Insuring Against the Inevitable: The Promises and Pitfalls of Cyber Insurance

Alyssa Julia Picard

Table of Contents

Introduction ....................................................................................................................................2

I. Hacking, Data Breaches, and Other “Cyber Risks” Represent a Significant Source of First- and Third-Party Liability ...........................................................................................4

   A. Consumer Class Actions ........................................................................................................8

   a. Tort Claims ...........................................................................................................................8

   b. Contract Claims ................................................................................................................10

   c. Statutory Claims .................................................................................................................11

   d. Common Issues: Theories of Harm .....................................................................................12

   B. Securities Fraud Class Actions ............................................................................................15

   C. Federal Regulatory Actions ..................................................................................................16

II. Companies Have Been Generally Unsuccessful in Obtaining Coverage for Cyber Risks Through Their Commercial General Liability Insurance Policies ........................................20

III. Cyber Insurance Has Developed as a New Product to Cover Third-Party Liability Arising Out of Cyber Risks ....................................................................................................22

IV. Cyber Insurance Raises Particular Issues Concerning Its Viability Not Found to the Same Extent in Traditional Lines of Insurance ...............................................................................23

   A. Difficulties in Valuation .....................................................................................................23

   B. Correlated Risks and Enormous Losses ............................................................................24

   C. Barriers to Cyber Insurance Providing Effective Regulatory Governance ....................25

   D. Risk of Moral Hazard .........................................................................................................28

V. Cyber Insurance Merits More Critical Study Than It Has Attracted to Date, and Questions of Intervention and Regulation Should Not Be Considered in a Vacuum. ..........................30

Conclusion ....................................................................................................................................32
Introduction

For several years now, cybersecurity and its failures have never been far from the forefront of the global consciousness. Data breaches exposing the personal information of millions of individuals have struck both government agencies and private companies, while Russian cyberattacks have been blamed for interference in the American electoral process. And these are only three incidents out of countless representative examples from the past three years alone.

Failures of cybersecurity can be debilitating to national security and feelings of personal privacy, of course, but they come with a calculable price tag as well. To take one extreme example, the most expensive data breach on record struck Equifax in 2017 and has cost the company $1.35 billion so far, with costs still mounting.

Given the potential costs of failures in cybersecurity, it comes as no surprise that organizations would seek to insure against these risks and that recently a new “cyber insurance” market has sprung up to meet the demand. This paper will provide an overview of the potential liabilities a company faces following a data breach and discuss how this new insurance product works in response.

Although the cyber insurance market is rapidly expanding, to date there has been relatively little scholarship approaching it from a legal perspective. Many of the serious studies have been primarily descriptive in nature, usually providing an in-depth market survey of the cyber insurance sector. This paper draws on that work but makes no attempt to perform a similar market survey. Given the rapid evolution of this market, such an exercise would have only short-lived utility, and would merely duplicate the valuable research others have conducted in this space. Outside of these descriptive studies, the little that has been written on cyber insurance has tended to be published in bar journals, the popular press, or in blog posts. On the whole, these writings paint the product in a

---

positive light or even present it as a panacea. Every company faces the risk of serious cyber liability; this new insurance product is designed to help mitigate that risk; therefore every company should obtain cyber insurance coverage—or so the logic runs. Only a small handful of scholars have given the subject a more academic treatment.

In light of its rapid growth, it is clear that cyber liability insurance will be an important subject in insurance law and policy in the years to come. But the success or failure of the cyber insurance market and the ways the insurance product develops is worth the attention of those beyond insurance scholars and professionals or technology policy wonks.

Insurance—of all sorts—is pervasive in our society, and its effects run deep. The structure of a particular insurance policy profoundly affects the insured party’s incentives to act a certain way, insurance’s widespread availability facilitates negotiation and contracting between parties, an insurance company operating within a particular sector can serve as both a repository of expert knowledge of best practices and a de facto regulator of the industry, and the list could easily go on. Indeed, many have looked at insurance’s far-reaching impact and recognized that addressing insurance is one way to address the many disparate threats, harms, and policy issues we find in our world. Insurance impacts everything.
And so, in turn, does cybersecurity. Anyone who thinks about national security, economic stability, public health, technological innovation, or personal privacy is in all likelihood already aware of how cybersecurity and its failures touch all of our lives. As such, we cannot afford to overlook insurance as a central factor in how cybersecurity develops and responds to challenges. In short, the emergence of cyber liability insurance is not a niche or technical topic that can safely be ignored.

This paper attempts to move the conversation on cyber insurance forward. It offers a more critical assessment of cyber insurance’s viability as an insurance product and cybersecurity measure than what has previously been put forward, and compares it to other traditional lines of insurance.

Part I will outline the nature and extent of the liabilities stemming from data breaches and other “cyber risks,” as well as the legal issues commonly confronted in litigation over the third-party liabilities in particular. Part II will discuss the failures of the “traditional” insurance market to cover these liabilities, and Part III will then introduce the new cyber insurance market that has developed to address these risks. Part IV will explore some of the unique features of cyber insurance as compared to more traditional lines of insurance, and discuss how these may pose problems for its continued growth or effectiveness as a cybersecurity measure. Finally, Part V offers suggestions for how the cyber insurance sector and the discourse around it should evolve in light of these issues.

I. Hacking, Data Breaches, and Other “Cyber Risks” Represent a Significant Source of First- and Third-Party Liability

“Cyber risks” generally include “any loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality.” The most prevalent cyber risk

today (as one commentator puts it, “cyber risk’s poster child”\textsuperscript{17}) is the data breach, which usually involves stolen “personally identifiable information” about employees or customers, including payment card information, social security numbers, or medical records.\textsuperscript{18} For corporations, data breaches can also involve disclosures of sensitive or confidential information, including client records, trade secrets, financial records, or litigation information.\textsuperscript{19} Data breaches could be caused by a malicious or criminal attack (e.g., hacking, phishing, or distributing malware), a system glitch, or simple human error.\textsuperscript{20}

The Privacy Rights Clearinghouse reports that 8,073 data breaches were publicly announced between 2005 and April 2018, which resulted in the disclosure of at least 10,276,848,439 individual records.\textsuperscript{21}

