Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity

Lauren Miller[*]

ABSTRACT

Cyber insurance policies, also known as cyber risk insurance or cyber liability coverage, have become imperative as data breaches and information theft continue to proliferate and adversely affect a vast array of American society. The current U.S. federal regulatory scheme fails to hold corporations accountable for negligent data management, and leaves victims facing countless obstacles in litigating their losses. Yet, the frequency and volume of class actions and derivative lawsuits concerning corporate data theft is only likely to increase. This Article seeks to propose that a large-scale adoption of corporate cyber liability coverage would generate a market solution to rampant data theft by aligning incentives to implement and maintain robust cybersecurity frameworks. This would, in turn, reduce the burden on corporations, while simultaneously fostering a durable data protection infrastructure and a compensation system for data theft victims.

It is undeniable that the world is evolving into a technologically dominated society. Consumers patronize businesses that only operate online, pay bills from mobile devices, and earn academic degrees from the comfort of their homes—all without stepping into brick and mortar facilities. This digital transition has significantly reduced information costs and physical waste,[1] *increased efficiencies in communication,*[2]

---

[*] J.D. candidate at the University of Maryland Francis King Carey School of Law.

[1] *See, e.g.*, Andrew P. Morris, *Real People, Real Resources, and Real Choices: The Case for Market Valuation of Water*, 38 TEX. TECH L. REV. 973, 980 (2006) (discussing technology and cost reductions); Angela Yu, *Let's Get Physical: Loss of Use of Tangible Property As Coverage in Cyber Insurance*, 40 RUTGERS COMPUTER & TECH. L.J. 229, 233 (2014) (noting reductions in paper waste due to technology).

[2] *See generally* Alan Cowell, *Embracing the Power of the Internet*, N.Y. TIMES (Jan. 23, 2014), https://www.nytimes.com/2014/01/24/world/europe/embracing-the-power-of-the-internet.html (exploring the "revolutionary changes in the global flow of information" and the unintended effects it has brought upon the news industry).

and entirely transformed business management practices.[3] *However, as the recent data breach of Equifax, Inc. demonstrates, entrusting the intricacies of modern life to the cyber realm has inadvertently ushered in an increased risk of harm.*[4] *With the growing trend of data breaches comes the expanding scope of corporate liability, spurred in part, by the affected individuals. This Article concludes by contending that a compulsory, nation-wide adoption of cyber insurance coverage would encourage corporations to be proactive about cybersecurity practices through monetary incentives and pressure from insurance carriers to prevent future breaches, and therefore, litigation.*[5]

I. INTRODUCTION

As of 2017, fifty-two percent of all data breaches that occurred in the United States were committed by malicious or criminal hackers, while twenty-four percent were caused by human error and twenty-four percent attributable to network glitches.[6] As the former Acting Deputy Under Secretary for the U.S. Department of Homeland Security (DHS), Greg Schaffer, stated:

> The reality is that we are increasingly under attack in a dangerous cyber environment. The attacks are more targeted, more sophisticated, and more serious than they have been in the past. Our

[3] *See* Hazel Glenn Beh, *Physical Losses in Cyberspace*, 8 CONN. INS. L.J. 55, 57 (2001) (observing that "[t]he assets of businesses are increasingly intangible");

[4] On September 7, 2017, consumer credit reporting agency Equifax Inc. disclosed one of the largest data breaches in U.S. corporate history. *See* Alison Frankel, *Equifax Data Breach Liability Could Hinge on Where Case is Tried*, REUTERS (Sept. 12, 2017, 2:25 PM), https://www.reuters.com/article/us-otc-equifax/equifax-data-breach-liability-could-hinge-on-where-case-is-tried-idUSKCN1BJ2BO. Among the data compromised were records containing "the names, Social Security numbers and driver's license numbers, of as many as 143 million U.S. consumers." *Id.*; *see generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 2 (2017) (defining a "data breach" as "an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers, or financial information such as credit card numbers").

[5] *See infra* Part II.A.

[6] PONEMON INST., 2017 COST OF A DATA BREACH STUDY 15 (2017).

> adversaries are stealing sensitive information, both from government and from industry, and they are taking away our comparative economic advantage as they do so, as well as jeopardize individual privacy.[7]

When a corporation's infrastructure is hacked, valuable data is usually stolen and sold for profit.[8] This often includes the personally identifiable information (PII) of customers or employees used for identity theft, or financial information used for account takeovers or carding.[9] Cyberattacks generate substantial costs for corporations that suffer from data breaches.[10] These losses are not limited to repairing the cyber infrastructure and replacing physical hardware, but includes the intangible damage to goodwill, reputation, and stock valuations.[11] As the scope and magnitude of data breaches increase, companies are forced to rethink how they protect themselves and their customers.

In its *Security and Privacy Enhancing Best Practices* report, the Online Trust Alliance surveyed 500 data breaches in 2014 and revealed that ninety percent of them could have been prevented with simple security measures.[12] Data breaches cost an average of $225 per stolen record in the United States, however strong information security systems coupled with "dedicated security specialists, structured breach

---

[7] *Cyber Security: Threats to the Financial Sector: Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the H. Comm. on Fin. Servs.*, 112th Cong. 11 (2011) (statement of Greg Schaffer, Acting Deputy Under Secretary, DHS).

[8] Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 264 (2012).

[9] Identity theft occurs when "an individual's sensitive personal information is used fraudulently," whereas an account takeover is where existing bank accounts are compromised. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 1–2, 9; *see* Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375, 380–81 (2009) (stating that "[t]he term [carding] has evolved . . . to include an assortment of activities surrounding the theft and fraudulent use of credit and debit card account numbers including computer hacking, phishing, cashing-out stolen account numbers, re-shipping schemes, and Internet auction fraud").

[10] *See infra* Part I.A.

[11] Matt Egan, *The Disclosure Debate: When Should Companies Reveal Cyber Attacks*, FOX BUS. (Oct. 28, 2011), http://www.foxbusiness.com/features/2011/10/28/disclosure-debate-when-should-companies-reveal-cyber-attacks.html.

[12] ONLINE TR. ALL., SECURITY AND PRIVACY ENHANCING BEST PRACTICES 1 (2015).

preparedness, and response systems" significantly reduce this cost, which evinces that investment in cybersecurity can yield large returns over time.[13]

Not fully reflected in this per-record cost are the potential expenses associated with class action litigation brought on behalf of consumers whose data was stolen.[14] Litigants seeking to hold corporations liable for data breaches face several hurdles such as: the federal circuit split on granting Article III standing for victims of cyberattacks;[15] establishing causation between the information stolen during a particular breach and any subsequent fraud suffered;[16] and the economic loss doctrine as an absolute bar against common law negligence claims.[17]

Class actions so far have proceeded on statutory claims, such as (1) New York's deceptive trade practices statute in *In re Anthem, Inc.*,[18] where following a 2014–2015 data breach of the insurance provider, the personally identifiable information of 80 million people was stolen; and (2) California's Customer Records Act in litigation against Adobe Systems, Inc. following a 2013 data breach that implicated 38 million customer records.[19] Similarly, Equifax, Inc. is currently facing claims brought under the Fair Credit Reporting Act (FCRA).[20] However, many statutory claims do not provide a private right of action, or only

[13] PONEMON INST., *supra* note 6, at 5; *see* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 621 (2015).

[14] Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 557–58 (2016).

[15] *See infra* notes 39 and 42, and accompanying text.

[16] *See infra* note 42.

[17] *See infra* notes 48 and 49.

[18] *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 967 (N.D. Cal. 2016); *see* N.Y. GEN. BUS. LAW § 349 (McKinney 2014).

[19] *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014); CAL. CIV. CODE § 1798.82 (West 2017).

[20] *See, e.g.*, Complaint at 15, Jimenez v. Equifax, Inc., No. 1:2017-cv-03885-TWT (N.D. Ga. Oct. 14, 2017), ECF No. 1 (alleging that "Equifax willfully and/or recklessly and/or negligently violated the FCRA . . . by providing prohibited access to consumer reports and by failing to implement and maintain the reasonable procedures . . . designed to limit the unauthorized provision of consumer reports.").

apply to notice and do not cover actual losses.[21] There is currently no comprehensive federal framework addressing data breaches and corporations are often given safe harbor if they comply with notice requirements.[22]

Conversely, it is predicted the law governing corporate liability for data breaches will soon adapt to the growing demand for victim compensation, eventually lessening the burden on litigants seeking recovery from the corporation.[23] As Justice Rehnquist aptly stated:

> Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.[24]

The present landscape regarding corporate liability after a cybersecurity breach is likely to shift as data theft grows in both frequency and magnitude. Moreover, there is likely to be an onslaught of derivative suits brought by shareholders alleging gross negligence for the board of directors' failure to manage and oversee the implementation of data security reasonably sufficient to protect their consumers from cybercrime.[25] If corporations utilized cybersecurity

---

[21] Michelle A. Reed et al., *Fiduciary Duties of Directors Are Key to Minimizing Cyber Risk*, NAT'L ASS'N OF CORP. DIRS., May–June 2015, at 41, https://www.akingump.com/images/content/3/6/v2/36491/NACD-article.pdf.

