Minnesota Journal of Law, Science & Technology

Volume 18 | Issue 1 Article 8

1-2017

Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches

Minhquang N. Trang

Note

Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches

*Minhquang N. Trang**

INTRODUCTION

This article will recommend that hospitals, banks, and major corporations be compelled to purchase cyber-liability insurance in order to outsource corporate cybersecurity regulation to the insurance industry. The ever-expanding nature of cyber threats makes them difficult for federal agencies to regulate with the limited resources available.[1] A compulsory cyber-liability regime ensures that modern, updated cybersecurity standards are implemented to help prevent data breaches and mitigate damages.

Cyber-attacks that target personal, private information are increasing in frequency and are difficult to prevent entirely.[2] FBI Director James Comey stated that "there are two kinds of big companies in the United States . . . those who've been hacked . . . and those who don't know they've been hacked."[3]

---

* J.D. Candidate 2017, University of Minnesota Law School; B.A. 2010, University of Illinois Urbana-Champaign.

1. *See generally Cyber-Attacks: Threats, Regulatory Reaction and Practical Proactive Measures to Help Avoid Risk*, KATTEN L. (June 24, 2015), https://www.kattenlaw.com/Cyber-Attacks-Threats-Regulatory-Reaction-and-Practical-Proactive-Measures-to-Help-Avoid-Risks (discussing the current status of cyber threats, the regulations that seek to prevent them, and suggested legislative action going forward).

2. *See* STEVEN R. GILFORD, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 16:1 (Kristen J. Matthews ed., 2016); *see also The Cost and Frequency of Cyber Attacks on the Rise*, HELP NET SECURITY (Oct. 9, 2013), https://www.helpnetsecurity.com/2013/10/09/the-cost-and-frequency-of-cyber-attacks-on-the-rise/.

3. *See* James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014), http://www.businessinsider.com/fbi-

Because corporate cyber-attacks may significantly harm the public through the unintended disclosure of private information[4], this article will explore compulsory cyber-liability insurance and the benefits of having the insurance industry act as a private regulator.

Businesses operations are dependent on data and information technology.[5] Corporations collect and store sensitive and personal information from millions of consumers, including credit card information, social security numbers, and even medical history.[6] According to NetDiligence,[7] personal information was improperly exposed in eighty-six percent of data breaches in 2015.[8] The SANS Institute[9] estimates that over fifty-three million people had their personal information exposed in 2005.[10] Hackers use the personal information for illegal purposes that harm those who identify with that

---

director-china-has-hacked-every-big-us-company-2014-10 (citing FBI Director James Comey's remarks concerning international hacking by Chinese hackers).

4. *Cyber Claims Study*, NETDILIGENCE 3 (2015), https://netdiligence.com /wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015 .pdf (noting that the healthcare sector experiences the second largest amount of breaches (21% of total breaches), followed by the financial sector (17% of total breaches)).

5. PWC, INSURANCE 2020 & BEYOND: REAPING THE DIVIDENDS OF CYBER RESILIENCE 7 (2015), http://www.pwc.com/gx/en/insurance/publications/assets /reaping-dividends-cyber-resilience.pdf ("The digital revolution has created a highly interconnected world that is awash with data, much of it sensitive."); *see also* GUIDE FOR CONDUCTING RISK ASSESSMENTS, NAT'L INST. OF STANDARDS & TECH. 1 (Sept. 2012), http://nvlpubs.nist.gov/nistpubs/Legacy /SP/nistspecialpublication800-30r1.pdf ("Organizations in the public and private sectors depend on information technology.").

6. *See Cyber Claims Study*, *supra* note 4, at 11; *see also* NAT'L INST. OF STANDARDS & TECH., *supra* note 5, app. B, at B-7 (suggesting certain standards companies should adopt in their data protection regimes).

7. NetDiligence is a privately held cyber risk assessment and data breach services company. *See About*, NETDILIGENCE, http://netdiligence.com /pages/about/ (last visited Sept. 9, 2016).

8. NETDILIGENCE, *supra* note 4, at 3.

9. The SANS Institute is a cooperative research and education organization in security. The organization has trained more than 165,000 security professionals around the world. *See About*, SANS INST., https://www.sans.org/about/ (last visited Sept. 9, 2016).

10. Peter Gordon, *Data Leakage – Threats and Mitigation*, SANS INST. 18 (Oct. 15, 2007), https://www.sans.org/reading-room/whitepapers/awareness /data-leakage-threats-mitigation-1931.

information.[11] For example, cybercriminals may sell stolen information on black markets, use the information to access bank accounts, extort companies, or trade on insider information.[12] Occasionally, employees inadvertently cause a security incident,[13] which can be as devastating as an intentional, malicious hack.[14] Cybercrimes can be costly and challenging to detect.[15]

As a result, companies experience business interruptions and are then incapable of meeting contractual obligations when their data is lost or distorted.[16] Cyber breaches may account for more than $400 billion in losses annually.[17] Corporate boards of directors face both class action lawsuits filed by those who had their private information stolen and suits filed by affected

---

11. *Id*. at 18–19 (discussing hacker use of stolen credit card and other personal information).

12. *See* BURT WELLS ET AL., 4 NEW APPLEMAN ON INSURANCE LAW & PRACTICE § 29.01[2][a][iv] (Jeffrey E. Thomas ed., 2016).

13. A security incident is "an event that violates an organization's security or privacy policies involving sensitive information." Rick Kam, *What's in a Name? Defining Event vs. Security Incident vs. Data Breach*, IDEXPERTS (July 8, 2015), https://www2.idexpertscorp.com/blog/single/whats-in-a-name-defining-event-vs.-security-incident-vs.-data-breach. Data breaches "are a serious type of security incident that involves the release of personally sensitive, protected and/or confidential data." A small percentage of security incidents escalate into data breaches. *See id.*; Kate Brew, *What's the Difference Between a Data Breach and a Security Incident?*, ALIEN VAULT (Dec. 30, 2014), https://www.alienvault.com/blogs/security-essentials/whats-the-difference-between-a-data-breach-and-a-security-incident.

14. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 5, at 10 (explaining how predisposing conditions that exist within an organization, such as lack of employee training, increases the likelihood of cyber-attacks); *see also* David Emm et al*., IT Threat Evolution in Q2 2015*, KASPERSKY LAB 4 (July 30, 2015), https://securelist.com/analysis/quarterly-malware-reports/71610/it-threat-evolution-q2-2015/ (demonstrating how cyber espionage hacker CozyDuke used malware emails in ways that encourage employees to distribute the malware to other employees by embedding the malware in a funny video stream).

15. *See generally* Gordon M. Snow, Assistant Dir. Cyber Div., Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, (Apr. 12, 2011) (transcript available at https://archives.fbi.gov/archives/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism) (speaking on the current state of cybercrime, the costs associated with such crime, and the difficulty in combating cybercrime).

16. *See* GILFORD, *supra* note 2, at § 16:1 ("[B]usiness interruption, inability to perform obligations to others, and loss or distortion of company and client data.").

17. PWC, *supra* note 5, at 4.

financial institutions.[18] More recently, boards of directors have also been subject to derivative lawsuits filed by their shareholders for damages caused by cyber breaches.[19] This notion is evidenced by the derivative suits filed against the boards at Sony, Wyndham Worldwide, and Target by their shareholders.[20]

The first part of this article will discuss the current state of corporate cybersecurity risks and cyber-liability insurance coverage. Part II will explore the policies behind compulsory insurance and explain why those policies apply to cybersecurity risks. Part III will address counter-arguments against a compulsory cyber-liability insurance regime. Part IV will explore necessary components in mandatory coverage and the obstacles in implementation.

I. CURRENT CYBERSECURITY RISKS & AVAILABLE COVERAGE

A. CURRENT STATE OF CYBERSECURITY RISKS

Companies have cybersecurity risks because of various vulnerabilities and the multitude of cyber threats.[21] Vulnerabilities act like "an unlocked door . . . but not a threat if no one wants to enter."[22] However, a single vulnerability may lead to multiple threats from outside actors who wish to harm companies by exploiting other vulnerabilities.[23]

Cyber risks are unique from other security risks due to "the speed with which the threats are evolving and proliferating,"[24] and from the ease at which an "adversary can

---

18. GILFORD, *supra* note 2, at § 16:1.

19. Palkon v. Holmes, No. 2:14–CV–01234 (SRC), 2014 WL 5341880, at *2–6 (D. N.J. Oct. 20, 2014); *In re* Sony Gaming Networks and Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014); Complaint, F.T.C. v. Wyndham Worldwide Co., No. 2:12-cv-01365-SPL, 2012 WL 12372027, at ¶43 (D. N.J. Aug. 12, 2012) [hereinafter *Wyndham Worldwide* Complaint].

20. *Palkon*, 2014 WL 5341880; *In re* Sony Gaming Networks., 996 F. Supp. 2d, at 966; *Wyndham Worldwide* Complaint, *supra* note 19, at ¶43.

21. P.W. SINGER & ALLAN FRIEDMAN, CYBER SECURITY AND CYBER WAR: WHAT EVERYONE NEEDS TO KNOW 37 (2014).

22. *Id*. at 37.

23. *Id.* at 38; *see also* 2016 DATA BREACH INVESTIGATIONS REPORT, VERIZON (Apr. 25, 2016), http://www.verizonenterprise.com/DBIR/2015/.