Some of the more high-profile among these breaches struck large U.S. companies: a hack on Target Corporation in 2013 stole information on 40 million payment-card accounts and personally identifiable information of up to 70 million customers, costing the company $248 million by the end of 2014;\textsuperscript{22} Home Depot’s hack in 2014 revealed the information on 56 million payment-cards, costing it $43 million;\textsuperscript{23} the 2014 hack against Sony Pictures Entertainment cost it at least $15 million.\textsuperscript{24} The total cost of Equifax’s 2017 data breach has yet to be fully determined, but the credit reporting bureau’s most recently announced quarterly report (for the quarter ending March 31, 2019) recorded its total losses from the breach so far as $1.35 billion.\textsuperscript{25} A full year previously, with total costs only a fraction of what they are today, the chair of the Ponemon Institute felt comfortable deeming this “the most expensive breach in history.”\textsuperscript{26}

\textsuperscript{18} Podolak, \textit{supra} note 16.
\textsuperscript{19} \textit{Id.}
\textsuperscript{20} A combination thereof can also be extremely effective; “hacking humans” is an easy way to infiltrate a computer network. See, e.g., Matthew Tischer et al., \textit{Users Really Do Plug in USB Drives They Find}, in \textit{PROC. 2016 IEEE SYMP. ON SEC. AND PRIVACY}, 306 (finding that nearly half of individuals taking part in the study plugged a USB drive they found in the parking lot into their work computes). See generally \textit{THE HUMAN FACTOR} (Proofpoint ed., 2017) (providing statistics on the efficacy of targeting human users).
\textsuperscript{23} \textit{Id.} at 7.
\textsuperscript{25} Schwartz, \textit{supra} note 4.
Although media coverage naturally focuses on the most high-profile targets and largest-scale hacks, small- and mid-sized companies also suffer from data breaches that can be devastating to their businesses.27 As former Federal Bureau of Investigation Director Robert Mueller has claimed, “there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”28

A data breach brings with it both first- and third-party liabilities.29 Other, more established lines of insurance in other sectors have addressed both. Insurance for first-party liabilities provides coverage for losses and damages sustained by the insured.30 For example, when an insured’s home is damaged in a fire, she has sustained a first-party loss, and her fire insurance provider is obligated to pay benefits directly to her. Common examples of first-party insurance policies include life, disability, health, fire, theft, and casualty insurance.31 In contrast, an insurance policy for third-party liability provides coverage for the liability of the insured to another party.32 That third party makes a claim against the insured, and the insured seeks coverage from the insurer to indemnify the insured against liability to the third party, and often to defend lawsuits brought by the third party against the insured.33 For example, plaintiffs may sue a company seeking damages for bodily injury and property damage allegedly resulting from the company’s disposal of toxic waste, and that company may seek coverage for those damages under its comprehensive general liability policy.34 Common third-party liability policies include comprehensive general liability, directors’ and officers’ liability, and errors and omissions insurance.35 Some lines of insurance include coverage for both types of liability. For example, when an insured crashes her car, a typical automobile insurance policy will cover first-party liabilities like the damage to the insured’s car and the insured’s own medical costs, and will also cover third-party liabilities like the damages sought by third parties who claim they were injured by the insured’s driving.

Much like a car crash, a data breach usually means there are both first- and third-party liabilities at issue.

corporate-history-idUSKCN1GE257.

27 4 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 29.01 (2017).
29 THOMAS, supra note 27.
30 2 WITKIN, SUMMARY 11TH INSURANCE § 114(1) (2019).
32 WITKIN, supra note 30, at § 114(2).
33 Id.
35 39A CAL. JUR. 3D INSURANCE CONTRACTS § 450 (2019)
In the cybersecurity context, first-party liabilities are suffered directly by the organization affected by the cyber risk event. They include the costs of detecting and containing a data breach; the costs of replacing or repairing compromised hardware or software; lost sales and productivity in the time it takes to restore a system to normal function or restore necessary data; and the post-breach costs of investigation, assessment, audit services, and communication to executive management and the board of directors. Compliance with regulation (for example, requirements to notify customers) also entails substantial first-party liability for a company. This is especially true in the United States, where the average cost of regulatory compliance activities post-breach was $0.69 million. These costs include the creation of contact databases, the determination of all regulatory requirements, the engagement of outside experts, postal expenditures, email bounce-backs, and inbound communication setups.

But the direct costs to a company are only part of the story. When a data breach exposes information about employees or customers, it can result in third-party liability as well. When these parties sue, an affected company may be liable to pay them damages stemming from its cybersecurity failures.

Third-party liability arising from data breaches sits in a complex and evolving legal landscape. Depending on the circumstances of the breach, shareholders, customers, and employees may claim they have suffered some form of personal or business loss—but given the relative novelty of this type of harm, there is no coherent body of law setting forth the legal duty of care or the bases for civil liability following cybersecurity failures. In data breach litigation, plaintiffs try to shoehorn their claims into existing tort, contractual, and statutory theories of liability with varying levels of success. Despite the legal uncertainty, though, plaintiffs have filed and in all likelihood will continue to file hundreds of post-data breach lawsuits.

38 PONEMON, supra note 36, at 5.
39 Id.
41 Id. at 31.
42 See Sasha Romanosky et al., Empirical Analysis of Data Breach Litigation, 11 J. EMPIRICAL LEGAL STUD. 74, 93 (2014) (noting that from 2000 to 2011 there were 231 federal lawsuits filed over data breaches).
The resulting third-party liabilities generally fall into three categories.

A. Consumer Class Actions

The first is the most varied. Consumers whose personal information has been compromised in a company’s data breach may bring (very often in an attempted class action) a variety of common law and statutory causes of action. These include negligence, invasion of privacy, breach of fiduciary duty, and assertions of the violation of state unfair and deceptive commercial acts and practice statutes (UDAP laws), state data security laws, and federal laws like the Stored Communications Act (SCA) and the Fair Credit Reporting Act (FCRA). This is far from an inclusive list—a study of 230 data breach lawsuits between 2004 and 2014 found that plaintiffs brought more than eighty-six different causes of action.44

Given their potential scale, consumer class actions have the potential to be extraordinarily costly for affected companies. Equifax, for example, was facing more than 240 lawsuits seeking class action status just two months after its breach was announced,45 while Target’s hack resulted in over 140 lawsuits.46 Equifax recently settled most of these claims (along with state and federal investigations) for a total of about $650 million, the largest-ever data breach settlement so far.47

A few of the most common causes of action, along with the legal issues most often raised in their litigation, will be canvassed here.

a. Tort Claims

Many potential third-party liabilities surrounding cyber risks are based in tort.