[22] *Id.*; *see, e.g.*, S.C. CODE ANN. § 39-1-90a (providing a "person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.").

[23] Reed et al., *supra* note 21, at 41 ("At the state level, class action plaintiffs generally bring claims for negligence, breach of express or implied contract, unjust enrichment, mitigation costs, and lost time and inconvenience, with varying levels of success. The recent Sony breach highlights that risk is no longer limited to the payment card industry or similar third-party cases.").

[24] Bartnicki v. Vopper, 532 U.S. 514, 541 (2001).

[25] *See, e.g.*, *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

insurance, the currently misaligned incentives to protect consumer data will be corrected with pressure from the insurance provider to prevent future cyberattacks.[26] This in turn will create a robust data security infrastructure—lessening the likelihood of a successful data breach—and provide recourse to victims when a breach does occur.

II. INCREASING FREQUENCY OF DATA BREACHES: LITIGATION ON THE HORIZON AND THE (DIS)INCENTIVES TO PROTECT INFORMATION

A. Current Costs Associated with Data Breaches

Following a cyberattack, corporations are faced with the costs of repairing or updating their security systems, notifying potentially impacted customers about the breach, and possibly working with law enforcement to identify the culprit(s).[27] While each of these activities are costly, corporations also face a loss of consumer confidence and loyalty, reduced stock prices, and damage to goodwill.[28]

A 2017 report by McAfee estimates that cyberattacks cost approximately $400 billion annually for companies and governments across the globe.[29] In its annual *Cost of Data Breach Study* in 2017, the Ponemon Institute analyzed 419 companies from around the world that experienced a data breach and found the average cost per institution was the highest in the United States at $7.35 million.[30] Of this amount, $0.65 million is purely attributable to notification costs, while another $1.56 million are costs associated with ex post remedial efforts such as product discounts and identity protection services, inter alia.[31]

Industries with the highest per capita costs after a cyberattack include the health, financial, services, education, and life sciences,

---

[26] *See infra* Part I.D.

[27] *See infra* note 31, and accompanying text; *see also Information Sharing and Awareness*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/topic/cybersecurity-information-sharing (requesting private sector information following cyberattacks) (last visited July 1, 2019).

[28] *See infra* note 36.

[29] MCAFEE, TILTING THE PLAYING FIELD: HOW MISALIGNED INCENTIVES WORK AGAINST CYBERSECURITY 6 (2017).

[30] PONEMON INST., *supra* note 6, at 5. Brazil had the lowest average cost at $1.52 million.

[31] *Id.* at 21, 22.

respectively.[32] Of the three root causes of a data breach—malicious hacking, human error, and system glitches—the per capita cost of a malicious hacking is the most expensive at $244, twenty-two percent higher than that of a system glitch.[33] Companies in the United States that experience revenue losses due to these attacks also face subsequent reductions in employment, where "$100 billion translates to approximately 508,000 lost jobs."[34]

In addition to the expenses that are incurred in attempting to rectify a data breach, corporations also "see tangible drops in consumer confidence and profitability, which in turn affects their bottom line and the value of the corporation through the eyes of its shareholders."[35] The Ponemon Institute estimates that corporations in the United States incur approximately $4.13 million in lost business costs after a cybersecurity breach.[36] Included in this figure are "abnormal turnover of customers, increased customer acquisition activities, reputation[al] costs[,] and diminished goodwill."[37] However, breaches involving the loss of customer data are likely to cause higher lost business costs.[38]

B. Anticipated Costs Associated with Litigation

Breached corporations that lose the personally identifiable information of their customers are also certain to experience increased litigation from class actions brought on behalf of the victims. Prior to 2007, class action certification for data breach victims was denied as the victims could not allege a substantial injury-in-fact for Article III standing because: (1) no particular injury had yet occurred or may ever

---

[32] *Id.* at 13. The industries least likely to experience a data breach are the public sector, research, media, transportation, and hospitality industries, respectively.

[33] *Id.* at 16.

[34] Matt Egan, *Report: Cyber Crime Costs Global Economy Up to $500B a Year*, FOX BUS. (July 22, 2013), http://www.foxbusiness.com/features/2013/07/22/report-cyber-crime-costs-global-economy-up-to-1-trillion-year.html.

[35] Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 200 (2014).

[36] PONEMON INST., *supra* note 6, at 22.

[37] *Id.* This was calculated by assigning a "lifetime value" to an average customer, then analyzing existing customer turnover and estimating the number of target customers lost due to the breach. *Id.* at 30.

[38] *Id.*

occur, and (2) the link between the data theft and any subsequent identify theft or fraud could not likely be established.[39]

However, in *Pisciotta v. Old National Bancorp*, the Seventh Circuit granted standing to the victims of a 2005 data breach that implicated the bank's customers' personally identifiable information, such as social security numbers, driver's license numbers, mothers' maiden name, and financial account numbers.[40] The Court held that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions," which data theft satisfies.[41] On the other hand, most other Circuit Courts consistently still deny standing to victims of corporate data breaches.[42] If the Circuit split swings in favor of the Seventh Circuit's approach, corporations are certain to face significant increases in the quantity of lawsuits instigated after a data breach.

---

[39] U.S. CONST. art. III, § 2. See Clara Kim, *supra* note 14, at 557, 575, for a discussion of standing in data breach cases:

> In data breach cases, many plaintiffs have not been able to meet the standing requirement. District courts across the country have often imposed a high bar, often dismissing these cases before they even get through the door.
>
> . . . .
>
> As more class actions are granted standing, more of them have a chance at succeeding on their merits, and companies will be exposed to a greater risk of being liable. Currently, stringent interpretation of standing requirements is a major obstacle to getting consumer victims into court across the board, not just in the realm of data breach cases.

[40] 499 F.3d 629, 364 (7th Cir. 2007).

[41] *Id.* The Supreme Court issued an opinion further tightening the standing requirements, *see* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013), but the Seventh Circuit subsequently revisited the matter and came to the same conclusion. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

[42] *Se,e e.g.,* Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008) (finding that the plaintiff's actual financial losses were sufficient to establish standing, but the risk of identity theft in the future was "somewhat 'hypothetical' and 'conjectural'"). The Ninth Circuit is the only other Circuit to find a heightened risk of future harm is sufficient to establish an injury-in-fact for data theft. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

In the event that standing is granted, litigants primarily bring statutory claims.[43] Nearly every state has enacted a law "governing data security breach notification, while only a handful of states have implemented data security requirements applicable to any entity collecting information about residents of their state."[44] However, there is currently no comprehensive federal regulatory scheme for data security.[45] The Federal Trade Commission (FTC) is the regulatory body most likely to bring enforcement actions against corporations following a breach of consumer data.[46] Common among the statutes enforced by the FTC is that the institution must have either violated a notice requirement, taken an action deemed "unfair or deceptive," or violated a statute pertaining to one of the few regulated industries, such as health care, banking, or credit reporting to incur liability.[47] This exempts from liability under the Federal Trade Commission Act any corporation that does not operate in one of the few regulated industries, that suffered a cyberattack, but met the notification requirements.

C. Litigation Going Forward

Corporations that currently do not fall under the federal regulations would face a substantial increase in liability if the victims of data breaches were not barred by the economic loss doctrine in

---

[43] *See supra* notes 18–20. In lieu of statutory claims, consumers could theoretically bring a breach of contract claim, except where there is an exculpation clause for data theft hidden in the fine print.

[44] Crystal N. Skelton, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 COMPETITION: J. ANTI., UCL & PRIVACY SEC. ST. B. CAL. 305, 305–06 (2016).

[45] *Id.* at 305.

[46] *Id.* at 306.