24. PWC, *supra* note 5, at 4.

pick and choose which vulnerability to exploit for any given goal."[25] In order to obtain sensitive, personal information, cybercriminals constantly probe vulnerabilities and adapt their tactics to new security measures.[26] An example of cybercriminals evolving their tactics is in the area of social engineering,[27] where hackers evolved "phishing" into "spear phishing."[28] A successful spear phishing attempt will give the hacker an employee's login information, which will grant the hacker "root access."[29]

Another evolving cyber threat that is difficult to defend against is automated malicious software called malware.[30] Some emails contain attachments that release malware once opened.[31] These malicious codes are programmed to autonomously search for stored credit card information to send back to their master.[32] Malware is one of the fastest evolving forms of cyber threats.[33] In 2010, McAfee[34] discovered "a new specimen of malware every fifteen minutes."[35] By 2013, that rate increased to a new specimen every second.[36] The banking and financial industries are most at risk from malware

---

25. SINGER & FRIEDMAN, *supra* note 21, at 38.

26. PWC, *supra* note 5, at 7.

27. Social engineering is defined as a "confidence trick." A hacker pretends to be technical support staff in order to trick employees into disclosing network access information. *See id.* at 40.

28. "Phishing" is a method where a seemingly legitimate email from the employee's company asks the target employee to login on a false but seemingly official company website. *See id.* at 41. "Spear phishing" personalizes the email message with information that specifically pertains to the target employee. *See id.*

29. Root access is defined as "the ability to execute any command" leaving the victim "completely vulnerable." *See id.* at 40.

30. *See id.* at 38.

31. *See Malicious Email Attachments*, MAKEITSECURE.ORG, http://www.makeitsecure.org/en/malicious-email-attachments.html (last visited Sept. 9, 2016) (explaining what malicious emails are, how to recognize them, and how to avoid them).

32. SINGER & FRIEDMAN, *supra* note 21, at 38.

33. *Id.* at 60.

34. McAfee is a cybersecurity firm and common anti-virus provider. *See About Intel Security*, MCAFEE, http://www.mcafee.com/us/index.html (last visited Sept. 21, 2016) (click through the tab at the bottom of the website's page to read explanations of what their security products provide and protect against).

35. SINGER & FRIEDMAN, *supra* note 21, at 60.

36. *Id.*

threats.[37] In the second quarter of 2015 alone, banking malware increased from 71% to 83% in a single quarter.[38]

An example of evolving malware is ransomware,[39] which evolved into crypto-ransomware.[40] Crypto-ransomware has been utilized against hospital systems because the inability to access patient information creates a sense of urgency to quickly pay the ransom.[41] However, even after a hospital pays the ransom to regain information access, the hackers may elect to maintain control or attack again.[42]

Another sophisticated method of cyber-attack is the "waterhole attack."[43] In 2015, hackers attacked United States defense contractors and financial institutions "by compromising the Forbes.com 'Thought of the Day (ToTD)' Adobe Flash widget . . . that appears initially whenever anyone visits any

---

37. *See* Emm et al., *supra* note 14, at 21.

38. *Id.*

39. Ransomware is malware that "prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' [access to] files." *Definition: Ransomware*, TRENDMICRO, http://www.trendmicro.com/vinfo/us/security/definition/ransomware (last visited Sept. 9, 2016).

40. Crypto-ransomware "encrypt[s] certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key." *Id.*

41. *See* Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ (quoting Stu Sjouwerman, CEO of the security firm KnowBe4, stating, "If you have patients, you are going to panic way quicker if you are selling sheet metal.").

42. In February 2016, Kansas Heart Hospital paid a $17,000 ransom to regain access to patient information after being attacked by crypto-ransomware. The hackers only released some of the locked information and demanded more money. *See* Bill Siwicki, *Ransomware Attackers Collect Ransom from Kansas Hospital, Don't Unlock All the Data, Then Demand More Money*, HEALTHCAREITNEWS (May 23, 2016, 2:58 PM), http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom.

43. A "waterhole attack" compromises a legitimate website to target a company that often visits that website. *See* Stephen Ward, *Cyber Espionage Campaign Compromises Web Properties to Target US Financial Services and Defense Companies, Chinese Dissidents – CVE-2015-0071 and CVE-2014-9163*, ISIGHTPARTNERS (Feb. 10, 2015), http://www.isightpartners.com/2015/02/codoso [https://web.archive.org/web/20160410055615/http://www.isightpartners.com/2015/02/codoso/]. The moment a target company's employee visits the compromised website, the hacker will have access through the vulnerabilities of that website. *Id.*

Forbes.com page or article."[44] Since Forbes.com is a highly trafficked website by many different users, it is difficult to determine how many companies were affected.[45]

Damages caused by a single breach are comparable to natural catastrophes.[46] The danger is further exacerbated by the fact that cyber breaches are becoming more frequent.[47] Since 2006, 500 to 800 publicly reported data breaches occur per year.[48] With the probability of catastrophic damage being high and increasing, it is prudent for at-risk companies to have insurance in order to ensure that the latest cybersecurity measures are implemented.[49]

B. COMPANIES AT RISK

Determining which types of information are highly sought after helps determine which industries and companies are at risk for cyber-attacks.[50] Personally identifiable information (PII) accounted for 45% of data breach claims, making it the most frequently exposed kind of data in 2015.[51] The next two most exposed information types were payment card industry information (PCI) and protected health information (PHI), which comprised 27% and 14% of data breach claims, respectively.[52]

---

44. *Id.*

45. *Id.*

46. PWC, THE PROMISES AND PITFALLS OF CYBER INSURANCE 3 (Jan. 2016), http://www.pwc.com/us/en/insurance/publications/assets/pwc-insurance-top-issues-cyber-insurance.pdf (explaining that the extent of damage that can be caused by a cyber-attack is similar in magnitude to a natural disaster, but the frequency at which cyber-attacks happen compared with natural disasters may put limits on what insurers could cover such crime and resulting damage).

47. *Id.*

48. WELLS ET AL., *supra* note 12.

49. *See* Amit Jain et al., *Using Insurance to Mitigate Cybercrime Risk*, CAPGEMINI 3 (2012), https://www.nl.capgemini.com/resource-file-access/resource/pdf/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf (arguing that cybersecurity measures alone are insufficient to mitigate all vulnerabilities, and that a cybersecurity/cyber-insurance regime is necessary to protect businesses and other institutions).

50. *Id*. at 4–6 (explaining the different forms of cyber-attacks and the losses suffered across different industries).

51. NETDILIGENCE, *supra* note 4, at 3.

52. *See id.*

These three kinds of sensitive, private information are stored by companies in different economic sectors, placing those companies at risk for cyber breaches.[53] According to NetDiligence, the most affected industries were the healthcare, retail, and financial services industries.[54]

The healthcare sector was the most frequently breached, and also had the second largest single breach behind the retail sector.[55] The financial industry was second to the healthcare industry in frequency.[56] In 2014, financial information was involved in 35.5% of breaches in the retail industry, almost doubling the previous year.[57] The retail industry has the distinction of exposing the largest number of identities, accounting for almost 60% of all identities reported exposed.[58] According to the Bureau of Economic Analysis, these three industries make up roughly a third of the United States economy.[59] Institutions such as stores, hospitals, and financial institutions are at a high risk for data breaches. The amount of consumers in each of the three industries makes a data breach publicly and economically catastrophic.[60]

Despite efforts by some firms in the financial sector to increase their own cybersecurity, "many of those same firms expose themselves to vulnerabilities by doing business with other companies that do not maintain effective cybersecurity

---

53. *See id.* at 18 (finding that fifteen business sectors comprise about 90% of all cyber breaches between 2012 and 2015).

54. *See id.* at 18.

55. *See id.* at 20 (noting that the largest breach in the retail sector was the loss of 110,000,000 records, and the largest breach in the health care sector was an 80,000,000 record loss).

56. *See id.* at 20.

57. *2015 Internet Security Threat Report,* SYMANTEC 83 (Apr. 2015), https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

58. This rate increased from 30% in 2013. *Id.*

59. The financial, health care, and retail industry composed of 32.9% of the national GDP in 2014. *See Value Added by Industry as a Percentage of Gross Domestic Product*, BUREAU OF ECON. ANALYSIS (Feb. 19, 2016), http://bea.gov/industry/gdpbyind_data.htm (then follow "XLSX" hyperlink under "Value Added").

60. Jonathan House, *Five Takeaways from New GDP-by-Industry Report*, WALL ST. J.: REAL TIME ECON. (Apr. 25, 2014, 2:30 PM), http://blogs.wsj.com/economics/2014/04/25/five-takeaways-from-new-gdp-by-industry-report/ (finding that finance "remains a cornerstone of economy").

procedures."[61] Breaching a large company collaterally is a trend that is making small and midsize businesses (SMBs) the "principal targets" of cybercriminals.[62] In 2014, 60% of all targeted attacks struck SMBs.[63] Furthermore, any industry that is involved with e-commerce is also at risk for cyber threats.[64]

C. LIABILITIES FOR COMPANIES

After a cyber breach, the breached company may suffer damage from the stolen information.[65] These companies may face consumer lawsuits, FTC and SEC enforcement actions, and shareholder derivative suits—all of which are likely to incur costly legal fees and high settlements.[66]

A large corporation storing PII and PCI is liable for protecting that private information.[67] Improper disclosure of such information exposes organizations to civil liability to the victim consumers.[68] Some jurisdictions are imposing a duty to

---

61. Dixie L. Johnson et al., *SEC Releases Results of Financial Industry Examination Sweep Regarding Cybersecurity*, KING & SPALDING: CLIENT ALERT 3 (Feb. 6, 2015), http://www.kslaw.com/imageserver/KSPublic/library/publication/ca020615.pdf.