For instance, data breaches frequently give rise to class actions for common law negligence.48 The theory in such a case is that the affected company unreasonably failed to maintain adequate security and protect consumers’ data from third-party access.

The crucial question becomes whether the corporate defendant had a threshold duty to protect consumers’ personal information at all. Some courts will resolve this question quickly in the

44 Romanosky, supra note 42, at 102.
48 Jordan Elias, Course Correction—Data Breach as Invasion of Privacy, 69 BAYLOR L. REV. 574, 576 (2017) (“[I]t was the negligence tort that dominated the early years of data breach litigation.”); Hooker, supra note 40, at 34.
negative. Others, though, have been willing to find applicable duties of care to consumers in the
cybersecurity realm. In the wake of Target's hack, a federal court in Minnesota noted that plaintiffs
bringing a class action suit had “plausibly alleged” two different duties to support their negligence
claims. First, Target had a duty to exercise reasonable care in “obtaining, retaining, securing,
safeguarding, deleting and protecting [plaintiffs’] personal and financial information in its
protection,” and second, Target had a duty to “timely and accurately disclose” that plaintiffs’
information had been compromised. Target subsequently reached a $19 million settlement with
MasterCard and a $10 million settlement with the impacted customers.

Assuming the duty question is resolved in plaintiffs’ favor, tort suits sounding in negligence
will also have to survive the economic loss rule, which provides that, absent physical injury of
damage to property, there can be no tort recovery for negligent conduct that causes purely financial
losses. Following a data breach, consumers may seek damages for expenses like credit monitoring
services, transactional costs in obtaining new credit cards or bank accounts, or the lost time-value of
money as they wait for their bank to reimburse them following identity theft. If these injuries stand
alone, in some states consumers may be unable to mount a tort suit based on the company’s
negligence.

Consumers may also try to bring tort claims for invasion of privacy. While this seems in
many ways fitting and conceptually appealing—after all, the interest that consumers are really trying
to protect here is the right to keep their information private—none of the existing privacy torts
offer a good fit for data breaches. The tort of public disclosure of private facts, for example,
contains as a required element that the defendant published the plaintiff’s private information. But
in a data breach situation, the defendant has usually failed to secure the plaintiff’s information,

---

Ga. Feb. 5, 2013) (“[N]o duty of care exists in the data breach context where, as here, there is no direct
relationship between the plaintiff and the defendant.”).


51 Id. at 1171.

52 Allison Grande, Target Strikes $19M Deal with MasterCard over Data Breach, LAW360 (Apr. 15, 2015),


54 The situation is, of course, more nuanced than this brief treatment lets on. Much depends on how the
particular governing state law interprets the economic loss rule and on how it defines the rule’s various
exceptions. For a full discussion of the rule’s operation in the cybersecurity realm, see generally Catherine

55 See generally Elias, supra note 48, at 576-77 (arguing that “courts should embrace invasion of privacy
principles” in data breach cases).

56 See, e.g., id. at 575 (“[T]he dominant harm from data breaches lies not in low-level fraud but in the loss of
private facts themselves and consequent damage of an intangible nature: anxiety, embarrassment, and
distress.”); see also Solove, supra note 43, at 746 (arguing that “anxiety over the loss of personal data (such as
a Social Security number and financial information) should be treated as a privacy harm akin to the
emotional distress caused by the publication of “a nude photo or sex video of a person without consent”).
leaving it vulnerable to theft—but has not itself engaged in the required publication. Similarly, a
claim for intrusion would be inapt against a company that had suffered a data breach—the
defendant in these cases may have failed to protect against access to the plaintiff’s personal
information, but the tort charges that the defendant itself improperly accessed such information. 57

A final privacy tort, though, has seen some application in cases of “informational
trafficking.” 58 A cause of action for appropriation of name or likeness would not find much
purchase in a traditional hacking or data breach situation. But under certain circumstances—where a
corporate defendant has sold private information to third-party advertisers or otherwise
appropriated the information for its own commercial use—this tort can offer plaintiffs a path to
recovery. 59 The Northern District of California, especially, has been host to several data misuse cases
in which the plaintiffs have attempted to bring this cause of action. 60 It has seen at least one notable
success. In Fraley v. Facebook, Inc., the plaintiffs alleged that Facebook had misused their personal
information, namely their names and likenesses obtained from their Facebook accounts, in paid
advertisements without their consent. 61 The court held that the plaintiffs had sufficiently alleged
injury in order to state a claim for misappropriation under the applicable right of publicity statute, 62
and the case later settled. 63 Such a claim is of limited application, of course, but nonetheless has
proven to be a source of third-party liability for a very specific type of cyber risk.

b. Contract Claims

Alternatively or in addition, plaintiffs may try to recover based on contract theories.
Plaintiffs will allege that the defendant company made a contractual promise to protect their
personal information and breached that obligation by failing to prevent the exposure of that
information. The breach may be one of an express contract. For example, members of health care
plans administered by AvMed brought a breach of contract claim after their information was stolen
from unencrypted laptops in the AvMed office; they based the claim on a service agreement
requiring the company to ensure the confidentiality of their medical information. 64 But even in the
absence of any express promise, affected consumers may still be able to bring a claim for breach of

57 See Robert L. Rabin, Perspectives on Privacy, Data Security and Tort Law, 66 DePaul L. Rev. 313, 326 (“Here,
the self-evident problem is one of the misplaced defendant.”); see also Steinberg v. CVS Caremark Corp.,
899 F. Supp. 2d 331 (E.D. Pa. 2012) (“[L]iability for intrusion upon seclusion cannot exist where a
defendant legitimately obtains information from a plaintiff. . . . This is so even where those facts voluntarily
offered are later disclosed to a third party . . . .” (citations omitted)).
58 Rabin, supra note 57, at 327.
59 Id.
60 See, e.g., Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190 (N.D. Cal. 2014); C.M.D. v. Facebook, Inc., No. C
62 Id. at 810.
63 Rabin, supra note 57, at 327.
implied contract. As the First Circuit has explained,

Under Maine law, a “contract includes not only the promises set forth in express words, but, in addition, all such implied provisions as are indispensable to effectuate the intention of the parties” . . . . When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.65