[47] *See, e.g.,* Gramm–Leach–Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (2018) (requiring financial institutions protect consumers' nonpublic personal information pursuant to the "Safeguards Rule," which requires a rigorous written information security program); Federal Trade Commission Act of 1914 (codified as amended at 15 U.S.C. § 45(a)(1) (2018)) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."); Fair Credit Reporting Act, 15 U.S.C. § 1681s (2018) (prescribing that a "violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce, in violation of section 5(a) of the Federal Trade Commission Act").

bringing common law tort claims such as negligence.[48] Recently, both the First and Third Circuits dismissed claims of negligence brought against corporations following a data breach where the personally identifiable information of consumers was stolen, but where there was no physical damage to person or property.[49] Given that the economic loss doctrine bars negligence claims seeking only monetary losses in order to have the issues adjudicated under contract law, data breach victims are left without recourse where: (1) there exists no contract between the corporation and consumer;[50] (2) the relevant state laws do not provide a private right of action, or (3) where there is a state statute, but it applies only to notifying potential victims.[51]

Nonetheless, as the Seventh Circuit's approach to Article III standing indicates, courts or legislatures may eventually be willing to allow consumers to overcome this doctrine as the future risk of harm becomes more prevalent and the demands for recovery mount.[52] Negligence claims could be established by proving that the breached cybersecurity system did not meet industry or national standards, or that the corporation unreasonably failed to take adequate steps to

[48] Giles v. Gen. Motors Acceptance Corp., 494 F.3d 865, 873 (9th Cir. 2007) (explaining "[t]he economic loss doctrine provides that certain economic losses are properly remediable only in contract. The doctrine has roots in common law limitations on recovery of damages in negligence actions in the absence of physical harm to person or property").

[49] *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009) (dismissing negligence claim based on economic loss doctrine under Massachusetts law in absence of property damage); Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 175–77 (3d Cir. 2008) (dismissing negligence claim based on economic loss doctrine under Pennsylvania law in absence of property damage).

[50] For example, in the Equifax breach, consumers' information was collected involuntarily. *See* Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, N.Y. TIMES (Sept. 8, 2017), https://nyti.ms/2wPtl6g ("[C]onsumers have little choice, since banks and other companies hand over financial information and other data directly to the bureaus.").

[51] *See, e.g.*, Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009) (finding no private right of action for negligence, permitting only the Missouri A.G. to bring notification claims under MO. REV. STAT. § 407.1500).

[52] *See supra* notes 40–41, and accompanying text.

protect consumer data or mitigate losses.[53] This is especially critical where the consumer information was involuntarily collected, such as was the case with Equifax, because the consumer had no opportunity to decline to interact with that corporation and therefore escape injury.[54] Rather, corporations are the sole party in a position to safeguard the information they collect, and from which they profit.

In addition to suits brought by consumers, there is likely to be an increased number of derivative actions following a data breach.[55] Recently, shareholders of Home Depot filed a derivative suit following the 2014 cybersecurity breach that implicated the financial information of 56 million customers.[56] In their complaint, the shareholders alleged three corporate officers and four board members breached the duty of loyalty by: (1) not implementing sufficient internal controls to protect against the breach; and (2) by disbanding an oversight committee in charge of cybersecurity.[57] Though the district court dismissed the case, similar suits are still being filed.[58]

Corporate directors and managers should also be wary of the vendors with whom they contract and come into digital contact. As Target has experienced, security breaches can originate in the hardware of third parties, unbeknownst to the contractor.[59] Going forward,

---

[53] Plaintiffs, even if able to establish that merchants who collect their data owe them a duty in the absence of a statutory provision creating such a duty, would most likely struggle to prove a causal link between any one particular hacking incident and subsequent identity theft. The harm suffered would be money spent on credit monitoring, and inconvenience in freezing accounts, etc.

[54] *See supra* note 50.

[55] Michelle Reed et al., *supra* note 21, at 41.

[56] *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

[57] *Id.* at 1321.

[58] *See* Alison Frankel, *An Opening for Shareholders in Federal Court Derivative Suits?*, REUTERS (Dec. 1, 2016, 5:35 PM), http://www.reuters.com/article/us-otc-derivative/an-opening-for-shareholders-in-federal-court-derivative-suits-idUSKBN13Q5WG; *see also* Judy Greenwald, *Data Breaches Bring Litigation Related to Directs and Officers Liability*, BUS. INS. (June 8, 2014, 6:00 AM), http://www.businessinsurance.com/article/20140608/NEWS07/306089968 (discussing the derivative suits filed by shareholders of Target and Wyndham Worldwide Corp.).

[59] *See* Gregory Wallace, *HVAC Vendor Eyed as Entry Point for Target Breach*, CNN MONEY (Feb. 7, 2014, 10:39 AM), http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html.

derivative actions may be based on corporate insiders' failure to exercise appropriate oversight in confirming that third parties with whom the corporation interacts, operate strong cybersecurity systems to ensure the vendors do not pose a risk to customers' data.

D. Misaligned Incentives

There are several expenses associated with data protection that disincentivize corporations from implementing a robust cybersecurity infrastructure, such as: the ongoing cost of security administration and updates;[60] information costs related to understanding and advocating for industry best practices;[61] and oversight costs once the mechanisms are put in place.[62] This is evidenced by the current state of industry standards in cybersecurity. As the former Assistant Director of the Cyber Division for the FBI, Gordon M. Snow, stated:

> [I]f we look at the standards, the industry standards, across networks in all organizations, whether it is government, private sector or public sector, I don't think they are very high. We talk a lot about the advanced persistent threat. It may be persistent because it is still resident in the system, but I don't know that the techniques that we are using, to use a high school analogy, is the varsity team that is coming in. It is the freshman team who is walking in with phishing emails and getting a socially engineered attack that allows the malware to move laterally across the systems.[63]

Furthermore, while robust cybersecurity implementation may be cost prohibitive, the attendant breaches do not have a substantial financial impact that warrants increasing data protection measures regardless. Benjamin Dean, a fellow for cybersecurity and internet

---

[60] *See, e.g.*, Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1511–12 (2013) ("Studies conducted in 2009 and 2011 by McAfee . . . revealed low levels of investment in cyber-defense. The studies found that many firms regard cyber-security as little more than 'a last box they have to check,' and that they neglect network security because they find it too expensive.").

[61] *See, e.g.*, David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE NOVO 151, 152–54 (2015) (discussing broad misunderstandings and questions surrounding what comprises "cybersecurity").

[62] *See, e.g., supra* notes 56–57, and accompanying text.

[63] *Cyber Security: Threats to the Financial Sector*, *supra* note 7, at 16 (statement of Gordon M. Snow, former Assistant Director, Cyber Division, FBI).

governance at Columbia University, analyzed the Home Depot, Sony, and Target breaches revealed in 2014 and calculated that these cyberattacks costed each company less than one percent of their revenue.[64] Target, for example, lost $252 million after the cyberattack, but received $90 million from insurance and another $57 million in tax deductions, bringing the net loss down to $105 million.[65] Home Depot, on the other hand, lost only $28 million (one tenth of one percent of revenue) after the cybersecurity breach that implicated 56 million credit and debit card accounts.[66]

Moreover, once an individual's identity has been stolen and financial accounts are compromised due to a corporate data breach, it is not the merchant but rather the banking system that bears the costs.[67] This burden includes "(1) costs associated with reissuing new payment cards, (2) costs associated with monitoring open accounts for fraud (with or without reissue), and (3) fraud losses."[68] After the Home Depot breach, banking institutions "claim to have spent $60 million in September 2014 alone in replacing compromised cards," more than double Home Depot's losses.[69]

An illustration of the banking system carrying the financial burden of cyberattacks is found where MasterCard demanded from Target $28 million in damages arising out of the data breach revealed in 2014.[70] This was later settled for $19 million, but as a proviso of the agreement, Target requested that MasterCard approach each bank that

---

[64] 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.

[65] *Id.*

[66] *Id.*

[67] *See* Kim, *supra* note 14, at 584 ("Other entities that private companies work with—such as insurance companies, credit card companies, and banks—might incur the most costs from data breach losses. In fact, holding the company liable does not necessarily incentivize companies to better protect data in those cases, since currently credit card companies and financial institutions are often covering the damages associated with compensating data breach consumer victims in the moments immediately after a breach.").

[68] Peretti, *supra* note 9, at 380 (quoting Declaration of Joel S. Lisker at 11, *In re* TJX Companies Retail Sec. Breach Litig., No. 1:07-CV-10162-WGY (D. Mass. Oct. 26, 2007)).

[69] Kassner, *supra* note 64.

[70] *In re* Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522 (PAM/JJK), 2015 WL 2165432, at *1 (D. Minn. May 7, 2015).

issues its card and request Target be released from potential liability.[71] The banks were approached on April 16, 2015 and MasterCard offered a fixed percentage of their estimated losses if they agreed to release their claims by May 20, 2015.[72] Though the issuing-banks were dissatisfied with the settlement agreement due to the unreasonably short amount of time given to accept the partial reimbursement and sought to have it enjoined, the court denied their claim because "[a]lthough the settlement may not 'pass the smell test,' as the saying goes, it is not serious misconduct."[73]

This paradigm where the responsibility falls on the banking system to remedy consumer losses from fraud and financial account takeover provides an incentive for corporations to reduce investments in data protection rather than implementing cybersecurity measures.[74] As noted by one commentator, "the only tangible, significant incentives for companies to prevent data breach are relatively 'soft' factors, such as consumer trust, consumer loyalty, and public perception concerns. From this point of view, banks might be footing the bill for companies' negligence in most data breaches."[75]

To solve this misalignment, cybersecurity insurance can step in as an external gate-keeping mechanism and fill the gap in oversight of corporate data security implementation. Previously, it may have been possible to reduce expenses by not performing best practices in cyber hygiene, but proliferate data breaches are changing the cybersecurity landscape at the expense of consumers.[76] While the cost of internalizing these expenses is great and presently unattainable through tort law, companies that elect to forgo investing in cybersecurity may face unprecedented liability in the near future.[77] It is in the best interests of corporations and consumers to realign incentives to maintain strong

---

[71] *Id.*

[72] *Id.*

[73] *Id.* at 2.