62. *See* LUIS A. AGUILAR, COMM'R OF U.S. SEC. EXCH. COMM'N, THE NEED FOR GREATER FOCUS ON THE CYBERSECURITY CHALLENGES FACING SMALL AND MIDSIZE BUSINESSES (Oct. 19, 2015), https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.

63. SYMANTEC, *supra* note 57, at 6.

64. WELLS ET AL., *supra* note 12.

65. *See* GILFORD, *supra* note 2; *see also* NETDILIGENCE, *supra* note 4, at 3.

66. *See* Palkon v. Holmes, No. 2:14–CV–01234 (SRC), 2014 WL 5341880, at *2–6 (D. N.J. Oct. 20, 2014) (where the board of directors was subjected to a derivative suit filed by shareholders); Press Release, Jessica Rich, Dir. Fed. Trade Comm'n Bureau of Consumer Prot., Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment (settlement of FTC charges relating to "the company's security practices [which] unfairly exposed the payment card information of hundreds of thousands of consumers"); NETDILIGENCE, *supra* note 4, at 6–7 (showing distribution of the costs that affect companies subject to cyber breach).

67. *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 316 (2015).

68. Gordon, *supra* note 10, at 25.

employ reasonable data security measures under the fiduciary duty of care.[69]

1. Class Action: An Example

Consumers filed a class action lawsuit against Target Corporation in response to a 2013 data breach.[70] Hackers had obtained the financial information of more than forty million consumers[71] from Target's database. Target argued for dismissal of the ensuing consumer class action for want of standing because there was no injury in fact.[72] For the most part, the court agreed that most consumers either suffered no concrete injury or very small losses.[73] However, the court denied Target's motion to dismiss because "[s]ome consumers undoubtedly suffered some injuries."[74]

On September 17, 2015, Target settled the consumer class action lawsuit for $10 million.[75] Despite this large settlement, the company's consumer liability is still not completely resolved—at least four consumers are seeking to opt out of the class settlement to pursue their own claims.[76]

Affected consumers are just one of Target's concerns in relation to the 2013 data breach.[77] Financial institutions,

---

69. California and Massachusetts are the most recent states to impose a cybersecurity duty on corporate boards. *See* Shackelford et al., *supra* note 67, at 316 (citing *In re* Sony Gaming Networks and Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014)).

70. *See In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, 2015 WL 7253765, at *1 (D. Minn. Nov. 17, 2015) (memorandum & order).

71. *See* Kelly Clay, *Forty Million Target Customers Affected by Data Breach*, FORBES (Dec. 18, 2013, 5:57 PM), http://www.forbes.com/sites/kellyclay/2013/12/18/millions-of-target-customers-likely-affected-by-data-breach/#4ba97fa21481 (discussing how around Black Friday, hackers were able to obtain the data stored on the magnetic strip of credit cards, i.e.; debit/credit card numbers, card holder names, and the CVV number).

72. *In re Target Corp.*, 2015 WL 7253765, at *1.

73. *Id.*

74. *Id.*

75. The average payout per claim were estimated to range from $300 to $2200 per claimant. *Id.*

76. *See generally* Court Docket at 1, Gibson v. Target Corp., No. 15-3914 (8th Cir. Dec. 21, 2015); Court Docket at 1, Miorelli v. Target Corp., No. 15-3915 (8th Cir. Dec. 21, 2015); Court Docket at 1, 5–9, Olson v. Target Corp., No. 15-3912 (8th Cir. Dec. 21, 2015); Court Docket at 1, Sciaroni v. Target Corp., No. 15-3909 (8th Cir. Dec. 21, 2015).

77. *See* Jonathan Stempel & Anita Bose, *Target in $39.4 Million Settlement with Banks over Data Breach*, REUTERS (Dec. 2, 2015, 9:15 PM),

including MasterCard, filed a separate class action lawsuit claiming damages for the cost of fraudulent charges and the replacement of exposed payment cards.[78] Target settled with the financial institutions for $39 million[79] and individually with Visa for $67 million.[80] The breach may have cost Target over $290 million, though the company expects insurers to cover $90 million.[81]

Target is just one of many companies subjected to class action lawsuits over data breaches.[82] T-Mobile and Experian North America Inc. had class action lawsuits filed against them for allegedly having substandard security practices that improperly exposed over fifteen million customers' private information.[83] The plaintiffs in these suits charged that

> it was reasonably foreseeable to defendant that its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect plaintiffs' and class members' consumer credit information would result in a security lapse, whereby unauthorized third parties would gain access to, and disseminate, plaintiffs' and class members' consumer credit information into the public domain for no permissible purpose under FCRA.[84]

---

http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.

78. *See id.*

79. *See* Ahiza Garcia, *Target Settles for $39 Million Over Data Breach*, CNN MONEY (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

80. Ellen Rosen, *SEC Won't Recommend Enforcement Action Over Target's Data Breach*, BLOOMBERG BNA (Aug. 27, 2015), https://bol.bna.com/sec-wont-recommend-enforcement-action-over-targets-data-breach/ ("The retailer has reached a settlement with Visa Inc. over the attack and will pay as much as $67 million to banks that issue Visa cards, a person familiar with the matter said at the time.").

81. Stempel & Bose, *supra* note 77 (affirming that the data breach affected consumers, banks, lenders, and credit unions).

82. Melissa LaFreniere, *T-Mobile, Experian Hit with Data Breach Class Action Lawsuit*, TOP CLASS ACTIONS (Oct. 6, 2015), http://topclassactions.com/lawsuit-settlements/lawsuit-news/181853-t-mobile-experian-hit-with-data-breach-class-action-lawsuit/ (discussing how T-Mobile and Experian North America Inc. are being subject to litigation stemming from hacked T-Mobile data being stored Experian servers).

83. *Id.*

84. *Id.* (quoting the plaintiffs' accusations against Experian).

NetDiligence estimates that the average claim payout against a large corporation is $4.8 million dollars.[85]

2. FTC Enforcement Action

In addition to consumer and corporate class action lawsuits, companies may have to defend against FTC enforcement actions.[86] Any "unfair or deceptive acts or practices . . . affecting commerce" are unlawful and subject to FTC enforcement.[87] The FTC deemed the negligent protection of consumer data to be "unfair" if it is "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves," and it is "deceptive" if consumers believe their information is more protected than it actually is.[88] In such a circumstance, the FTC is authorized to obtain "[a]ll remedies available to the Commission . . . including restitution to domestic or foreign victims" under the FTC Act § 5.[89]

The FTC used this broad authority against ChoicePoint.[90] ChoicePoint is a consumer data broker that had more than 163,000 of its consumers' personal financial information compromised.[91] In 2006, the FTC brought a § 5 enforcement action in response to the data breach and ChoicePoint paid a $10 million civil penalty in addition to $5 million in consumer

---

85. *See* NETDILIGENCE, *supra* note 4, at 3.

86. *See* FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE 1 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf ("[T]he FTC uses a variety of tools to protect consumers' privacy and persona information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior."); *see also* Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, WESTIN RES. CTR. 8 (Sept. 19, 2014), https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf (arguing that companies should not be afforded "safe harbor from [FTC] enforcement nor immunity from a privacy or security breach, [given that] such a program will mitigate risk and strengthen a company's hand in dealing with any adversity").

87. 15 U.S.C. § 45(a)(1) (2012).

88. *Id.* § 45(n); *Wyndham Worldwide* Complaint, *supra* note 19, at ¶43.

89. 15 U.S.C. § 45(a)(4)(B).

90. Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

91. *Id.*

redress in its settlement with the FTC.[92] The ChoicePoint data breach improperly disclosed over eight hundred consumers' private information.[93]

A more recent FTC enforcement action was brought against Wyndham Worldwide in 2012.[94] Between 2008 and 2009, Wyndham's computer system was hacked on three separate occasions.[95] The FTC alleged that Wyndham deceived its consumers by representing that it implemented reasonable and appropriate security measures against unauthorized access.[96] The alleged deception occurred through the privacy policy Wyndham issued to consumers.[97] The FTC argued the misrepresentation was deceitful because it induced consumers to entrust their private information to Wyndham's purportedly updated security system.[98]

The Wyndham data breach led to more than "$10.6 million in fraud loss, and [the] export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia."[99] On December 9, 2015, Wyndham settled with the FTC.[100] Although the settlement did not require Wyndham to pay any penalties, the terms of the agreement were costly for the company.[101] The settlement agreement requires Wyndham's security system to conform to the Payment Card Industry Data Security Standard for certification and to obtain annual audits for certification compliance.[102] Additionally, Wyndham must provide the FTC with an assessment if another data breach that affects more than ten thousand payment card numbers occurs.[103] Wyndham is subject to these and other monitoring and reporting

---

92. *Id.*
93. *Id*.
94. *E.g.*, F.T.C. v. Wyndham Worldwide Co., 799 F.3d 236 (3d Cir. 2015).
95. *See id.* at 236.
96. *Wyndham Worldwide* Complaint, *supra* note 19, at ¶44.
97. *See id.* at ¶21.
98. *See id.* at ¶48.
99. *Id.* at ¶2.
100. *See, e.g.*, Stipulated Order for Injunction, F.T.C. v. Wyndham Worldwide Co., No. 2:13-CV-01887-ES-JAD (D. N.J. Dec. 11, 2015) [hereinafter *Wyndham Worldwide* Stipulated Order]; *see also* Rich, *supra* note 66.
101. Rich, *supra* note 66.
102. *Id*.
103. *Id.*

requirements for at least the next twenty years.[104] Abiding by the heightened security standards only prevents FTC enforcement action in the event of another breach.[105] Civil class actions from consumers and financial institutions may still be filed.[106]

3. SEC Enforcement Action

The FTC is not the only federal agency with the authority to bring government actions in the event of a data breach.[107] The SEC may also bring enforcement actions under the Securities Exchange Act of 1934.[108] The SEC issues penalties and orders when a breached company discloses inaccurate or misleading information to investors after a data breach,[109] or if the breach involves investment advisers.[110]

The Securities Exchange Act Section 10b and SEC Rule 10b-5 require companies to disclose any material fact about the company to investors.[111] A fact is material if its misrepresentation or its omission convinces the investor to trade shares of the company.[112] The fraud-on-the-market theory stipulates that the "market price of shares traded on well-developed markets reflects all publicly available

---

104. *Wyndham Worldwide* Stipulated Order, *supra* note 100, at 4, 13.