Claims based on equitable theories like unjust enrichment often accompany the breach of contract allegations. In the AvMed lawsuit, the plaintiffs’ unjust enrichment claim survived a motion to dismiss alongside their explicit contract claim. They had alleged that part of the monthly premiums they paid to AvMed were used to pay for data security and that AvMed was unjustly enriched because it did not maintain adequate data-security standards.66 Plaintiffs in the Target lawsuit were not able to use a similar “overcharge” argument, but were able to base their unjust enrichment claim on a different theory: If plaintiffs shopped at Target after Target knew about its breach, but would not have shopped there if they had been informed of the breach, “a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target ‘in equity and good conscience’ should not have received.”67 Under certain circumstances, either an “overcharge” theory or a “would not have shopped” theory can support a claim for unjust enrichment.

c. Statutory Claims

Finally, consumers may supplement their common law claims with statutory ones. Some states have passed legislation meant specifically for this purpose. As mentioned in the discussion of first-party liabilities supra, all states now have some form of a data breach notification law.68 A few of these states allow for a private cause of action upon their statute’s violation.69

Plaintiffs have also tried to find private causes of action over data breaches under more general federal statutes, though the obstacle there tends to be that these laws have specific requirements for their applicability. For example, plaintiffs may allege that the company’s data breach violated the SCA, which prohibits an entity that provides an electronic communication service or remote computing service to the public from divulging the contents of the communications it stores.70 The plaintiffs in In re Michaels Stores Pin Pad Litigation alleged such a

66 Resnick, 693 F.3d at 1328.
68 See supra note 37.
violation after their financial information was stolen from the craft store Michaels. However, the court dismissed that claim after concluding that Michaels provided neither service that would bring it within the ambit of the statute. Similarly, data breach claims brought under the FCRA are often dismissed because most defendants cannot be called “consumer reporting agencies” under the terms of the statute.

d. Common Issues: Theories of Harm

Despite the many potentially applicable causes of action in the data breach context, many of these consumer class actions fall down on the issue of defining the harm suffered. This can be framed as a problem of Article III standing if the case proceeds in federal court: following a data breach at a company that was storing their personal data, have the consumers suffered an injury-in-fact? Or, it may be a matter of whether damages for the injury are recoverable under the chosen tort, contract, or other theory in the case: for example, even if a company was negligent, did the consumers suffer merely economic harm? These are distinct legal issues, but the underlying facts in the cyber risk context that throw up these hurdles are similar.

One commonly advanced theory of harm is that plaintiffs’ risk of future harm, such as the risk that their identity will be stolen, has increased after the data breach exposed their information. This may be more than an abstract fear. In cases like In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation, plaintiffs may be able to quantify that risk—there, they alleged that they were ten times as likely to be victims of identity theft following the breach. In analyzing whether this is sufficient for standing or for the substantive causes of action, courts have emphasized different factors and have split along several axes. In Khan v. Children’s National Health System, the court did an admirable job of summarizing the results of this “frequently litigated” issue in the other circuits and attempting to find unifying principles. The court reasoned that although

71 830 F. Supp. 2d 518, 522 (N.D. Ill. 2011).
72 Id. at 524.
74 See Solove, supra note 43, at 743-44 (“In data-breach cases, the nature of the injury has seemingly befuddled the courts. . . . To many judges and policymakers, recognizing data-breach harms is akin to attempting to tap dance on quicksand, with the safest approach being to retreat to the safety of the most traditional notions of harm.”).
76 Compare Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010) (holding that plaintiffs whose names, addresses, and Social Security numbers were stolen suffered an injury-in-fact based on increased risk of identity theft, even though only one plaintiff alleged his Social Security number had been misused) with Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (holding that plaintiffs alleging an injury-in-fact from an increased risk of identity theft lacked standing).
previous courts’ decisions on the subject seem to be all over the map, there was not necessarily a circuit split.78 Rather, “the difference appears to arise not from the application of a different legal standard, but rather from crucial distinctions in the underlying facts.”79 Thus, the Khan court concluded:

[I]n the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs’ personal data to engage in identity fraud.80

However, near as this formulation may be, it is too early to tell whether it will be widely accepted by other courts.81

Another type of injury often alleged concerns the out-of-pocket costs plaintiffs incur (in time and money) to mitigate their risk of identifying theft or fraud after they are notified their information has been exposed.82 For example, they may need to freeze their credit score, subscribe to identity-theft protection services, get new credit cards, or more. Whether or not this is enough often rises and falls with courts’ treatment of the first theory of harm. If the court rejects the risk-of-future-injury theory, they are likely to reject these preventative measures as equally inadequate harms, viewing these expenses as plaintiffs’ attempts to “manufacture” injury.83 The same courts that tend to allow for increased-risk theories, though, may also look favorably upon these out-of-


79 Khan, 188 F. Supp. 3d at 530.

80 Id. at 531.


82 Solove, supra note 43, at 752.

83 See, e.g., Clapper v. Amnesty Int’l USA, 568 U.S. 398, 422 (2013) (“We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm.”); Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (rejecting the “claim that plaintiffs incurred expenses in anticipation of future harm” as insufficient for standing purposes after concluding that the increased-risk theory was also insufficient).
pocket losses. In *Dieffenbach v. Barnes & Noble, Inc.*, for example, the Seventh Circuit explained:

> The plaintiffs have standing because the data theft may have led them to pay money for credit-monitoring services, because unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value of one’s own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries can justify money damages, just as they support standing.\(^84\)

Even in a court that looks favorably on this type of harm, however, if these injuries stand alone the economic loss rule may still pose a problem for allegations of negligence, as discussed *supra*.

Finally, plaintiffs may proceed with an emotional distress-type theory of harm. They may claim, for instance, that they suffer from anxiety, fear, or embarrassment now that the company has exposed their personal information. These types of claims tend to fare especially badly. Only a few causes of action will allow recovery for emotional distress standing alone. The privacy torts, for instance, do allow recovery for pure emotional distress, but successful privacy claims are difficult following a data breach.\(^85\) Claims brought under FCRA similarly may allow recovery for these injuries. Courts have held that the “actual damages” available under the statute\(^86\) include recovery for emotional distress.\(^87\) To bring a successful FCRA claim, though, plaintiffs must be sure to assert more than conclusory statements of emotional distress: “Mental pain and anxiety can constitute actual damages, . . . but emotional distress damages must be supported by competent evidence of ‘genuine injury,’ which ‘may be evidenced by one’s conduct and observed by others.’”\(^88\) And for most other types of claims, standalone emotional distress is an insufficient injury: “Courts across the country have rejected ‘emotional distress’ as a basis for standing” when plaintiffs fear that their exposed personal data will be used in a malicious way.\(^89\)

---

Despite the doctrinal hurdles and consumer class actions’ checkered record of success, these lawsuits still represent a major source of potential third-party liability for companies facing cyber risks.\(^90\) Moreover, given that the governing law contains so many splits, uncertainties, and open

---

84 887 F.3d 826, 828 (7th Cir. 2018).
85 See *supra* notes 55-63.
88 *Taylor*, 710 F.3d at 828 (citation omitted) (quoting Carey v. Piphus, 435 U.S. 247, 264 n.20 (1978)).
90 See *supra* notes 44-46.
questions, it is a source of liability that stands to remain a company’s (or its insurer’s) least favorite type: one of unpredictable scale.