[74] Kim, *supra* note 14, at 578.

[75] *Id.* at 585.

[76] Stephanie Cohen & Mark Morril, *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 FORDHAM INT'L L.J. 981, 1014 (2017) ("Cybersecurity experts agree that good cyber 'hygiene'—basic everyday habits relating to technological use—is essential to a strong, baseline defense.").

[77] Sales, *supra* note 60, at 1520.

cybersecurity policies and protect personally identifiable information.[78]

III. CYBER INSURANCE: A SOLUTION TO CORPORATE DATA BREACHES

Though cyber insurance may not yet be mainstream, it has been in existence since the 1970s and is purchased by clients of all sizes.[79] The current "[t]otal annual cyber premiums have reached $2.5 billion, with some predicting the market could grow to $20 billion or more" in the next decade.[80] A recent survey of companies that do not currently carry cybersecurity insurance found that seventy-four percent of these enterprises are contemplating purchasing a policy within the next two years.[81] However, even some massive enterprises elect to forgo purchasing this insurance, such as in the banking industry where the ten largest United States banks run the gambit between no cybersecurity insurance to $400 million in specific cyber coverage.[82]

Cyber insurance helps corporations achieve "risk management, where risk is a function of three variables: vulnerabilities, threats, and consequences."[83] By carrying this type of insurance, companies mitigate: (1) their own losses incurred as a result of cyberattacks and those subsequently induced by litigation; (2) damage to their network

---

[78] See, for example, Avellan, *supra* note 35, at 195–96, for a discussion of the various parties implicated by growing prevalence of data breaches:

> The ripples and reverberations that follow a major data breach are felt by the affected corporation, its board of directors, shareholders, and customers. In today's online business forum, cybersecurity is vital. The increasing rate of major data breaches implicates various parties: the SEC is involved through its obligation to protect investors, boards of directors are involved through their disclosure and cybersecurity obligations (or lack thereof), and a corporation's shareholders are involved through their ownership and stake in the corporation.

[79] Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, J. CYBER POL'Y, Mar. 27, 2017, at 53, 55.

[80] *Id*. at 59.

[81] AM. BANKERS ASS'N, FIN. SERVS. SECTOR COORD. COUNCIL FOR CRITICAL INFRASTRUCTURE & HOMELAND SEC., 2016 CYBER INSURANCE BUYING GUIDE 3 (2016), https://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf [hereinafter FSSCC REPORT].

[82] *Id.* at 5.

[83] Sales, *supra* note 60, at 1511.

and associated hardware, (3) and interruption of business operations.[84] Insurance companies, in an effort to ameliorate vulnerabilities and prevent losses, would require strong security measures by the insureds which would facilitate the development of industry wide best practices in cyber hygiene, if widely adopted.[85] This is becoming especially critical as traditional commercial general liability insurance now routinely excludes data breaches.[86] However, market entrants are hesitant to join this emerging industry sector due to a lack of actuarial information on the true costs associated with cybercrime, as well as uncertainties in potential liability.[87]

Cyber insurance comes in both first and third-party coverage; the former may cover losses from property damage, stolen funds, business interruption, and extortion if the system is held for ransom; whereas the latter may cover stolen consumer and employee data, victim notification, and public-relations remediation, but most likely not damage to reputation.[88] After the myriad of data breaches in 2014, premiums greatly increased and coverage caps of $100 million were implemented.[89] To purchase better protection and coverage, companies "tower" policies whereby one premium policy is purchased and then subsequent policies are "layered" on top to achieve the desired amount of coverage.[90]

After the data breach of Anthem, the health insurer struggled to renew its cyber insurance policy at first, but eventually managed to secure $100 million in coverage—after agreeing to cover the first $25

---

[84] *See Cybersecurity Insurance*, DEP'T OF HOMELAND SEC. (June 30, 2016), https://www.dhs.gov/cybersecurity-insurance.

[85] *See id.*

[86] FSSCC REPORT, *supra* note 81, at 6.

[87] John Winn & Kevin Govern, *Identity Theft: Risks and Challenges to Business of Data Compromise*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 49, 53 (2009).

[88] Sarah Brown, *Ten Things You Need to Know About Cybersecurity Insurance*, DATA CENTER JOURNAL (June 15, 2016), http://www.datacenterjournal.com/ten-things-need-know-cybersecurity-insurance.

[89] Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*, REUTERS (Oct 12, 2015, 1:33 AM), http://www.reuters.com/article/us-cybersecurity-insurance-insight/cyber-insurance-premiums-rocket-after-high-profile-attacks-idUSKCN0S609M20151012.

[90] FSSCC REPORT, *supra* note 81, at 2 (stating that no more than $400 million in coverage is available even with the largest of these towers).

million incurred as a result of any future data breaches.[91] In October 2017, drug maker Merck & Co suffered a world-wide cyberattack from malware known as "NotPetya" and endured significant disruption of its business operations.[92] Though the full extent of the damage is not yet known, it is possible that cybersecurity insurance may pay up to $275 million for the portion of losses covered by its cybersecurity policy.[93] Interestingly, Target likewise carries cybersecurity insurance but not one or two all-encompassing policies.[94] Rather, Target's coverage is towered among nine separate cybersecurity insurance policies.[95] On the other end of the spectrum, Equifax has $100 million to $150 million in cybersecurity insurance but will also attempt to use its other insurance policies—crime, business interruption, and general-liability, for example—to cover some of the losses that are very well likely to exceed $150 million.[96]

A. Aligns Incentives

As described in Part I.D, the incentives for corporations to reduce investments in cybersecurity appear to outweigh the incentives to implement and maintain secure data protection systems.[97] Widely adopted cyber liability insurance can remedy this by realigning these

---

[91] Finkle, *supra* note 89.

[92] *Merck Cyber Attack May Cost Insurers $275 Million: Verisk's PCS*, REUTERS (Oct. 19, 2017, 1:37 PM), http://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP (according to one insurer, cybersecurity insurance can cost up to $100,000 for $10 million in data breach coverage).

[93] *Id.*

[94] Judy Greenwald, *Target Has $100M of Cyber Insurance, $65M of D&O Cover: Sources*, BUS. INS., (Jan. 14, 2014), http://www.businessinsurance.com/article/20140114/NEWS07/140119934.

[95] *Id.* ("Target is self-insured for the first $10 million of cyber coverage . . . [with] additional cyber insurance through: $15 million of excess coverage with Ace Ltd.; then a $15 million layer with American International Group Inc.; a $10 million layer with Bermuda-based Axis Capital Holdings Ltd.; another $10 million coverage layer with AIG; then a quota share for the next $40 million of cyber insurance divided among four unidentified insurers.").

[96] Sonali Basak, *Is Equifax's Cyber Insurance Enough to Cover Breach?*, INS. J. (Sept. 11, 2017), https://www.insurancejournal.com/news/national/2017/09/11/463769.htm.

[97] *See supra* Part I.D.

incentives and facilitating the adoption of industry best practices in cybersecurity. If the market for this product became attractive enough for insurance companies to enter and provide policies that were more economical than reducing data protection costs and suffering the potential losses, enterprises would purchase this product to protect themselves, and in turn would conform to the standards mandated in the policy or otherwise risk losing coverage.[98]

Policy conditions may include the adoption of particular security mechanisms or meeting specified industry or national best practices.[99] There would be monetary incentives for creating a robust security system as premiums for cybersecurity insurance would be based on how secure the cybersecurity infrastructure is, measured in part by the frequency and magnitude of cyberattacks that successfully penetrate the infrastructure, as well as any exemplary cyber hygiene practices, or lack thereof.[100] By requiring these practices as a condition of coverage, the cybersecurity insurance industry would facilitate the wide-spread adoption of sophisticated data security systems in the effort to ward off both business and consumer losses.[101] With sufficient popularity and time, the adopted robust data protection mechanisms would become the new industry standards. Moreover, when an enterprise invests in stronger cybersecurity, the data security infrastructures of the other corporations it interacts with likewise become more protected because the investment will "prevent the firm's system from being used to inflict harm on others' systems."[102]

Even prior to purchasing a policy, corporations will begin to improve their security measures and cyber hygiene practices as underwriters will investigate the cybersecurity infrastructure already in place in order to price coverage.[103] The measures and practices an underwriter will inquire about are: the employ of dedicated information security personnel; compliance with standard industry or national cybersecurity procedures; employee training and testing on phishing and other user errors; incident response planning; security mechanisms

---

[98] *See supra* Part I.A.
[99] FSSCC REPORT, *supra* note 81, at 4.
[100] *Cybersecurity Insurance*, *supra* note 84.
[101] *Id.*
[102] Sales, *supra* note 60, at 1527.
[103] FSSCC REPORT, *supra* note 81, at 7.

employed; third-party vendor oversight and management; and board oversight.[104]

Though a completely secure system is unachievable and costly both in terms of the security mechanisms implemented and the expenses associated with oversight, purchasing these policies and attempting to protect consumer and corporate information may be less cost prohibitive in the future if class action litigation following data breaches is permitted to go forward under a negligence regime.[105] As one commentator noted, enterprises currently underfund their cybersecurity measures because the cost of internalizing the negative externalities of information theft are too substantial, and tort law does not force them to do so.[106] However, if faced with the possibility of litigation for negligent data protection, corporations would provide more secure cybersecurity infrastructures to prevent losses and turn to insurance as a safeguard when the threat of liability is imposed.