105. Rich, *supra* note 66 ("[I]f Wyndham successfully obtains the necessary compliance certifications, it will be deemed in compliance with the comprehensive information security program provision of the order."). Wyndham is just one of fifty-three corporations the FTC has settled with concerning data security. Rosen, *supra* note 80 ("According to the FTC, the agency has already settled 53 data-security cases against companies including SnapChat Inc., Reed Elsevier Inc. and Credit Karma Inc.").

106. Rich, *supra* note 66.

107. *See, e.g.*, Securities Exchange Act of 1934 § 21, 15 U.S.C. § 78u (2012).

108. *Id*.

109. 15 U.S.C. § 78m (2012); 17 C.F.R. § 240.10b-5 (2016); Rosen, *supra* note 80 ("The SEC has the authority to impose penalties on companies that don't disclose the magnitude of data breaches or fail to properly detail their policies and procedures in protecting consumer data.").

110. Investment Advisers Act of 1940 § 203, 15 U.S.C. § 80b-3 (2012); 17 C.F.R. § 248.30 (2016).

111. *See* Securities Exchange Act of 1934 § 12, 15 U.S.C. § 78l (2012) (requiring that a security be registered if it is to be traded on a national security exchange); 17 C.F.R. § 230.120 (2016) (requiring that registration statements be made public).

112. Basic, Inc., v. Levinson, 108 S. Ct. 978, 983 (1988).

information, and, hence, any material misrepresentations."[113] The SEC cautions that data breaches may require disclosure.[114]

The investment advisory firm R.T. Jones Capital Equities Inc. suffered a data breach in July 2013 which allowed an unauthorized, unknown intruder access to the PII of more than 100,000 individuals.[115] As a result, the SEC brought an action against R.T. Jones for violating the Safeguards Rule.[116] The SEC alleged that R.T. Jones failed to properly implement measures that reasonably protected the private information of its clients.[117] R.T. Jones and the SEC settled the matter.[118] R.T. Jones agreed to implement better safeguards of PII, preventing another incident in addition to paying a $75,000 penalty to the SEC.[119] Although the penalty was small in amount, the legal fees incurred may have been substantial.[120]

The R.T. Jones proceeding is just one instance of the SEC closely scrutinizing data breaches.[121] As cybersecurity risks threaten more and more corporations, the SEC is expanding its focus on data security.[122] SEC Commissioner Luis A. Aguilar placed a board of directors on notice for cybersecurity liability when he said "[b]oards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk — and there can be little doubt that cyber-risk also must be considered as part of a

---

113. Halliburton Co. v. Erica P. John Fund, Inc., 134 S. Ct. 2398, 2408 (2014) (quoting Basic, Inc. v. Levinson, 108 S. Ct. 978, 991 (1988)).

114. *See* SEC. EXCH. COMM'N., CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm ("Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents.").

115. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846, at *2 (Sept. 22, 2015).

116. *Id.*

117. *Id.*

118. *Id.* at *1.

119. *Id.* at *4.

120. *See* NETDILIGENCE, *supra* note 4, at 3 ("[T]he average cost for legal defense was $434,354.").

121. *See, e.g.*, Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016); Marc A. Ellis, Exchange Act Release No. 64220, 2011 WL 1325566 (Apr. 7, 2011); LPL Fin. Corp., Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775, 2008 WL 4179915 (Sept. 11, 2008).

122. *See* AGUILAR, *supra* note 62.

board's overall risk oversight."[123] The SEC even suggested that SMBs should have a greater focus on cybersecurity risks.[124]

4. Shareholder Derivative Lawsuits

In addition to class action lawsuits, FTC enforcement actions, and SEC enforcement actions, boards of directors may be subject to derivative lawsuits filed by the company's shareholders.[125] Derivative lawsuits over cybersecurity breaches usually allege that the board of directors breached its fiduciary duty of care.[126]

The Wyndham Worldwide data breach resulted in such a derivative suit.[127] In *Palkon v. Holmes*, shareholder Dennis Palkon sued Wyndham's board of directors for refusing his demand to bring a lawsuit against the board itself on the company's behalf.[128] The court ruled that the decision to bring a suit on behalf of the company is reviewed under the business judgment rule.[129] Under the business judgment rule, courts presume that boards of directors make their decision "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company."[130] The court dismissed the suit because the plaintiff could not rebut the strong presumption that the decision was made in good faith.[131]

The problems facing corporate boards of directors do not end after dismissal of a derivative suit.[132] A proxy firm addressing the Target data breach called for the ouster of most

---

123. Luis A. Aguilar, Comm'r of U.S. Sec. Exch. Comm'n, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Conference Speech at the New York Stock Exchange (June 10, 2014) (transcript available on the SEC website at https://www.sec.gov/News/Speech/Detail/Speech/1370542057946).

124. *See* AGUILAR, *supra* note 62.

125. *See, e.g.*, Palkon v. Holmes, No. 2:14–CV–01234 (SRC), 2014 WL 5341880 (D. N.J. Oct. 20, 2014).

126. *See, e.g.*, *id.* at *2 ("At the heart of Plaintiff's Complaint is an assertion that Defendants failed to implement adequate data-security mechanisms.").

127. *See id.* at *1–2.

128. *Id.* at *2.

129. *Id.* at *3.

130. *Id.* at *3 (quoting Spiegel v. Buntrock, 571 A.2d 767, 774 (Del. 1990)).

131. *Id.* at *6–7.

132. Aguilar, *supra* note 123.

of the Target directors for failure to appropriately manage the risks.[133] The SEC said that "Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks," which suggests the possibility that boards of directors will have the duty to manage cybersecurity risks incorporated into their fiduciary duty of care.[134] Although Target's board ultimately remained unchanged, Target's CEO was ousted as a result of the data breach.[135]

In analyzing cyber risks, corporations often overlook, or underestimate legal fees. The defense cost after a data breach was $434,354.[136] Even after paying damages, penalties, and legal fees, there is still the cost of required monitoring and reporting from FTC settlements—some of which last for twenty years.[137] Such damages and costs may put a company out of business.[138] Businesses may need an insurance policy to cover these expenses to remain solvent and to ensure best safeguarding practices.[139]

D. CURRENT AVAILABLE COVERAGE

Currently, the insurance market views cyber risk as "a risk like no other" because of limited publicly available data and the quick evolution and proliferation of threats.[140] Quick growth in threats is why annual gross written premiums are expected to increase from $2.5 billion to $7.5 billion by the end of the decade.[141]

---

133. *Id.*

134. *Id.*

135. Matt Townsend et al., *Target CEO Ouster Shows New Board Focus on Cyber Attacks*, BLOOMBERG (May 6, 2014), http://www.bloomberg.com/news/articles/2014-05-05/target-ceo-ouster-shows-new-board-focus-on-cyber-attacks.

136. NETDILIGENCE, *supra* note 4, at 3.

137. *Wyndham Worldwide* Stipulated Order, *supra* note 100, at 4, 13.

138. Gordon, *supra* note 10, at 25.

139. *See* Brian Krebs, *The Case for Cybersecurity Insurance, Part I*, KREBS ON SEC. (June 22, 2010), http://krebsonsecurity.com/2010/06/the-case-for-cybersecurity-insurance-part-i/ (discussing a company that had cybersecurity insurance and was the victim of cybercrime).

140. PWC, *supra* note 5, at 4, 7.

141. *See id.* at 4.

Even with the likely increase in premiums, the coverage available may not be adequate.[142] Insurance products and the applicable law have not been "keeping pace with the emergent ubiquity of information technology in commercial enterprises."[143] An example of how insurance policies and laws fail to keep up with cyber risks is the way courts are interpreting the scope of coverage in common commercial general liability policies (CGL).[144] Most companies depended on CGL policies to cover liabilities and losses involved in data breaches, but courts have found no coverage.[145] State courts are split on whether "Property Damage" coverage encompasses loss or corruption of electronic data because there is a dispute on the definition of "tangible property."[146]

One case that ruled on the "tangible property" issue is *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.*[147] In that case, Ward General's systems crashed and the company lost the electronically stored data it used to service its clients' insurance policies.[148] Ward General lost $53,586.83 in expenses to restore its database in addition to $209,442.80 in business income, losses of productivity, commissions, and profits.[149] The defendant insurance company refused to cover the damages due to the policy explicitly covering only a "'direct physical loss' to property covered."[150] The court ruled in favor of the insurance company because Ward General did not suffer a direct physical loss.[151] In data breaches, the property lost is the data; courts have defined data as "factual or numerical 'information.'"[152] Loss of a database is the loss of organized information, and courts reject the notion

142. WELLS ET AL., *supra* note 12.

143. *Id*.