**B. Securities Fraud Class Actions**

If a company’s data breach results in a diminution in its stock value, its shareholders may claim they relied to their detriment on the company’s material misrepresentations (for example, public statements concerning its cyberattack readiness or the nature or extent of a past breach) and bring a securities fraud class action suit.

The 2017 Equifax data breach has already given rise to one of these actions, which has recently survived a motion to dismiss. The value of Equifax’s stock fell 36% over the course of a week. Litigation is still ongoing, but at the pleading stage the plaintiffs adequately alleged that Equifax’s misrepresentations as to the personal information it collected, its vulnerability to cyberattacks, and its compliance with cybersecurity best practices “artificially inflated the value of Equifax’s securities, causing a loss in value of the class’s investments when the truth was revealed after the Data Breach.”

Of course, to bring this type of action following a data breach, the damages of the breach must manifest as a reduction in stock value. Courts may define this stringently: some that have considered the question have looked for a “statistically significant” decline in the company’s stock price, which may necessitate the use of expert witnesses and complex valuation models. As an additional wrinkle, the causation of the stock value reduction needs to be tied not to the data breach, but rather to the company’s misrepresentations themselves. This requirement alone will prevent this form of third-party liability from playing an appreciable role for many cyber risks.

Furthermore, establishing that company statements rise to the level of “material misrepresentations” in the technologically complex and constantly evolving cybersecurity context can be difficult for plaintiffs.

On this point, *In re Heartland Payment Systems, Inc. Securities Litigation* is instructive. That case arose out of a 2007 cyberattack on the payment processing company Heartland, which allowed the hackers to steal 130 million credit and debit card numbers stored on its computer networks over the course of 2008. After Heartland discovered and subsequently disclosed the breach in 2009, its

---

92 Id. at 1214.
93 Id. at 1205.
94 Hooker, supra note 40, at 34.
95 *Equifax*, 357 F. Supp. 3d at 1247.
97 Id. at *1.
stock declined nearly 80% in value. The plaintiffs pointed to many statements from the company touting their cybersecurity measures and general readiness for cyberattacks in earnings conference calls and in their 2007 Annual Report filed with the Securities and Exchange Commission after the attack took place. The court held that none of these statements, however, rose to the level of a material misrepresentation. Underlying this conclusion seemed to be the common-sense understanding that no computer system could be perfectly invulnerable and that all cyber risks cannot be perfectly anticipated:

The fact that a company has suffered a security breach does not demonstrate that the company did not “place significant emphasis on maintaining a high level of security” . . . [and] the fact that a company faces certain security problems does not of itself suggest that the company does not value data security.99

Under this standard, the mere fact that a breach occurred will not render statements about the high quality of a company’s cybersecurity materially false. Given that many cyberattacks will exploit previously-unknown vulnerabilities, this standard may save many companies’ statements about their cybersecurity measures from being actionable.

Finally, complaints that allege fraud under federal securities law—including fraud outside of the cyber risk context—need to contend with the heightened pleading requirements of both the Federal Rules of Civil Procedure’s Rule 9(b) and the Private Securities Litigation Reform Act of 1995.100 The former requires any complaint to “state with particularity the circumstances constituting fraud,”101 while the latter adds supplemental requirements to the misrepresentation and scienter elements of the claim, with the intent of “cur[ing] perceived abuses in prosecuting class actions brought pursuant to federal securities laws.”102 In line with this intent, these requirements make it easier for courts to dismiss claims at the pleadings stage.103

There have been relatively few data breach-related securities fraud actions, especially compared to the expansive litigation and varied legal theories in the consumer class action space. The general difficulty of bringing a securities fraud class action, together with the special challenges of mounting a successful data breach case, may explain why.

C. Federal Regulatory Actions

Finally, a company may also incur third-party liabilities to the government, as federal

---

98 Id.

99 Id. at *5 (citation omitted).

100 Equifax, 357 F. Supp. 3d at 1215.

101 FED. R. CIV. P. 9(b).


agencies can bring various types of enforcement actions in response to data breaches.

The Federal Trade Commission (FTC) finds their authority for such actions under § 5 of the Federal Trade Commission Act, under which they prosecute inadequate data security resulting in breaches as unfair and deceptive trade practices. In 2015, the Third Circuit affirmed in *FTC v. Wyndham Worldwide Corp.* that the agency does have its asserted power to regulate cybersecurity policies through § 5.

The Federal Communications Commission (FCC) has recently increased its own enforcement of private-sector data security practices. In 2015, the agency settled with AT&T for $25 million after employees of foreign-based call centers gained authorized access to customers’ names and personal information, which they then sold to third parties. In that settlement, the FCC justified its enforcement authority under the Communications Act: “The failure to reasonably secure customers’ proprietary information violates a carrier’s statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act.”

Finally, the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), and the U.S. Department of Health and Human Services (HHS) have brought enforcement actions over data security practices when such enforcement falls within their specific mandates.