B. Need for Oversight

Cybersecurity insurance companies would provide the necessary oversight for the implementation of these required data security measures. Although the FTC has the authority monitor companies that are found to have violated a cybersecurity regulation, this applies ex post and only to enterprises that violate notification requirements or operate in one of the few regulated industries.[107] Corporations that do not prioritize data security and invest in data protection systems are unlikely to employ managerial oversight of their cybersecurity systems, leaving themselves vulnerable to cyberattacks and litigation from both consumers and shareholders.[108]

On the other hand, a recent survey found that more than half of business leaders rank cybersecurity as a severe risk.[109] Where strong cybersecurity is expected or advocated for by owners, corporate

---

[104] *Id.*

[105] *Cyber Security: Threats to the Financial Sector*, *supra* note 7 (statement of Carolyn Maloney, former ranking minority leader).

[106] Sales, *supra* note 60, at 1520.

[107] 15 U.S.C. § 45(l) (2018).

[108] Skelton, *supra* note 44, at 316.

[109] INSURANCE 2020 & BEYOND: REAPING THE DIVIDENDS OF CYBER RESILIENCE, PRICEWATERHOUSECOOPERS 8 (2017).

insiders must monitor their officers to ensure that these measures are put in place and continually updated in anticipation of cyberattacks from sophisticated malware.[110] The duty owed by the board to shareholders regarding the oversight of data protection is paramount to risk management, but there remains a significant disparity between the magnitude of cyber-threats and affirmative actions taken by the board to combat these risks.[111]

The need for oversight could be met where companies have a cybersecurity insurance policy because insurers would require reports and system inspections as conditions of coverage.[112] These reports could be both periodic and ad hoc as severe risks and attacks arise.[113] Based on these reports, insurance companies could create analytics that identify industry-wide vulnerabilities and threats. With this information, insurers would direct their clients to anticipate these risks and provide instruction on how to mitigate them. Furthermore, insurance companies would likely need to develop an investigatory body that audits the insureds' cybersecurity infrastructures to determine if the policy conditions are being met.[114] By inspecting the security systems of the corporations, insurance companies ensure that the cybersecurity infrastructures are strong, but also create new

---

[110] *See supra* notes 56–59, and accompanying text.

[111] Luis A. Aguilar, Comm'r, Sec. & Exch. Comm'n, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Address at the "Cyber Risks and the Boardroom" Conference (June 10, 2014), https://www.sec.gov/news/speech/2014-spch061014laa (listing several examples of board oversight activities that mitigate cybersecurity risks, including "undertaking key oversight activities related to cyber-risks, such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks").

[112] INSURANCE DATA SECURITY MODEL LAW § 4(E) (NAT'L ASSOC. OF INS. COMM'RS, Proposed Draft No. 6, 2017), http://www.naic.org/documents/cmte_ex_cswg_final_model_law_v6_clean.pdf.

[113] *Id.* § 6.

[114] The corporate insider counterpart to this would be a committee of board members or other managers that are tasked with evaluating cybersecurity standards compliance. The external investigatory body could either be brought in-house by insurance companies or outsourced, for which Apple and Cisco currently advocate. *See* Stephen Nellis, *Apple, Cisco Team Up to Push for Cyber Security Insurance Discounts*, REUTERS (June 26, 2017, 2:49 PM), https://www.reuters.com/article/us-tech-cyber-apple-cisco-systems/apple-cisco-team-up-to-push-for-cyber-security-insurance-discounts-idUSKBN19H2BK.

industry standards as these measures become uniform for all companies with similar policies.

C. Threats from Moral Hazard and Reinsurance

If cybersecurity insurance were to become the touchstone of data protection, consumers would face threats to the security of their data due to moral hazard, and corporations would face threats to recovery if a breach occurred because of the potential for reinsurers to seize on the ambiguities surrounding cybersecurity insurance. Moral hazard is where the incentives to mitigate against harm decrease as insurance softens the hardship of risks and losses for which the insurance was purchased.[115] The economic view of moral hazard posits that the more insurance compensates for actual loss, the less it is appreciated or "felt," and that incongruity in turn encourages more risk-taking behavior until the loss felt makes that behavior cost prohibitive.[116] To combat this lack of due care, insurance companies elect to inflate premiums for riskier practices or parties, withhold payments where an event stipulated in the policy occurs, or simply refuse to insure particular parties.[117]

In the cybersecurity insurance context, premiums would be based on the findings of the underwriting process, as well as which industry the enterprise operates in, and the type of data it collects.[118] By basing premiums on the security mechanisms already in place, the likelihood of moral hazard is reduced at the onset because corporations would already be incentivized to ameliorate cybersecurity risks.[119] Moral hazard after a policy is in place is further tempered by requiring

---

[115] Tom Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV. 237, 238–39 (1996); *see* A.M.I. Diamonds Co. v. Hanover Ins. Co., 397 F.3d 528, 530 (7th Cir. 2005) (defining moral hazard as "the effect of insurance in causing the insured to relax the care he takes to safeguard his property because the loss will be borne in whole or part by the insurance company.").

[116] Baker, *supra* note 115, at 271.

[117] *Id.* at 240–41; A.M.I. Diamonds Co., 397 F.3d at 530. Insurance companies also offer policy discounts, or conversely require high deductibles. *See supra*, text accompanying note 91.

[118] *See supra* note 102, and accompanying text; *Insurance 2020 & Beyond*, *supra* note 109, at 10 (identifying, for example, the health care industry as a market sector particularly vulnerable to data breaches and in demand of cybersecurity insurance).

[119] *See supra* note 101, and accompanying text.

risk reports and system inspections because what constitutes adequate data protection and industry best practices—conditions of coverage—frequently change and would need to be monitored and complied with in order to meet policy requirements.[120] Where these reports and inspections reveal the corporation was negligent in meeting mandatory standards, the insurance company would be able to defend against making settlement payments following a data breach. This, in turn, would encourage corporations to stay vigilant about data protection or risk bearing the full burden of a cybersecurity breach independently.

When a data breach does occur, reinsurance poses a threat to claims settlements due to the uncertainties of this emerging market. Reinsurance is a loss spreading mechanism utilized by the insurance industry, whereby one insurance company (the "reinsured") pays a premium to have another (the "reinsurer") assume a specified risk.[121] In developing insurance market sectors, reinsurance is vital for selling new types of policies because the uncertainties regarding potential losses are mitigated by risk distribution, which also brings down policy prices and attracts more customers.[122] However, the same uncertainties can be used by the reinsurer as grounds for indemnification refusal.[123] Most jurisdictions only recognize four circumstances where a reinsurer can be excused from paying its portion of the settlement under the reinsurance contract, which includes:

---

[120] *See supra* notes 98–100, and accompanying text.

[121] *See generally* N. River Ins. v. Ace Am. Reinsurance Co., 361 F.3d 134, 137 (2d Cir. 2004) (defining reinsurance as a "contract [where] the original insuring entity (the 'reinsured') transfers, or 'cedes,' part or all of its risk under its policy of insurance to another entity (the 'reinsurer')"). There are two types of reinsurance, indemnity and assumption; in the first, the reinsurer reimburses the primary insurer for losses and in the former, the reinsured directly transacts with the policyholder and assumes the liability. Colonial Am. Life Ins. v. C.I.R., 491 U.S. 244, 244 (1989).

[122] *See* Roberta Romano, *What Went Wrong with Directors' and Officers' Liability Insurance?*, 14 DEL. J. CORP. L. 1, 18 (1989) (discussing the role of reinsurance in new insurance markets).