144. *See* Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. COMPUTER & INFO. L. 379, 383–84 (2014) (describing a court's ruling that a commercial general liability policy did not cover cyber-attacks).

145. *Cf. id*. at 385 (stating that many businesses consider cybersecurity insurance to be too costly).

146. WELLS ET AL., *supra* note 12, § 29.02[1].

147. 7 Cal. Rptr. 3d 844 (Cal. App. 4th Dist. 2003).

148. *Id.* at 846.

149. *Id.* (alteration in original).

150. *Id.* at 848.

151. *Id.* at 849.

152. *Id.* at 850.

that information can have a material existence, be formed of tangible matter, or be perceptible to touch.[153] Loss of the physical data storage medium, such as paper or hard drive, may be covered as a "direct physical loss," but the value of the information stored is not deemed a loss because information is intangible.[154]

Courts have ruled similarly to *Ward General Insurance* in its view that data and information are not tangible and thus are not covered.[155] Courts have applied this ruling to third-party coverage insurance policies.[156] In *America Online, Inc. v. St. Paul Mercury Insurance Co.*, the Fourth Circuit ruled that the commercial general liability coverage does not cover information because data are "abstract ideas, logic, instructions, and information."[157]

Due to the high potential for damages arising out of a data breach and the courts' unwillingness to extend general liability coverage to electronic information, it is important for a company to purchase an insurance policy that specifically covers cyber-liability.[158] The current coverage available may not be ideal for companies since most policies are "Named-Peril" policies.[159] Currently, first-party coverages may include losses resulting from "responding to a data breach . . . [,] loss of electronic data, software, hardware, and costs of reconstructing data[,] loss of use and business interruption[,] data security and privacy injury[,] . . . business interruptions due to improper access to computer systems[, and] public relation for cyber

---

153. *Id.* at 851.

154. *Id.*

155. *See, e.g.*, State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1115–16 (W.D. Okla. 2001) ("[C]omputer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.").

156. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003).

157. *Id.* at 96.

158. *See* GILFORD, *supra* note 2, at 16-5 (noting that recent CGL and property insurance policies attempt to explicitly exclude coverage for cyber risks).

159. Named-Peril policies "cover only specified 'perils' or risks." *Id.* § 16:3.1 at 16-29 to 16-30. This format may result in "restrictive exclusions and conditions–such as state-of-the-art data encryption or 100% updated security patch clauses–which are difficult for any business to maintain." PWC, *supra* note 46, at 2.

risks."[160] Insurers are constantly changing and reevaluating their cyber-liability policies in response to evolving cyber risks.[161] Risk managers seeking cyber-liability coverage should evaluate their needs and risks relative to a detailed evaluation of the offered coverage.[162]

Frequent policy reformation negatively impacts those who seek to purchase policies.[163] An issue that arises is determining the overlap between cyber-liability policies and traditional policies.[164] The traditional policy provider may not be the same provider for the cyber-liability policy.[165] An overlap in coverage would mean that the policy holder would pay for the same coverage twice and it would prolong the claims process with "two carriers arguing with each other as to which is responsible, or about how to allocate responsibility between them for a particular loss."[166]

The changing definition of what a "claim" is can be important to the policy holder as well.[167] The definition establishes the formalities required for coverage availability for a particular regulatory initiative.[168] How a "claim" is defined determines whether the holder is covered during government enforcement actions, either by the FTC or SEC.[169] For example, certain policies may require "the filing of a notice of charges, an investigative order, or similar document," which means that formal administrative actions may be a precondition to coverage.[170] However, policy holders often prefer that administrative proceedings remain informal, and often times they are.[171] Furthermore, most policies exclude coverage for

---

160. GILFORD, *supra* note 2, at § 16:3.1.

161. *Id.* § 16:3, at 16-28.

162. *Id.*

163. *Cf. id.* ("[I]t is likely that gaps in coverage for cyber and privacy risks will continue to widen as insurers increase the number of exclusions.").

164. *Id.* § 16:3.2.C, at 16-34.

165. *Cf. id.* (referring to two carriers in the context of overlapping insurance policies).

166. *Id.*

167. *See id.* § 16:3.2, at 16-37 to 16-38.

168. *Id.* at 16-36 to 16-37.

169. Office Depot, Inc. v. Nat'l Union Fire Ins. Co., 453 F. App'x 871, 875 (11th Cir. 2011).

170. GILFORD, *supra* note 2, § 16:3.2.F, at 16-38 to 16-39.

171. *Id.*

fines, penalties, and violations of law as a matter of public policy.[172]

These non-explicit exclusions cause problems when policy holders try to claim coverage from their insurers.[173] Companies may pay a high premium for little or no benefit. The current gross written premium for cyber risk is around $2.5 billion.[174] Companies using outdated security protocols risk damages caused by data breaches, including not receiving coverage after paying high premiums, negative impact of financial stability, and harm to consumers.[175]

II. POLICIES FOR COMPULSORY INSURANCE

A. OUTSOURCING REGULATORY DUTIES

Compulsory insurance benefits the public by outsourcing the role of regulator to insurance companies.[176] Outsourcing the regulatory role is best done in areas that are difficult for the government to regulate either due to logistical difficulties or political climate.[177] For example, a recent push to outsource the government's role as regulator is in gun control.[178] The push behind mandatory firearm liability insurance arose from the fact that "stringent gun control while the norm elsewhere seems politically impossible here."[179]

Some state legislators proposed mandatory firearm liability insurance "to manage gun violence and to cause gun owners, rather than taxpayers, to bear the costs of firearm

---

172. *Id.* § 16:3.2.G, at 16-41 to 16-44.

173. *E.g.*, Office Depot, Inc., 453 F. App'x at 871; MBIA, Inc. v. Fed. Ins. Co., 652 F.3d 152 (2d Cir. 2011).

174. PWC, *supra* note 5, at 4, 7.

175. *See* PWC, *supra* note 46, at 2 (mentioning insurers' high prices and strict limits on coverage).

176. *See* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 200–03 (2012) (describing how private insurers reduce risk by modifying insured's behavior).

177. *See* Tom Harvey, *The Case for Compulsory Gun Insurance*, HUFFINGTON POST (Oct. 2, 2013, 6:18 PM), http://www.huffingtonpost.com/tom-harvey/the-case-for-compulsory-g_b_4029894.html (describing how compulsory gun insurance could avoid the political difficulty of other methods of gun regulation).

178. *See, e.g.*, *id.*

179. *Id.*

accidents."[180] Compulsory insurance is a private means to regulate a problem without focusing on the cause.[181] Mandatory insurance would be a method to impose firearm regulations and controls without the government's involvement.[182]

Insurance companies set compliance requirements as part of their insurance policies.[183] These requirements sometimes are more stringent than government regulations[184] and help decrease risk by increasing levels of care.[185] Insurance companies adjust premiums based on whether the policy holder implements safety conditions to create a monetary incentive to comply with the stricter standards.[186] Insurance companies regulate an industry by using the "private marketplace to reduce the negative—and if possible, increase the positive—externalities associated with that activity."[187] Essentially, insurers directly influence the behavior of those they insure.[188]

Insurers have a monetary incentive to ensure compliance with the requirements of the policy.[189] This monetary incentive makes insurers adept at collecting data on the insured activity and the risks associated with the activity.[190] Legislators hope that subjecting insurers to claims will incentivize them to study gun violence to develop methods to reduce its frequency and severity for the policy holders to follow.[191] Teaching the insured best prevention methods is something that public regulators rarely do.[192] Unlike government regulators, insurance companies often offer their policyholders training to identify

---

180. George A. Mocsary, *Insuring Against Guns?*, 46 CONN. L. REV. 1209, 1217 (2014).

181. Harvey, *supra* note 177.

182. *Id.*

183. Ben-Shahar & Logue, *supra* note 176, at 211.

184. *Id.*

185. Steven Shavell, *Minimum Asset Requirements and Compulsory Liability Insurance as Solutions to the Judgment-Proof Problem*, 36 RAND J. ECON. 63, 65 (2005).

186. Rob Hillenbrand, *Heller on the Threshold: Crafting a Gun Insurance Mandate*, 95 B.U. L .REV. 1451, 1459 (2015).

187. Mocsary, *supra* note 180, at 1230.

188. *See id.*

189. *Id.* at 1234–35.

190. *Id.* at 1231.

191. *Id.* at 1234.