The SEC has brought charges against public companies for their failure to properly protect the personal information of customers. The basis for these actions is often the violation of SEC’s “safeguards rule,” which requires registered brokers, dealers, investment companies, and investment advisers to adopt written policies and procedures to reasonably protect client records and information. In 2015, the agency settled with the investment advisor R.T. Jones for $75,000 after it “fail[ed] to adopt any written policies and procedures reasonably designed to safeguard its clients’ [personal information] as required by the Safeguards Rule.” More recently, the SEC reached a settlement with the entity formerly known as Yahoo! Inc., in which the company would pay a $35 million penalty for failing to disclose to investors a 2014 cyberattack that compromised personal

---

105 799 F.3d 236, 240 (3d Cir. 2015).
data associated with hundreds of millions of user accounts.\textsuperscript{111}

The Dodd-Frank Act gives the CFPB statutory authority to directly fine companies that violate its provisions governing unfair business practices, including those related to data security.\textsuperscript{112} In 2016, the CFPB brought an action under the Act against Dwolla, Inc., a digital payment company, for misrepresenting its data security practices and failing to adequately secure sensitive consumer personal information.\textsuperscript{113} That action resulted in a $100,000 penalty and an order to “implement reasonable and appropriate data-security measure to protect consumers’ personal information.”\textsuperscript{114}

HHS has the authority to enforce various federal laws, but the most relevant here is the Health Insurance Portability and Accountability Act (HIPAA). HHS mandates data breach notification rules pursuant to HIPAA,\textsuperscript{115} and also has brought enforcement actions over compliance with its regulations regarding the privacy and security of personal health records.\textsuperscript{116}

The incursion of these agencies into the cybersecurity realm is not without controversy.\textsuperscript{117} In part, this is because regulating cyber risks is not clearly within the mandate of any one agency, so the agencies involved are arguably stretching their authority to reach the conduct at issue, and may not be able to focus on the most relevant areas of industry conduct.\textsuperscript{118} In a similar vein, such fragmented regulatory authority in this area means that there is still no coordination or uniform standards for private-sector cybersecurity measures.\textsuperscript{119} Finally, because these administrative agencies tend to only regulate data breaches through individual enforcement actions, there remains substantial uncertainty among businesses as to the governing standards for cybersecurity and as to whether they will actually be subject to an enforcement action in any given instance.\textsuperscript{120}


\textsuperscript{112} Rabin, \textit{supra} note 57, at 320-21.


\textsuperscript{116} Rabin, \textit{supra} note 57, at 321.

\textsuperscript{117} Hooker, \textit{supra} note 40, at 37. For a criticism of the FTC’s current involvement in particular, see generally Michael D. Scott, \textit{The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?}, 60 ADMIN. L. REV. 127 (2008).

\textsuperscript{118} Rabin, \textit{supra} note 57, at 323.

\textsuperscript{119} \textit{Id.}; see also Hooker, \textit{supra} note 40, at 37.

\textsuperscript{120} Rabin, \textit{supra} note 57, at 324.
If any common theme can be drawn from the foregoing three sections, it is that litigation over cyber risks remains an unpredictable area of the law, which means that the scale of the third-party liabilities a company may incur is similarly variable. Arguably, many of the common law or statutory claims commonly pursued offer only an uneasy fit for the types of damage third parties usually suffer following data breaches. And indeed, some have argued that looking to tort to effectively “regulate” against further damaging breaches (through deterrence or cost-shifting) is misguided for precisely this reason, even as others argue that federal regulatory action is no better. Nonetheless, as of this writing, these lawsuits seem likely to keep coming. In the absence of comprehensive regulation or technological change to “fix” the data breach problem, affected parties will continue turning to the legal system to redress their injuries. And as long as this goes on, there will be continued arguments over and advocacy for expanding pathways for cyber risk liability within the existing system.

Taken together, these first- and third-party liabilities mean that cyber risks are expensive. According to the Ponemon Institute’s most recent estimates, every record lost or stolen costs a company an average of $141. For companies in the United States, this cost is higher: $225 per record. And, of course, most material breaches are comprised of many records: a data breach costs a company an average total of $3.62 million, and, as previously discussed, in some particularly severe cases the costs soar significantly higher, into the hundreds of millions of dollars.

The volume and extent of news coverage surrounding major data breaches has certainly done some consciousness raising surrounding the treatment and protection of consumer data. But

---

121 See, e.g., id. at 336 (“In the final analysis, my view is that the most promising pathway for achieving the collective goal of enhancing corporate data security via tort-type remedies lies outside the tort arena . . . : A growing recognition that substandard practices might be re-cast as unfair competitive activity through federal regulatory enforcement.”).

122 See supra notes 117-120.

123 See, e.g., Julie E. Cohen, Information Privacy Litigation as Bellwether for Institutional Change, 66 DEPAUL L. REV 535, 538 (2017) (“[C]ourts must reconsider some of the procedural barriers they have put in place to deflect responsibility for resolving . . . information privacy claims in particular.”); Felix T. Wu, How Privacy Distorted Standing Law, 66 DEPAUL L. REV. 439, 440 (2017) (arguing that the use of standing law to dismiss data breach privacy claims has become “unprincipled” and “seems to be serving no purpose other than toconstitutionalize a deregulatory agenda”).

124 PONEMON, supra note 36, at 1.

125 Id. at 5.

126 Id. at 1.

127 Although it raises issues distinct from the cyber liabilities covered here, the current controversy surrounding the privacy of Internet platform users and the calls for increased regulation of these platforms (precipitated mainly by the revelations that platforms like Facebook and Twitter had been flooded by and potentially amplified Russian propaganda and hoaxes aimed at American users during the 2016 election, and that the data of 50 million Facebook users had been harvested by Cambridge Analytica for use in
even as the average organization’s (and indeed, the average person’s) level of attention to cyber risks has increased, the risks themselves have not diminished in response to such scrutiny or any related caution. In its 2017 report, the Ponemon Institute estimates that 27.7% of the organizations surveyed (every one of which had already experienced a data breach of at least 2,600 records) would experience another material data breach over the next 24 months, up from 25.6% in the 2016 report.128 Between the two reports, the average costs within the United States have increased on a per record basis,129 and the size of the average data breach in terms of the number of records stolen increased by 1.8%.130 The World Economic Forum has predicted that ineffective cybersecurity may cost the world’s economy as much as $3 trillion by 2020.131

II. Companies Have Been Generally Unsuccessful in Obtaining Coverage for Cyber Risks Through Their Commercial General Liability Insurance Policies

Given the potentially debilitating effects of cyber risks, it comes as no surprise that companies have tried to offset the costs through insurance. Many of the first-party liabilities discussed above can be covered by traditional commercial property insurance, business interruption insurance (sometimes included as part of a commercial property policy), or crime insurance.132 However, given that a data breach can also lead to substantial third-party liability, companies have sought to insure against these costs as well. Early attempts to do so saw companies seeking coverage through their commercial general liability (CGL) policies. The standard CGL insuring agreement provides for the payment of “those sums that the insured becomes legally obligated to pay as damages because of ‘bodily injury’ or ‘property damage,’”133 or “personal advertising injury,” including “oral or written publication, in any manner, of materials that violates a person’s right of privacy.”135

In response, the insurance industry launched an “aggressive campaign, both in the courts and through the modification of policy forms” to avoid coverage of cyber liabilities under these targeted political advertising) has only done more to focus attention on the value of individuals’ data held by companies. See generally, John Herrman, Cambridge Analytica and the Coming Data Bust, N.Y. TIMES MAG., Apr. 10, 2018, at MM12.

