber insurance may increase the temptation for companies to not disclose cyberattacks. The timely disclosure of cyberattacks is crucial for affected customers, hence why companies are held liable when they fail

155. *See id.* at § 77c(b)(4).

156. 17 C.F.R. § 248.30 (2020).

157. *Id.*

to disclose attacks in a reasonable amount of time. The pressure of a deductible and higher price for coverage in the future may motivate companies to try to keep cyberattacks quiet and out of the public eye. This is the exact opposite effect of what the proposal is trying to have. The goal is to motivate companies to work with insurance providers in hopes of improving cybersecurity systems and benefiting everyone. Unfortunately, not all companies will easily fall in line with this idea, and some may do even more harm to customers in the process of trying to cheat this system. Other drawbacks to this proposal include the enforcement cost and extra administrative time. These costs are burdens that the SEC must bear if its mission is truly to protect customers and investors.

CONCLUSION

Technology is constantly evolving, and the guidelines for cybersecurity should be as well. There are currently not enough incentives to motivate companies to protect customer data. Even considering all of the costs of a data breach, statistics show that those costs only account for a mere fraction of the company's revenue for the year of the breach.[158] Companies are run by humans who have a natural instinct to believe that nothing bad will happen to them. This is simply not the case for unpredictable cyberattacks. Mandatory cyber insurance would add an extra layer of accountability for companies to help ensure that customer data is being protected to the fullest possible extent. Even though implementation of such a mandate would have a few drawbacks, the benefits of the mandate would outweigh any inconvenience caused by it. Customers deserve to have their data protected to the most reasonable extent possible, and that is unlikely to occur until there is a cyber insurance mandate.

158. Kassner, *supra* note 93.