192. Ben-Shahar & Logue, *supra* note 176, at 210.

and control risks.[193] Insurers' involvement in their carrier's loss prevention program goes even further than just education.[194] It is not uncommon for insurers to "audit and inspect their clients, manage their prevention efforts, analyze their loss history, identify causes of accidents and how losses occur, and teach them how to avoid premium increases (or how to secure premium reductions)."[195]

Another instance of insurers acting as regulators is in the workplace.[196] Most employers are required to purchase workers' compensation insurance for work-related harms to their employees.[197] Insurers significantly engage in either ex ante underwriting or ex post experience rating, or both to accurately price their policies.[198] This results in regular visits from insurance representatives seeking to monitor employer compliance with both government and insurer codes and recommendations.[199]

B. ENSURING VICTIMS ARE MADE WHOLE

Compulsory insurance and optional insurance serve different purposes in terms of protection.[200] Where optional insurance protects the policy holder, compulsory insurance seeks to protect potential victims of the policy holder.[201] An example is automobile insurance, which is compulsory in nearly all states.[202] The justifications for having compulsory automobile insurance shed light on why cyber-liability insurance should follow that same route.

The New York state legislature implemented a compulsory regime for automobile insurance in response to its concern "over the rising toll of motor vehicle accidents and the suffering

193. *Id.*
194. *See id.*
195. *Id.*
196. *See id.* at 236–37.
197. *Id.* at 237.
198. *Id.*
199. *Id.*
200. 6 CHRISTOPHER J. ROBINETTE, NEW APPLEMAN ON INSURANCE LAW & PRACTICE § 61.02, at 61-17 (2015).
201. *Id.*
202. *Id.* at 61-16.

and loss thereby inflicted."[203] It became a "matter of grave concern that motorists shall be financially able to respond in damages for their negligent acts, so that innocent victims of motor vehicle accidents may be recompensed for the injury and financial loss inflicted upon them."[204]

A potential benefit of having a compulsory regime concerns the issue of whether certain exclusions or limitations apply.[205] When a dispute arises about whether an exclusion or limitation is valid, courts typically examine the public policy and purpose of the statute to determine the validity of an exclusion.[206] Courts will uphold an exclusion or limitation unless those terms are against public policy.[207] Courts have ruled that statutes express public policy and insurers may not circumvent a statute with a written restriction or exclusion.[208]

Because the public policy underlying compulsory insurance is victim protection, courts may rule more favorably towards providing coverage in an incident despite what is written in the insurance policy.[209] This will give consumer victims more security in being made whole. [210]

C. THE NEED FOR COMPULSORY CYBER-LIABILITY COVERAGE

1. Insurers Would Be Better Regulators

Compulsory cyber-liability insurance is needed for at-risk companies because government regulators are not properly staffed to oversee the affected industries.[211] Due to "the speed

---

203. Motor Vehicle Financial Security Act, N.Y. Veh. & Traf. Law § 310 (McKinney 2015).

204. *Id.*

205. *See* Mocsary, *supra* note 180, at 1218 (mentioning a Connecticut law which would have forbidden certain exclusions from compulsory insurance policies).

206. *See* State Farm Mut. Auto. Ins. Co. v. Smith, 757 N.E.2d 881, 883 (Ill. 2001).

207. *Id.*

208. *Id.*

209. *See, e.g.*, *id*. (holding void an exclusion in a compulsory auto insurance policy which violated the public policy embodied in a statute).

210. Harvey, *supra* note 177 ("[R]equired . . . insurance must be implemented in a way . . . that encourages safe practices [and] compensates victims.").

211. *See* Ben-Shahar & Logue, *supra* note 176, at 201 (illustrating the superior abilities of insurance companies at regulating risks related to data protection).

with which the threats are evolving and proliferating,"[212] the frequency and impact of data breaches will only increase.[213] The FTC only has forty-five members in its Division of Privacy and Data Protection to regulate the consumer retail industry.[214] The FTC's forty-five member division is responsible for keeping up with the latest threats and ensuring that companies are properly secured against those emerging threats.[215] Either the FTC would have to remain within its limited operative scope, or the taxpayers would have to fund expansion of the manpower in the Division of Privacy and Data Protection to adequately address the frequency of data breaches.[216] Insurance companies are better equipped with more resources to regulate risks that span across multiple industries, which ultimately eases the burden on taxpayers.[217] A comprehensive compulsory regime ultimately seeks to "remove pressure on governments to provide . . . relief."[218]

Manpower and resources are essential in regulating corporate cybersecurity because information governance systems require monitoring.[219] Monitoring compliance can be done ex ante (before harm has occurred) or ex post (after the harm has occurred).[220] Ex ante inspections would be "to confirm the installation of safety devices and inspect the conduct of

---

212. PWC, *supra* note 5, at 4.

213. Amy Lee, *Citigroup: $2.7 Million Stolen from Customers as Result of Hacking*, HUFFINGTON POST (Aug. 27, 2011, 10:12 AM), http://www.huffingtonpost.com/2011/06/27/citigroup-hack_n_885045.html ("Experts have suggested that hackers used spyware to capture data from customers as they logged in, though they were not able to get the CVV codes that accompany the physical card. With 154 million Americans owning credit cards, the incidence of such hacks is only expected to rise.").

214. *FTC Staff Directory*, FED. TRADE COMM'N (Sept. 18, 2013), https://www.ftc.gov/sites/default/files/attachments/contact-federal-trade-commission/whitepages.pdf.

215. *See id.* (listing the forty-five members of the FTC Division of Privacy and Data Protection); *see also* FED. TRADE COMM'N, *supra* note 86, at 1 (showing the tools available to the FTC to ensure data privacy).

216. *See generally* Bailin, *supra* note 86, at 2 (showing that the current scope of FTC involvement in data privacy cases has been limited to only forty-seven citations since 2002).

217. Mocsary, *supra* note 180, at 1231.

218. Michael Faure & Veronique Bruggeman, *Catastrophic Risks and First-Party Insurance*, 15 CONN. INS. L.J. 1, 41 (2008).

219. Ben-Shahar & Logue, *supra* note 176, at 236.

220. *Id.*

regulated parties."[221] Ex post monitoring would be done to determine liability or coverage after an occurrence.[222] Insurers will likely inspect risk-management techniques along with the disaster response plan.[223] Most importantly, insurers will be inspecting how employees and third-parties access the data systems.[224] Companies will have their areas of risks scrutinized and their vulnerabilities addressed.[225] These types of monitoring and regulatory inspections are "often done more effectively by insurers that develop regulatory practices and technologies that the government lacks."[226]

Compulsory insurance is needed for cyber-liability because of the lack of information available to companies.[227] Some companies are unaware of their own vulnerabilities and the threats to their data security.[228] In such a climate, compulsory insurance may mitigate the problems of asymmetric information and adverse selection.[229] When there is an imminent threat on which few companies have adequate information, a regulation would be an efficient method to cure the information deficiency[230] by introducing a general duty to insure.[231]

Similar to firearm liability insurance, compulsory cyber-liability insurance aims to have insurance companies provide and enforce best practices.[232] Insurers will directly influence corporate behavior once they "reduce the negative—and if

---

221. *Id.*

222. *Id.* at 236–37.

223. *Cyber Liabilities Policy*, NAIC (last updated Jan. 04, 2016), http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

224. *Id.*

225. *See* Ben-Shahar & Logue, *supra* note 176, at 203 (illustrating how risk assessment of companies allows insurance companies to spread their own risk out to minimize losses).

226. *Id.* at 236.

227. *See* Faure & Bruggeman, *supra* note 218, at 34–35 (explaining that companies may be a high risk for liability for a cyber-attack without knowing it).

228. *Id.* at 34.

229. *Id.* at 34–35.

230. *See id.* (showing that information problems occur when the potential victim cannot accurately assess the catastrophic risk he is exposed to or the benefits of the purchase of first-party insurance).

231. *Id.* at 35.

232. *See* Mocsary, *supra* note 180, at 1212 (proposing that mandatory insurance on firearm owners may be used as a form of private regulation).

possible, increase the positive—externalities" in managing cyber risks.[233] Giving insurance companies a monetary incentive in corporate cybersecurity ensures that insurers research risk minimizing practices and educate their insured.[234] The narrow policy terms and conditions[235] in cyber-insurance policies could incentivize organizations to focus more on their actual security rather than simply checking compliance checkboxes.[236] These practices would likely be required as part of their policy and compliance would be ensured through monitoring.[237] These measures will help increase levels of care in at-risk corporations more than what government regulators would provide.[238] The Deputy Treasury Secretary stated that "[q]ualifying for cyber-risk insurance can provide useful information for assessing [a] bank's risk level and identifying cybersecurity tools and best practices that [it] may be lacking."[239] Increasing compliance to higher standards may be a reason why some experts believe that "there's little doubt that cyber-insurance will be a requirement that the FFIEC[240] includes in its forthcoming cyber guidance" for banks.[241]

2. Insurance Ensures Victim Compensation

Similar to automobile risks, cyber-insurance has the potential to protect not just the breached company, but also millions of consumers.[242] Cyber risks have high potential

---

233. *Id.* at 1230.

234. *See* Ben-Shahar & Logue, *supra* note 176, at 210.

235. PWC, *supra* note 5, at 10.

236. Both Target and Neiman Marcus claim to have met PCI DSS requirements. Mark Campbell, *Mandatory Cyber Insurance – Driving Improved Security or Just Passing the Buck?*, CIPHERCLOUD (Mar. 17, 2014), http://www.ciphercloud.com/blog/mandatory-cyber-insurance-driving-improved-security-just-passing-buck/.

237. Ben-Shahar & Logue, *supra* note 176, at 236.

238. Shavell, *supra* note 185, at 65.

239. Tracy Kitten, *Will Banks Be Required to Have Cyber-Insurance*, BANKINFO SEC. (Dec. 12, 2014), http://www.bankinfosecurity.com/cyber-insurance-expectations-for-banks-a-7673/op-1.