128 PONEMON, supra note 36, at 1.
129 In the U.S., the average cost per record in 2017 has increased to $225 from the 4-year average of $216. Id. at 8.
130 Id. at 5.
131 WORLD ECON. F., RISK AND RESPONSIBILITY IN A HYPERCONNECTED WORLD 26 (2014).
132 See THOMAS, supra note 27; Podolak, supra note 17, at 395-397. There is certainly more to be said on how insurers and courts have treated first-party cyber liabilities, but this Note will focus instead on the more complicated landscape of third-party cyber liability insurance.
134 Id. at 6.
135 Id. at 14.
traditional policies.136

There was litigation on two key questions: whether cyber liability meant there was “property damage” or “personal injury,” with the personal injury question being implicated more often in the third-party cyber liability context.137 There are some favorable rulings for the insureds,138 but insurers have also been successful at excluding coverage. In Recall Total Information Management v. Federal Insurance Co., a storage vendor lost data tapes, which included the personal information of 500,000 IBM employees, and the tapes were never recovered.139 The court held that Recall could not recover the $6 million it had paid to IBM under its CGL policy, because the loss of the tapes did not necessarily mean they had been “published” and so there was no personal injury under the terms of the policy.140 Similarly, after a hack of Sony’s PlayStation Network that stole the personal information of 100 million users, Sony sought CGL “personal injury coverage” in Zurich American Insurance Co. v. Sony Corp. of America. In a ruling from the bench, the court agreed with the insurer that because hackers had stolen the information, Sony had not “published” anything and thus there was no coverage.141

Parallel to the litigation, insurers sought to exclude coverage of cyber liabilities under CGL policies by modifying their language. CGL policies are usually based on standardized language crafted by the Insurance Services Office, Inc. (ISO).142 Starting in 2014, ISO made available a new endorsement called “Access or Disclosure of Confidential or Personal Information and Data Related Liability—Limited Bodily Injury Exception Not Included,”143 which eliminated CGL coverage for

damages arising out of: (1) any access to or disclosure of any person’s or organization’s

136 Podolak, supra note 17, at 370.
137 Podolak, supra note 16.
138 See, e.g., Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C., 644 F. App’x 245, 247 (4th Cir. 2016) (holding that CGL coverage applied where confidential medical information was made available online, even without evidence that anyone viewed the information); Netscape Commc’ns Corp. v. Fed. Ins. Co., 343 F. App’x 271 (9th Cir. 2009) (holding that an Internet Service Provider’s interception and internal dissemination of users’ online activities for advertising purposes qualified as personal injury (breach of privacy)); Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at *13 (D. Md. Oct. 26, 2007) (holding that under the CGL policy’s advertising injury definition, “publication” did not need to be to a third party; the perpetrators’ wrongful access to the information was sufficient).
140 Id. at 672-673.
142 1 JEFFREY W.STEMPEL, STEMPEL ON INSURANCE CONTRACTS § 4.05[A], at 29 (3d ed. 2014) (explaining that ISO is a private trade association for the property-casualty insurance industry that drafts and revises standard form policies).
143 Podolak, supra note 16.
confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information; (2) or the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.144

When this endorsement is included in a CGL policy, coverage for third-party liability following data breaches is effectively foreclosed.

III. Cyber Insurance Has Developed as a New Product to Cover Third-Party Liability Arising Out of Cyber Risks

Because of policy modification and litigation, third-party liability for cyber risks is now largely uncovered by traditional policies. Yet the costs of these cyber risks continued to mount, and the widening gap in coverage began to attract insurers writing cyber risk-specific policies, the chief purpose of which was to provide indemnity from liability for the unauthorized disclosure of sensitive consumer information.145 This new line of insurance has been variously called cyber-liability insurance, cyber-risk insurance, cybersecurity insurance, and cyber insurance—and it has been deemed a “new frontier” in the modern insurance market.146 In its current form, it has been on the market since 2009.147

Unlike CGL policies, cyber insurance policies do not rely on a standard form.148 Instead, many different insurers write their own policies, with different language in each.149 Coverage can include “website publishing, security breach liability, programming errors and omissions, replacement of electronic data, and business income” (i.e., many types of both first- and third-party liability that can arise out of cyber risks),150 but the precise scope of coverage varies dramatically across policies.151 Major cyber insurance providers include ACE Ltd., American International Group Inc., the Beazley Group Ltd., Marsh, Liberty International Underwriters, Chubb Corp., and Zurich Insurance Co. Ltd.152 Around 70% of the market is concentrated in the hands of the six largest

146 Kesan, supra note 46, at 194.
148 Podolak, supra note 17, at 399.
149 Id.
150 Id.
151 BETTERLEY, supra note 5, at 3.
carriers, but there are over 50 total insurers currently active. In 2014, the cyber insurance market brought in approximately $2 billion in premiums. By 2020, these premiums are estimated to reach $6.2 billion.

While the cyber risks themselves only seem to be increasing, the global average cost of a data breach has been trending slightly down over the past few years (though not in the United States)—the Ponemon Institute credits part of this reduction to the purchase of cyber insurance. It is impossible to draw firm conclusions given the short time span of the data available, but this at least suggests that this new product has begun to go mainstream.

### IV. Cyber Insurance Raises Particular Issues Concerning Its Viability Not Found to the Same Extent in Traditional Lines of Insurance

Cyber insurance is undoubtedly responding to a clear market need; it is obvious why a computer-dependent business would want to seek coverage for the cyber risks that seem all but inevitable. Its emergence, then, is no mystery.

However, it is less clear that as an insurance product it will achieve the same success that other more traditional forms of insurance have enjoyed. There are certain features of cyber risks that make the viability of cyber insurance both as an effective risk-spreader and as a cybersecurity measure somewhat doubtful.