[123] Edward J. Ozog et al., *The Unresolved Conflict Between Traditional Principles of Reinsurance and Enforcement of the Terms of the Contractual Undertaking*, 35 TORT & INS. L.J. 91, 92 (1999) (explaining that the doctrines of uberrima fides and follow the fortunes "were never intended to insulate the cedant from the consequences of its own poor judgment, careless adjusting practices, or unreasonable coverage decisions").

> (1) the loss is beyond the scope of the reinsurance as a matter of law; or
> (2) the loss, in the case of a reinsurance coextensive with the underlying insurance, is beyond the scope of the underlying insurance as a matter of law; or
> (3) the settlement was fraudulent, collusive, in bad faith or otherwise dishonest; or
> (4) the reinsured failed to take all businesslike steps reasonably necessary to properly and carefully investigate and ascertain the amount of the loss.[124]

A reinsurer could seize the inherent uncertainties surrounding cybersecurity to potentially play with the aforementioned exceptions. As technology advances, new terms, cybercrimes, and job descriptions and titles emerge that reinsurers will assert fall outside the scope of the policy, as they were not originally contemplated by the parties.[125] Furthermore, there is currently a significant lack of actuarial data on the impacts of corporate data breaches, and as such, there will likely be large disparities between anticipated and actual losses until sufficient data becomes available to make more precise loss predictions.[126] Until that time comes, reinsurers that are faced with settling losses considerably larger than anticipated will attempt to claim that the risk transferred to them was not honestly or in good faith articulated during negotiations, as evidenced by an enormous loss to cost ratio.

Moreover, reinsurers may further play on the uncertainties of ascertaining the scope of damages and argue that the reinsured failed to fully investigate the breach and mitigate or accurately price the loss. This is especially easy to argue because the full impact of cybercrime is often not immediately realized, or is costlier than at first impression.[127] The average mean time to identify a malicious attack is approximately 214 days, followed by an additional seventy-seven days

---

[124] *Id.* at 93.

[125] Michael Sean Quinn, *The Cyber-World and Insurance: An Introduction to a New Insurance*, 12 J. TEX. INS. L. 20, 21 (2013) (analyzing that changes in the cybersecurity world include new employment roles with titles such as "architecture designers, code construction contractors, platform engineers, digital asset monitors, security risk inspectors and analysts, and many more, some with strange, some with witty, and some with informative descriptions").

[126] *See* Winn & Govern, *supra*, note 87.

[127] PONEMON INST., *supra* note 5, at 6.

to contain it.[128] If the reinsured does not reasonably analyze the breach in a timely manner and assist with mitigation efforts, reinsurers will refuse to pay settlements on the grounds that losses could have been reduced but for the reinsured's failure to carefully investigate and fully ascertain the impact of the breach.[129] This is particularly concerning where companies keep secret cyberattacks they experience.[130] For example, Uber revealed in November 2017 that it hid a data breach from a year prior of 57 million customer and driver records, at which time it paid hackers $100,000 to delete the stolen information.[131]

Eventually however, if cybersecurity insurance helps facilitate the adoption of new cybersecurity best practices and data breaches become adjudicated under a comprehensive statutory scheme, insurance policies—and therefore reinsurance policies—will become accurately priced and the claims process will be made uniform, ultimately lessening the chances of a reinsurer escaping the obligation to indemnify.[132]

IV. A FEDERAL STATUTORY SCHEME IS NECESSARY TO DETER WEAK CORPORATE CYBERSECURITY PRACTICES

A federal statutory scheme that grants a cause of action to victims of data breaches will provide recourse to consumers whose data was stolen, incentivize corporations to prioritize data protection, and if damages are limited, attract more market entrants into the cybersecurity insurance sector.[133] The structure of this statutory scheme would have to include provisions that effectually waive the economic loss doctrine and implement a damages cap.[134] Transgressions of this statutory scheme should not be *per se* violations, but rather these cases should

---

[128] *Id.*

[129] Egan, *supra* note 11 (noting that a 2010 breach of Google was first disclosed as email hacking but much later was revealed to also include a stolen password management system).

[130] To prevent this, insurance companies should void third-party cybersecurity policies where the corporation covers up all or part of a cyberattack.

[131] Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

[132] *See infra* Parts III.A. and III.C.

[133] *See infra* Part III.A.

[134] *See infra* Part III.A.1.

be adjudicatory on a standard similar to a products liability design defect claim.[135]

Congress may elect to structure the data breach statutory scheme similar to workers' compensation statutes for asbestos exposure, of which there exists an analogue.[136] This structure particularly recognizes the different classes of victims, but has short statutes of limitation and moderately low damage caps, which in the cybersecurity context would prevent the bankruptcy of corporations and attract cybersecurity insurers.[137] With this framework in place, cybersecurity insurance settlements will become routinized similar to those of the automotive insurance sector, which will provide an efficient process whereby victims receive compensation but litigation is preserved for egregious consumer data theft.[138]

A. A Private Right of Action Would Compensate Victims, Encourage Robust Corporate Data Security, and Generate More Cyber Liability Insurance Customers

The current inability of consumers to receive recourse after being victimized by a corporate data breach—for which the corporation is currently unlikely to incur significant liability—impermissibly discourages protecting personally identifiable information.[139] There is no way for victims to know when, if at all, their information will be used but a private cause of action available prior to any injury occurring beyond the initial data theft provides victims with a justified remedy.[140] The significantly greater likelihood of liability simultaneously deters corporations from practicing poor cyber hygiene and neglecting to prioritize cybersecurity.[141]

---

[135] *See infra* Part III.A.2.

[136] *See infra* Part III.B.

[137] *Id.*

[138] *See infra* Part III.C.

[139] *See supra* notes 39–51, and accompanying text.

[140] Individuals have a particularly bona fide claim where their sensitive information was collected involuntarily, or in the absence of a contract where the consumer had the ability to negotiate terms. *See supra,* notes 50 and 54, and accompanying text.

[141] *See supra* Part I.D.

Moreover, if corporations are susceptible to liability for data breaches, they would be more inclined to purchase cybersecurity insurance as a means of mitigating loss, which in turn would subject them to the stringent conditions mandated in their policies.[142] This cause of action should (1) have a damages cap that reflects the uncertainties of future injury and (2) be adjudicated on a quasi-design defect standard, but (3) offer no safe harbor to corporations regardless of timely notice after a cybersecurity attack or mere compliance with industry cybersecurity standards.

1. Damages: Compensating an Actual Injury with an Indeterminable Scope

A moderately low damages cap would be appropriate because some consumers will never suffer losses from identity theft, fraud, or financial account takeover, insurers would be increasingly hesitant to enter the market if susceptible to uncertain but potentially significant damages, and when data breaches occur, corporations are victims too. In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit held that consumer data theft is a concrete injury given the substantial risk of harm, and the time and money victims spend to prevent near imminent identity theft or fraud.[143] Congress should adopt this position, and extend it to recognize consumer data theft as an injury *per se* that may trigger litigation under a federal statutory scheme.[144]

This recognized injury should be balanced with a low damages cap because though there exists a substantial likelihood of future identity theft or fraud, it is impossible to ascertain if or to what extent that will occur. If a consumer's financial accounts are implicated, the banking system is still responsible for compensating for losses

[142] *See supra* Part II.A.

[143] 794 F.3d 688, 693–94 (7th Cir. 2015) (holding that credit monitoring services purchased by consumers after a data breach "easily qualif[y] as a concrete injury" because these services are not a *de minimis* expense).

[144] The *Remijas* Court found that victims suffered a concrete injury even though no social security numbers were implicated. 794 F.3d at 690. Congress should be particularly more inclined to recognize that consumers have suffered a real injury when more than just their financial information was implicated, such as with Equifax. *See supra* note 4.

regardless.[145] Moreover, if damages were boundless, insurers would not likely remain in this market sector and certainly would not expand any further into it.[146] A damages cap that compensates victims for current and future harms, but that is modest enough for cybersecurity insurers to be able to provide policies is ideal; premiums will decrease as the damage cap decreases, and more corporations will be inclined to purchase these policies when premiums become affordable.[147]

Some commentators assert that creating a private right of action is inappropriate because it punishes the corporation who is similarly a victim of the data breach.[148] In addition to suffering a breach resulting in information theft, the enterprise is also the party that "becomes the target of nasty headlines, an FTC investigation, and shareholder derivative actions . . . [and the party] that pays the costs of responding to the breach, repairing the breach, and notifying affected customers."[149] However, studies indicate that even minor additions to cybersecurity can dramatically decrease losses from a data breach, and while corporations should not be insurers of their data, they are the sole party in control of their customers' information.[150] A private right of action reflects that corporations are the party ultimately responsible for safeguarding the personally identifiable information they collect and profit from, but a moderately low damages cap recognizes that criminal acts by third-parties may at times be beyond the power of the corporation to prevent.