240. *About the FFIEC*, FED. FIN. INSTITS. EXAMINATION COUNCIL, https://www.ffiec.gov/about.htm (last visited Sept. 16, 2016).

241. Kitten, *supra* note 239.

242. Gordon, *supra* note 10, at 26 (explaining that financial institutions are required to have a security plan in place to protect consumer's information).

damages that may put a company out of business.[243] Cyber risk insurance helps companies remain solvent when making victims whole.[244] Companies with cybersecurity insurance were likely to recover their direct financial losses despite suffering substantial thefts.[245] In the case of Brookeland Fresh Water Supply District, cybersecurity insurance protected 1300 homes and businesses from not receiving water.[246]

Although large corporations are able to compensate consumers, SMBs[247] do not have the resources to do so.[248] The compulsory insurance regime would cover both large corporations and the smaller contractors they share data with.[249] This incentivizes large corporations to ensure that their contractors are properly equipped with the best practices at minimizing cyber risk as well.[250] If an SMB is breached for the data it receives from large corporations, the victims would be compensated.[251]

III. COUNTER-ARGUMENTS

A. THE ARBITRARY LINE

One problem with implementing a compulsory cyber-liability regime is that costly premiums will create an arbitrary line between affected large corporations and the exempted SMBs.[252] Although SMBs are more at risk than large

---

243. *Id*. at 25.

244. *See* Krebs, *supra* note 139, at 1 (showing how one company managed to remain solvent and recoup their losses through their cybersecurity insurance policy).

245. *Id.*

246. Brian Krebs, *The Case for Cybersecurity Insurance, Part II*, KREBS ON SEC. (July 14, 2010), http://krebsonsecurity.com/2010/07/the-case-for-cybersecurity-insurance-part-ii/.

247. Small and Medium Businesses.

248. AGUILAR, *supra* note 62.

249. *See id*. (explaining how cyber-attacks against SMBs may be used to gain access to larger corporations they do business with).

250. *Id.*

251. *E.g.,* Krebs, *supra* note 139 (showing how a medium sized business recovered all of their losses from a cyber-attack through their cybersecurity insurance policy by paying only their ten-thousand dollar deductible).

252. *See id.* (explaining how a medium sized business owner feared that after being targeted by a cyber-attack her insurance policy premiums would rise beyond her ability to pay them).

corporations due to their inadequate resources against cyber threats, the premiums for coverage are unaffordable.[253]

At first, the compulsory regime would require that large corporations not only cover their own liabilities, but also the liabilities of the companies they contract with. As will be further discussed in Part IV, hackers breached Target through a medium-sized company it contracted with, showing how working with insecure companies affects large corporations.[254] Hopefully, this will give large corporations the incentive to help medium-sized contractors improve their cybersecurity by providing training and the necessary resources to implement the adequate security measures.[255]

One of the main concerns in closely scrutinizing the security measures of smaller companies is that compliance costs might run them out of business.[256] This scenario can be avoided by giving SMBs a temporary tax incentive for focusing on data security.[257] This tax incentive will be available to SMBs while large corporations are compelled to purchase policies, which will, in time, drastically reduce the premiums to a level where the medium- and small-sized businesses can afford to participate.[258]

An aspect of cyber-insurance that would benefit from a compulsory regime is that the policies would become more sustainable for the underwriters and the companies being insured.[259] Requiring cyber risk insurance may reduce the premiums.[260] A reason for high premiums may be the limited number of participating insurers.[261] Mandating cyber-

253. AGUILAR, *supra* note 62 (stating that the majority of all cyber-attacks target small and medium sized businesses that do not have the resources available to prevent them).

254. *Id*. (describing how the costly cyber-attack against Target resulted from the breach of a much smaller company that Target conducted business with).

255. *See id*. (suggesting that government entities may also be able take part in educating SMBs on how to improve their cybersecurity).

256. *See id*. (confirming that generally SMBs lack the resources to fund a legitimate cyber defense).

257. *See id.* (suggesting that tax credits may be a viable option to encourage the development of viable cybersecurity solutions for SMBs).

258. *See id.*

259. PWC, *supra* note 5, at 10.

260. *Id.* (noting that the general cost of cyber-insurance policies are three times higher than other more common forms of insurance for the same limit).

261. *See id.*

insurance would push for research to make the necessary data more available for the underwriters to use as they develop their policies.[262] Once the premiums are more affordable, the SMBs will also be compelled to purchase these policies.[263]

B. SHIFTING COSTS TO CONSUMERS

Another concern of a compulsory cyber-liability regime is that large corporations will shift the cost to consumers by increasing their prices. Although this concern is likely to occur for most companies, some companies may choose to not shift the cost.[264] A company may avoid cost shifting if the company was a recent victim of a data breach.[265] When a company inadvertently exposes its customers' private information, it is unlikely that it will shift the cost to consumers to protect that information.[266]

For companies that do shift costs, having the consumers assume the cost is better than the alternative of having every taxpayer fund the expansion of government regulations.[267] Much like firearm liability insurance, those who would bear the costs are those who participate in the activity.[268] Therefore, price shifting is only a concern for those who shop at large retailers or enlist the services of large banks.[269] This may incentivize shoppers to shop locally at smaller businesses since those smaller businesses would be exempt from the cyber-liability insurance requirement. Furthermore, the cost shifting should be temporary, as premiums can be expected to decrease

---

262. *Id.* ("Part of the reason for the high prices is . . . the uncertainty around how much to put aside for potential losses[.]").

263. *Cf. id.* (requiring policy holders to have "state-of-the-art data encryption or 100% updated security patch clauses" has proved to be a heavy burden on businesses, regardless of size, in obtaining these policies).

264. *See* Debra L. Shinder, *Cyber-Insurance: Is it Necessary? Should it Be Mandatory?*, GFI BLOG (Dec. 4, 2014), http://www.gfi.com/blog/cyber-insurance-is-it-necessary-should-it-be-mandatory/ (stating that loss of customer trust may effect companies profitability in the event of a data breach and thus prevent the shifting of costs to customers so as to not further deepen this loss of trust).

265. *See id.*

266. *See id.*

267. *See* Ben-Shahar & Logue, *supra* note 176, at 210 (noting that private insurers often have an advantage over government regulations in this area).

268. *See id.*

269. *But see* AGUILAR, *supra* note 62 (stating that SMBs face the greatest threat from cyber-attacks).

after a compulsory regime is implemented.[270] Once premiums are lowered, the remaining increase in price should be minimal.[271]

C. MORAL HAZARD

There is an argument that a compulsory insurance regime would be a detriment to corporate diligence in managing cyber risk.[272] Some fear that "insurance might take away some of the financial incentive to avoid" data breaches since the losses and damages would be covered.[273]

There are many reasons why such a negative effect is not likely. The first is that insurance cannot recover consumer trust.[274] Without consumer trust, profitability becomes difficult.[275]

Another reason why cyber-liability insurance does not present a moral hazard is because it actually gives companies a monetary incentive to be diligent through premium increases or potential policy cancellation.[276] Compulsory liability coverage may force the policy holders to "make superior decisions about whether to engage in an activity and . . . have stronger incentives to reduce risk when they have at stake at least the required level of assets and/or liability insurance coverage if they are sued for causing harm."[277] Experience rating (basing an insured's premiums on prior claim experience) may incentivize a carrier to reduce the moral hazard by in turn incentivizing the policy holder to reduce risk of loss.[278] Another method of reducing the moral hazard of being insured is for the insurer to require strict compliance with security requirements as a condition for coverage.[279]

---

270. PWC, *supra* note 5, at 10.
271. *Id.*
272. Shinder, *supra* note 264.
273. *Id.*
274. *Id.*
275. *Id.*
276. *Id.*
277. Shavell, *supra* note 185, at 63.
278. Mocsary, *supra* note 180, at 1231.
279. *Id.* at 1235. One area that is commonly uninsured are losses from intentional harmful activities. *Id.*

There is still a concern that a moral hazard may appear once the monetary incentive from premiums diminishes.[280] A compulsory cyber-liability regime would decrease the premiums for those policies over time. Low premiums may be "ineffective in influencing insureds' behavior if actuarially-fair premiums would be low even for high risks because an increased-but-still-low cost may not alter one's behavior."[281] However, consumer trust is still an asset that cannot be replaced by insurance.[282]

IV. COMPREHENSIVE COMPULSORY COVERAGE

A. STANDARDS FOR COMPREHENSIVE COMPULSORY COVERAGE

Making cyber-liability insurance mandatory would mean that certain risks and liabilities must be covered to make the compliance costs and premium payments beneficial to the corporation.[283] A mandatory policy would need to cover loss arising from third-party claims, the direct first-party costs of responding to a breach, loss of income and operating expenses, and cyber extortion threats against a company.[284] Specifically, the policy should cover damages arising from lawsuits, government enforcement actions, legal fees, business interruption, system repair costs, data recovery costs, response costs, hardware damage, and third-party liability.[285]

The insurance policies should address the legal obligations that may arise from a data security breach.[286] Legal obligations may be payments of damages and settlement, civil penalties, and legal fees.[287] Other industry-specific obligations may also arise, depending on the industry. Generally, breached companies may be required to retain third-party investigators to identify the cause of the breach, the perpetrator, and the

---

280. *Id.* at 1232.

281. *Id.*

282. Shinder, *supra* note 264.

283. Kevin M. LaCroix, *Cyber Security, Cyber Governance, and Cyber Insurance: What Every Public Company Director Needs to Know*, D&O DIARY (June 4, 2014), http://www.dandodiary.com/2014/06/articles/cyber-liability/guest-post-cyber-security-cyber-governance-and-cyber-insurance-what-every-public-company-director-needs-to-know/.

284. *Id.*

285. *Id.*

286. *Id.*

287. *Id.*

victims to be notified, and further to remedy flaws in the security system.[288] If the company is in the financial or retail industry and carries financial information such as payment card information, the breached company may be required to provide credit monitoring services, copies of credit reports to account holders, and compensation to banks for fraudulent charges.[289] Monitoring and reporting requirements arising out of government enforcement actions may last as long as twenty years.[290]

Another area of coverage that needs to become mandatory for large corporations is the coverage of damages arising from SMBs.[291] SMBs are the biggest vulnerabilities large companies have.[292] Part of the reason is that they "face precisely the same threat landscape that confronts larger organizations, but must do so with far fewer resources."[293] The fact that SMBs face threats that can endanger large corporations with limited resources is made worse by the fact that SMBs tend to lack sufficient in-house expertise.[294]

Insurance companies that insure large corporations should be concerned with SMBs because "[m]any SMBs have direct and indirect business relationships with larger organizations, a fact well known to cybercriminals."[295] SMBs become a cybercriminal's gateway to access larger organizations.[296] However, large corporations often overlook the vulnerabilities opened up by SMBs.[297] For example, cybercriminals accessed Target's system after penetrating the network of the small heating and air conditioning business that services Target.[298] For an SMB, a data breach can be more impactful to the

---

288. *See* WELLS ET AL., *supra* note 12, at § 29.01[2][a][iii].

289. *Id.*

290. *See id.* at § 29.01[2][b][ii] (showing that these requirements may incentivize companies to settle for large sums of money in the event of a data breach, such as when TJ Maxx was the victim of cyber-attacks).

291. *See* AGUILAR, *supra* note 62.

292. *See id.* (stating that SMBs are often victims of cyber-attacks in an attempt to gain access to larger companies that they conduct business with).

293. *Id.*

294. *See id.*

295. *Id.*

296. *Id.*

297. *Id.*

298. *Id.*

business than it would be for a larger corporation.[299] It is estimated that 72% of SMBs that suffer major data loss shut down within twenty-four months.[300] Mandatory coverage would be essential for SMBs that deal with large corporations that maintain personally identifiable information, payment card information, or protected health information.[301]

The coverage would either be a flat overall limit, as in automobile insurance,[302] or a limit placed on each record exposed. The unique characteristic of data breaches is that a massive amount of data is usually exposed—not any particular piece. Recent studies have shown that the cost of a lost or stolen sensitive or confidential record averages around $154 per record.[303] For large corporations, a data breach may affect seventy million households and millions of small businesses.[304] The Target breach was estimated to be as high as 110 million affected customers.[305] Since one purpose of mandatory cyber-insurance is to protect the victimized consumers, the policy coverage should be based on the price per record.[306] Although other factors such as legal fees and other damages should be factored in, the price per record evaluation would assure that each victim is considered for redress.[307]

B. OBSTACLES

One obstacle to instituting a mandatory cyber-liability insurance regime is the level of concern companies attribute to cyber risks.[308] It is not uncommon for "those who professionally

---

299. *Id.* (stating that "it is becoming increasingly difficult for SMBs to recover from an attack").

300. *See* Carrie E. Scope & Ian Reynolds, *"Breaking Bad" in Cyber Space: A Challenge for the Insurance Industry*, 2015 EMERGING ISSUES 7296 (2015).

301. *See id.* (showing that in 2013, 61% of cyber-attacks targeted businesses with fewer than 2500 employees).

302. WELLS ET AL., *supra* note 12, at § 29.01.

303. PONEMON INST., 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2 (May 2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF.

304. *Id.* ("The JP Morgan Chase & Co. data breach affected 76 million households and seven million small businesses.").

305. Shinder, *supra* note 264.

306. *See id.* (stating that the average cost per record in 2014 was $201).

307. *Id.* (showing that this analysis of cost factored in both the direct and indirect costs of data breaches such as the value of customer loss).

308. SINGER & FRIEDMAN, *supra* note 21, at 37.

think and talk about cybersecurity [to] worry that their discussions of threats are ignored or downplayed."[309] Those who downplay the seriousness of cyber risks will deem a mandatory policy unnecessary.[310] Such an argument may have been true five years ago, but it no longer is today. The demand for cyber-liability coverage currently outstrips supply.[311] It is reported that Target couldn't find adequate coverage for cyber losses.[312] Although Target did eventually find coverage, the policy "will barely take care of an anticipated $1 billion in losses."[313] The Target breach demonstrates that demand is no longer the problem in insuring companies against cyber risk—it is now an issue of quality of supply.[314]

Another objection to making cyber-insurance mandatory is that the development of sufficient coverage is still too premature. Currently, insurers have "little historical information to draw on with respect to the frequency, severity and scope of data breaches, or other cyber-related losses, sustained by various industries for underwriting purposes."[315] Although more studies and data are being collected about cyber risk, the information is broad and not industry-specific.[316] Industry-specific information is important because of the industry-specific risks, which are dependent on the type of information being stored and protected.[317] For example, ransomware is unique to PHI, which places hospitals at risk of becoming victims of ransomware.[318]

---

309. *Id*.

310. *Id.*

311. *See* Aliya Sternstein, *WH Official: Cyber Coverage Will Be a Basic Insurance Policy by 2020*, NEXTGOV (Sept. 8, 2014), http://www.nextgov.com/cybersecurity/2014/09/wh-official-cyber-coverage-will-be-basic-insurance-policy-2020/93503/.

312. *Id.*

313. *Id.* (stating that "at least one carrier rejected the retailer" in its pursuit of finding cyber risk coverage).

314. *Id.* (explaining that before the Target breach, insurance companies didn't have enough data on breaches to determine what the costs of a policy should be, but that data is now forthcoming).

315. Scope & Reynolds, *supra* note 300, at 7.

316. *See id.*

317. *Id.* (stating that this information is becoming more readily available as state laws on these matters change).

318. *See id.* at 5 (adding that small businesses are also especially susceptible to ransomware).

A likely and difficult obstacle may come from the insurance companies themselves.[319] Historically, the insurance industry has been "adamantly opposed to any kind of compulsory insurance because it fears there would be associated regulation of the insurance itself."[320] The insurance industry heavily opposed compulsory automobile insurance since the law's inception in the 1920s.[321] Insurance companies like to have freedom in determining the terms of their policies without government oversight, which is lost in a compulsory regime.[322] Legislatures usually demand minimal coverage requirements in mandatory coverage.[323]

C. OVERCOMING OBSTACLES

In recognizing the complex issues involved in cybersecurity, the National Association of Insurance Commissioners (NAIC) created a special taskforce to coordinate insurance issues in cybersecurity.[324] This taskforce will help cyber risk insurers create coverage by providing the much needed data.[325] The NAIC taskforce seeks to "(a) monitor developments in the area of cybersecurity; (b) advise, report and make recommendations to the Executive Committee on cybersecurity issues; [and] (c) coordinate activities with the NAIC standing committees and their tasks forces and working groups regarding cybersecurity issues."[326]

The taskforce released twelve guiding principles that it believes will improve cybersecurity in the insurance industry, and may help in overcoming obstacles to an effective mandatory regime.[327] One aspect mentioned in improving the

---

319. Harvey, *supra* note 177.

320. *Id.*

321. *Id.*

322. *Id.*

323. *See, e.g.*, *id.* (giving no fault car insurance as an example of a minimal coverage requirement demanded by legislature).

324. *See* Press Release, NAIC, Insurance Regulators Establish Cyber Security Task Force (Nov. 19, 2015), http://www.naic.org/Releases/2014_docs/insurance_regulators_establish_cybersecurity_task_force.htm.

325. *Id.*

326. *2016 Adopted Committee Charges*, NAIC (Aug. 29, 2016), http://www.naic.org/documents/index_committees_2016_committee_charges.pdf.

327. NAT'L ASSOC. OF INS. COMM'RS, PRINCIPLES FOR EFFECTIVE CYBERSECURITY: INSURANCE REGULATORY GUIDANCE (2015), http://www.naic

state of cyber-liability insurance is the involvement of regulators.[328] The NAIC hopes that the involvement of regulators would identify uniform standards, promote accountability across the insurance sector, and provide access to essential information in order to identify risks and offer practical solutions.[329] A mandatory cyber-insurance regime cannot be done with just the regulators and it cannot be done solely by the insurance companies—it must be a joint effort.[330]

CONCLUSION

Implementing a mandatory cyber risk regime protects at-risk corporations and the public at large. The importance of having coverage increases as cyber threats evolve and more personal and financial information is stored. With data breaches becoming more frequent and more damaging with each passing year, the importance of state-of-the-art cybersecurity and prevention measures only increases. Furthermore, like automobile insurance, mandatory cyber-insurance assures that victims will be properly compensated in the event their personal and financial information is inadvertently exposed. All parties ultimately benefit from a compulsory cyber-insurance regime.

.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

328. *Id.* at 1.

329. *See id.*

330. *Id.* (showing that a joint effort is the most effective solution).

***