---

[145] *See supra* notes 67–68 (permitting corporations to escape liability while placing the burden on financial institutions to handle consumer losses disincentives data protection, therefore corporations should still be held accountable when a breach occurs). However, banks are not obligated to entirely reimburse all consumer losses. *Remijas*, 794 F.3d at 696–97. It is also possible that when cybersecurity insurance becomes commonplace, Visa and MasterCard will include a contract provision that requires merchants carry such a policy.

[146] *See* Winn & Govern, *supra* note 87, and accompanying text.

[147] A limit on damages will go into loss predictions and insurance companies will therefore be able to more accurately price premiums. *Id.* This cap may include a schedule organized based on the type of data collected and the number of people impacted. *See infra* note 173, and accompanying text.

[148] *See, e.g.*, Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get over It!*, 19 SMU SCI. & TECH. L. REV. 3, 30 (2016).

[149] *Id.*

[150] *See supra* text accompanying notes 13 and 53.

2. A Quasi-Design Defect Liability Standard

The standard on which to base liability should be structured similarly to a products liability design defect claim.[151] If data breach litigation were analyzed under a standard similar to the risk-utility test of a design defect claim, victims would receive recourse where a corporate data breach was egregious, but corporations would be protected against liability where stringent cybersecurity practices were followed.

The risk-utility test is a version of the Learned Hand Formula which balances the likelihood and severity of injury against the cost of safeguarding against this injury.[152] Traditional design-defect factors include "the availability of alternative designs, the cost and feasibility of adopting alternative designs and the frequency or infrequency of injury resulting from the design."[153] This translates well in the cybersecurity context as the design would the security infrastructure and alternatives would be available data protection mechanisms, such as those used elsewhere in the market.

When a corporation suffers a data breach and litigation is brought on behalf of the consumers impacted, courts can examine the security mechanisms in place and evaluate if: national or industry standards were followed or if they were forgone; the corporation's investment in its data protection mechanisms and information personnel; the diligence and oversight employed in preventing

---

[151] In a majority of jurisdictions, design defects are found where an injurious product fails the risk-utility test. *See* Raney v. Honeywell, Inc., 540 F.2d 932, 935 (8th Cir. 1976).

[152] *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (Hand, L., J.) (weighing the costs of injury against the burden of preventing such injury). The State of Washington provides a statutory cause of action using this standard:

> A product is not reasonably safe as designed, if, at the time of manufacture, the likelihood that the product would cause the claimant's harm or similar harms, and the seriousness of those harms, outweighed the burden on the manufacturer to design a product that would have prevented those harms and the adverse effect that an alternative design that was practical and feasible would have on the usefulness of the product . . . .

WASH. REV. CODE ANN. § 7.72.030(1)(a) (West 2019).

[153] *Raney*, 540 F.2d at 935.

cybercrime; and the aggregate cost of the corporation's cybersecurity infrastructure. These findings should be compared with what is typical in the relevant industry.[154] These factors would then be balanced against the number of people impacted by the breach and the type of information stolen. However, that the corporation followed the standards set forth by an insurer and/or met industry standards alone should not automatically release the corporation from liability as these merely represent compliance with custom.[155]

Where a corporation does not collect financial or personally identifiable information, it would be highly improbable that liability would attach as the severity of injury would be minimal.[156] Furthermore, where there is significant managerial oversight of data protection and exemplary cybersecurity mechanisms in place, courts would likewise be hesitant to impose liability because additional measures would be so costly as to tip the balance in favor of the corporation.

3. No Safe Harbor Provisions

However, Congress and courts should not find dispositive that a corporation met industry standards and insurance policy conditions alone. This would essentially represent compliance with custom and not necessarily reflect reasonable alternatives because it is possible that merely no enterprise in a particular industry adopted the latest advances in modern data security.[157] While some commentators advocate for a federal data breach statutory scheme which includes safe harbor provisions that grant immunity to corporations that follow particular standards or give timely notice to consumers after a breach, these

---

[154] What is typical in the relevant industry is the "reasonable alternative design," whereby the "design" is the security infrastructure and cyber hygiene practices. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (AM. LAW INST. 1998) (adopting a risk-utility analysis, with the additional requirement of an available "reasonable alternative design" that would have made the product safer).

[155] *See infra* Part II.A.3.

[156] Similarly, this would also be the case where only a handful of individuals were the victims of a corporate data breach.

[157] "Reasonable" is defined as "technologically feasible and practical" in the context of design defects. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) cmt. f.

exemptions from liability disincentivize strong cybersecurity.[158] Rather, corporations should continually update their security systems in light of advancing technology and increasingly sophisticated malware, and ultimately face liability where they failed to reasonably protect their consumers' sensitive information.

B. Analogue to Workers' Compensation Statutes and Asbestos Exposure Litigation

There are two classes of victims created after both exposure to asbestos and corporate data breaches—those suffering now and those likely to suffer in the future—which generate consideration when designing statutes to remedy injuries.[159] Given this parallel, Congress can look to workers' compensation statutes and litigation dealing with asbestos exposure in order to structure data breach statutes. Some overlaps include the parties involved, preemption, statutes of limitation, and damages.

In *Norfolk & Western Railway Co. v. Ayers*, the Supreme Court addressed whether or not workers injured by asbestos could receive compensation under the Federal Employers Liability Act (FELA) for the existent fear of potentially developing cancer.[160] Answering in the affirmative, the Court recognized the anguish felt during the quiescent period after exposure is worthy of compensation when coupled with an asbestos-related injury.[161] For victims of corporate data breaches, those that have yet to suffer from fraud, identity theft, or financial account takeover have still experienced an injury—information theft—and will forevermore be susceptible to involuntary and illegal uses of their data.

The Seventh Circuit in *Remijas* also recognized this dichotomy and held that consumers impacted by a corporate data breach did not have to wait until "the threatened harm [materialized]" because the causal connection between a data breach and a subsequent injury would

---

[158] Sales, *supra* note 60, at 1557.

[159] *See supra* notes 39–42 and accompanying text.

[160] 538 U.S. 135, 141 (2003).

[161] *Id.* at 149, 153 (stating "[p]hysically injured plaintiffs, it is now recognized, may recover for 'reasonable fears' of a future disease" and rejecting the Government's argument that plaintiffs should only recover when they develop cancer because the fear of cancer itself is a cognizable injury).

be too attenuated to establish liability.[162] Given the anxiety and potential for harm caused by a cybersecurity attack, and the decreased likelihood of victims prevailing in court if forced to wait until injury is realized, Congress should take the Supreme Court and Seventh Circuit's lead and create a statutory provision that permits litigation to commence immediately after a cybersecurity attack.[163]

Several state workers' compensation statutes and FELA provide guidance on other relevant statutory features. For example, FELA bars an employer from asserting a contractual exculpation clause as a defense against liability.[164] This is particularly applicable to corporate data breaches because consumers are seldom in a position to negotiate the terms of contracts, especially clickwrap or browsewrap agreements.[165]

Under Illinois law, an injured worker's last employer will be the one liable for the contraction of an occupational disease so long as the employee was exposed for at least sixty days.[166] If a consumer is the victim of multiple data breaches and has experienced fraud, Congress may mandate that the corporation that most recently revealed a breach be liable for financial losses.[167] The statute of limitations for consumers to bring a data breach claim may be short, similar to most workers' compensation statutes, in order for corporations and insurers

---

[162] 794 F.3d at 693.

[163] *See infra* Part III.A.1.

[164] 45 U.S.C. § 55 (2018) (voiding "any contract, rule, regulation, or device whatsoever, the purpose or intent of which shall be to enable any common carrier to exempt itself from any liability created by this chapter" except insurance indemnity agreements).

[165] *See generally* Kaustuv M. Das, *Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the 'Reasonably Communicated' Test*, 77 WASH. L. REV. 481, 482 (2002) (defining "clickwrap" as a pop-up window on a website that requires a consumer to click "I AGREE" or "I ACCEPT" to specified terms in order to proceed, and "browsewrap" as a contractual agreement hidden in a hyperlink on a website).

[166] 820 ILL. COMP. STAT. ANN. 310/1.

[167] However, corporations may strategically choose to disclose when their breaches occurred if there is such a temporal element to liability.

to anticipate litigation and accurately account for losses.[168] However, statutes of repose for products liability claims were implemented because manufacturers are held strictly liable, but if corporations were ever to face liability for the defective design of their infrastructures, this would likely be akin to a negligence regime.[169] North Carolina law expressly excludes all other "rights and remedies of the employee . . . against the employer at common law or otherwise on account of such injury or death;" Congress could borrow this or similar language to preempt state statutory claims against corporations that experience cyberattacks.[170]

Though the injury for information theft differs significantly from the bodily harm suffered by victims of silicosis, asbestosis, and mesothelioma, Congress could look to state statutes that limit damages, such as Pennsylvania and Nevada for example, at $12,750 and $14,250, respectively.[171] However, damages for asbestos injuries are paid out from a single fund if claimants forgo litigation, whereas victims of data breaches would either litigate or receive settlements directly from the offending enterprise or its insurer.[172] Rather, damages for consumers impacted by a corporate data breach should similarly be capped but awarded based on a schedule categorized by the type of information collected.[173]

---

[168] *See, e.g.*, NEV. REV. STAT. ANN. § 617.460 (West 2019) (mandating that "claims for compensation on account of silicosis or a disease related to asbestos are forever barred unless application is made to the insurer within 1 year after the date of disability or death and within 1 year after the claimant knew or should have known of the relationship between the disease and the employment").

[169] *See generally* J. Alex Bruggenschmidt, *Asbestos for the Rest of Us: The Continued Viability of Statutes of Repose in Product Liability*, 76 DEF. COUNS. J. 54, 56–57 (2009) (discussing the origins of statutes of repose in products liability).

[170] *See, e.g.*, N.C. GEN. STAT. ANN. § 97-10.1 (West). While some state statutes may be stricter, Congress might prefer to preempt them in an attempt to control damages and encourage cybersecurity insurers to enter the market.

[171] 77 PA. STAT. ANN. § 1401 (West); NEV. REV. STAT. ANN. § 617.460 (West).

[172] Lester Brickman, *The Asbestos Litigation Crisis: Is There A Need for an Administrative Alternative?*, 13 CARDOZO L. REV. 1819, 1833–34 (1992) (estimating that the asbestos compensation fund pooled between seven and nine billion dollars).

[173] For example, a damages award for only stolen names should be less than one for social security numbers.

C. Routinization and Efficiency in Claim Settlement Similar to Automobile Insurance Coverage

Another analogue to victim compensation for data breaches can be found in the automobile industry. Once thought of as a luxury item, the automobile led to unprecedented carnage as it became a common fixture in American life.[174] The substantial number of vehicular injuries and fatalities throughout the early twentieth century eventually fostered the demand for victim compensation, which gave way to the rise of automobile insurance.[175] Now a standard aspect of vehicle ownership, automobile liability insurance provides a claims settlement process whereby victims are compensated in a routinized manner, detached from the courts.[176] Importantly, this type of insurance is not utilized to safeguard the assets of the driver, but compensate victims.[177]

Similarly, although the first computer was invented during the mid-twentieth century, the Internet would not reach the general public until the mid-1990s.[178] Now, just as with the rise of the automobile, there is unprecedented harm inflicted by Internet-based cyberattacks.[179] This year alone, there have been over six billion

---

[174] *See generally* Jonathan Simon, *Driving Governmentality: Automobile Accidents, Insurance, and the Challenge to Social Order in the Inter-War* Years, 1919 to 1941, 4 CONN. INS. L.J. 521, 530, 541 (1998) (estimating that automobile accidents accounted for twenty-nine percent of all accidental deaths in 1929).

[175] *See generally* Samuel Issacharoff & John Fabian Witt, *The Inevitability of Aggregate Settlement: An Institutional Account of American Tort Law*, 57 VAND. L. REV. 1571, 1603–04 (2004) (finding that by the mid-1930s, a majority of states began mandating that drivers purchase car insurance or demonstrate sufficient financial means to compensate victims should an accident occur).

[176] *See* Christopher J. Robinette, *Two Roads Diverge for Civil Recourse Theory,* 88 IND. L.J. 543, 550–62 (2013) (discussing the routinization of automobile accident claims).

[177] Wheeler v. O'Connell, 9 N.E.2d 544, 546 (Mass. 1937) (stating "[t]he purpose of the compulsory motor vehicle insurance law is not, like ordinary insurance, to protect the owner or operator alone from loss, but rather is to provide compensation to persons injured through the operation of the automobile insured by the owner.").

[178] *See* Paula M. Yost et al., *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Computer Data*, 54 SMU L. REV. 2055, 2058–59 (2001) (estimating that over 259 million people were using the Internet by the twenty-first century).

[179] *See supra* Part I.A.

records exposed from data breaches.[180] The Equifax breach impacted nearly half of the United States' population, and as data breaches continue to grow in magnitude, the demand for victim compensation will also mount.[181]

If cyber liability insurance were to become widely adopted like automobile insurance, consumers could be compensated with the same efficiency and routinization provided to automobile accident victims. At present, cyber insurance provides mostly first-party coverage, but if Congress enacted a private right of action for consumers, third-party policies would become commonplace.[182] Given the frequency with which data breaches occur, insurance companies would likely settle claims with the same standardized process as automobile insurance in order to meet the insistence for victim recovery while simultaneously mitigating the costs associated with litigation.

V. CONCLUSION

As corporate data breaches become the norm, and consumers' personally identifiable information compromised, victims are left with losses that cannot be litigated due to a Circuit split on standing and the futility of bringing common law tort claims.[183] Absent a comprehensive federal statutory scheme to hold enterprises accountable, a majority of state statutory claims do not provide a useful private right of action.[184] Shareholders are unable to hold corporate insiders responsible for poor data protection, and the banking industry ultimately bears the burden compensating consumer fraud losses.[185] Although corporations incur several million dollars in losses following a single data breach, these expenses often prove to be less costly than the substantial investment required to implement preventative cybersecurity measures.[186]

---

[180] *Data Breaches*, PRIVACY RTS. CLEARINGHOUSE (last visited July 1, 2019), https://www.privacyrights.org/data-breaches (narrowing the search by selecting "2019" under the "Select Year(s)" column).

[181] Bernard & Cowley, *supra* note 50.

[182] *See supra* notes 88–98, and accompanying text.

[183] *See supra* Part I.B. and I.C.

[184] *See supra* notes 43–47, and accompanying text.

[185] *See supra* notes 55–58, and Part I.D., and accompanying text.

[186] *See supra* Parts I.A. and I.D., and accompanying text.

However, these disincentives to protect consumer data can be realigned with the widespread adoption of cyber liability insurance.[187] Enterprises would improve their cybersecurity infrastructures prior to purchasing a policy because the price of coverage would depend on the underwriting inspection of their system.[188] Once a policy is in place, stringent conditions of coverage that required maintenance of a robust cybersecurity infrastructure would also likely be followed to prevent cyberattacks and potential litigation.[189] If best practices and industry standards are not followed, a corporation would risk invalidating their policy and becoming liable for the sum total of losses in the event of a data breach.[190]

But in order to hold corporations fully accountable for failing to safeguard the sensitive information they collect, Congress must also enact a private right of action that allows consumers to seek redress in the immediate aftermath of a data breach.[191] Lawsuits for data breaches should be adjudicated under a standard resembling the model adopted for design defects in the Restatement (Third) of Torts.[192] By applying a risk-utility test and asking whether a corporation could have adopted reasonable, alternative security measures to better protect consumers, victims would be compensated for their negligent protection of data and corporations could avoid liability by demonstrating that sufficient cybersecurity measures were put in place.[193]

Such a scheme should also include a low damages cap because: (1) some victims may never suffer financial losses; (2) banks will most likely cover any financial losses; and (3) corporations are themselves victims as well.[194] That said, as the analogue to workers' compensation for asbestos exposure instructs, the apprehension of being victimized one day by a data breach, or resulting identify theft or fraud, is just as much an actual injury as monetary losses.[195]

---

[187] *See supra* Part II.A.
[188] *See supra* notes 103–104, and accompanying text.
[189] *See supra* Part II.A.
[190] *See id.*
[191] *See supra* Part III.
[192] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (AM. LAW INST. 1998).
[193] *See supra* Part III.A.2.
[194] *See supra* Part III.A.1.
[195] *See supra* Part III.B.

Lastly, there is a parallel between the advent of automobiles and the unprecedented carnage they wrought, and the advent of the Internet and the unprecedented rise in information theft. In both instances, the technological innovations created the demand for victim compensation that was previously unattainable.[196] For accident victims, this led to the widespread adoption of automobile liability insurance and a routinized claims settlement process.[197] It is possible that cyber liability insurance can answer the call for victim compensation of corporate data breaches, and may even lead to a similar standardized claim and settlement process if widely adopted.[198]

Corporations are failing to prioritize data security at the expense of consumers, who are currently without recourse. State and federal law currently fails to provide protection, and neither the banking industry nor corporate shareholders are able to hold corporations accountable for their negligent data protection. However, cyber liability insurance can step in and serve as an external gatekeeping role that forces policyholders to prioritize data protection and to act preemptively in preventing cyberattacks. Whereas, a private right of action would equip consumers with an added force to deter negligent data protection and provide the victims of data breaches with recourse for their losses.

---

[196] *See supra* Part III.C.
[197] *Id.*
[198] *Id.*