#### A. Difficulties in Valuation

To begin with, there are some practical problems with building an effective insurance marketplace for cyber liability.

Insurers have struggled to price cyber insurance effectively. Cyber risks change from year to year, and it is difficult to predict what vulnerabilities will emerge or be exploited. Kevin Kalinich, a consultant on cyber risk for firm Aon Risk Services, estimated that at least two decades

---

153 Hearing, supra note 147, at 5, 7 (statement of Catherine Mulligan).
154 Hearing, supra note 147, at 2 (statement of Ben Beeson, Vice President, Cyber Security and Policy, Lockton Companies).
155 Kesan, supra note 46, at 231.
156 Hearing, supra note 147, at 2 (statement of Ben Beeson).
158 PONEMON, supra note 36, at 3.
159 Kesan, supra note 46, at 195.
160 Hearing, supra note 147, at 8-9 (statement of Catherine Mulligan).
of reliable data will be required before cyber insurers can use pricing models effectively.\textsuperscript{161} As it stands now, cyber insurers simply do not have the comprehensive actuarial data that other lines of insurance rely on to inform decisions on pricing and exclusions.\textsuperscript{162}

Others in the industry have expressed skepticism that the typical model of reliance on actuarial data will even work in the cyber risk context: “in an environment with constantly evolving threats, pricing considerations based on the past make no sense.”\textsuperscript{163}

The cyber insurance market is still in its early stages, so this is an issue that might be solved simply given more time, but for the foreseeable future it will face significant valuation challenges not present in the traditional, more established lines of insurance. This poses a problem for cyber insurance’s viability, as uncertainty may result in insurers charging higher premiums, creating exclusions, and capping coverage more than they would under perfect conditions, which may limit the reach of the market and make it difficult to attract reinsurers.\textsuperscript{164}

\textbf{B. Correlated Risks and Enormous Losses}

Another reason cyber insurance has proven difficult to effectively price is that cyber liabilities do not offer insurers a market of independent risks of varying magnitudes. But that is the typical model that allows insurance to function: insureds carrying small risks will subsidize insureds carrying larger risks, and the insurance company will not bear a loss. In this case, the cyber risks that insured organizations bear are strongly correlated.\textsuperscript{165} If there is a security vulnerability in the way one company stores credit card transactional data, for example, it is quite likely that the same vulnerability could be exploited at any number of companies.

In this way, cyber insurance might be less like auto insurance (which provides a strong system of uncorrelated risks), and more like flood insurance—the only homeowners who buy such a product are those who face a real risk of flood damage, and when a flood occurs, many insureds will be damaged at once.

Flood insurance is, of course, a poster child for a system of insurance that only survives in its present form because of government intervention.\textsuperscript{166} There are those who argue that cyber insurance

\begin{footnotes}
\item[161] \textit{Cyber Insurance Underwriting}, \textit{supra} note 152.
\item[162] \textit{Id.}
\item[164] Kesan, \textit{supra} note 46, at 195; Wilbert, \textit{supra} note 163.
\item[165] Kesan, \textit{supra} note 46, at 199; Alistair Gray, \textit{Cyber Risks Too Big to Cover, Says Lloyd’s Insurer}, FIN. TIMES (Feb. 15, 2015), https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de.
\end{footnotes}
must go the same route if it is to be effective at meaningfully combating cyber risks. Industry experts have pointed out that in a worst-case scenario (a hack on a large bank or power utility), up to $1 billion in cyber insurance coverage would be required, yet in the current market companies would struggle to obtain even half of that.

Indeed, in practice, many clients have sought to purchase more coverage than cyber insurers have been willing to offer. After the 2013 Target hack (which cost $248 million), the company received a $90 million insurance payment, leaving it to bear the remaining cost of $158 million (plus what it paid for cyber insurance). After the $43 million Home Depot hack in 2014, insurance covered only $15 million. Equifax only recovered $125 million of the $1.35 billion (so far) cost of its data breach through insurance.

As long as cyber insurance policies limit their maximum payouts and require the high deductibles they currently do, they can only provide a band-aid for the cybersecurity injuries the economy bears, and they will not be the panacea some advocates make them out to be. Several insurance companies have expressed concern that cyber risks are both “systemic” (i.e. correlated) and simply “too big to cover,” and that governments must step in if adequate coverage is the goal.

C. Barriers to Cyber Insurance Providing Effective Regulatory Governance

It also remains doubtful whether cyber insurers are well-positioned to take on a regulatory function, reducing overall risks as insurers in other lines have been able to do.

While insurance providers in other sectors have been able to play a unique role in standard-
setting and compliance-monitoring, there are a few reasons to doubt that cyber insurance will be as effective a regulator.\textsuperscript{176}

First, cybersecurity is an area where many players have aligned interests. Insurers may want to research cyber risk reduction methods to reduce their own payouts, but insured organizations and the government have similarly strong incentives to engage in the same research. In addition to the first- and third-party liability that could be covered by cyber insurance, insureds still face reputational and customer-retention concerns, as well as the very real possibility that insurance payouts will not cover all of their costs.\textsuperscript{177} As a result, any computer-reliant organization will maintain an active IT department focused on training employees and minimizing cybersecurity risks. Likewise, the U.S. Government has made clear in recent years that it views cybersecurity as a matter of national security and critical infrastructure,\textsuperscript{178} and it seems likely that cybersecurity will remain a focus of Government attention and efforts going forward.\textsuperscript{179} Simply put, cyber insurers do not have a unique incentive to innovate in the risk reduction sphere, which is a barrier to them leading as a regulator.\textsuperscript{180}

\textsuperscript{176} This is another point on which I am less sanguine than some others who have written on the subject. See, e.g., Shauhin A. Talesh, Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers for Businesses, 43 L. & SOCIAL INQUIRY 417, 428 (2018); Lance Bonner, Note, 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, 30 WASH. U. J.L. & POL’Y 257, 276 (2012) (“[Government] regulations setting standards and policies will at best represent minimum requirements. The private insurance industry could instead foster best practices, as insurers require policyholders to minimize the risk they are insuring against. Furthermore, considering the ever-changing landscape of cyber risks, it is probable that private entities are more capable of changing industry-wide standards and procedures to match new risks.”); Minhquang N. Trang, Note, Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches, 18 MINN. J.L. SCI. & TECH. 389, 389 (2017) (“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. . . . A compulsory cyber-liability regime ensures that modern, updated cybersecurity standards are implemented to help prevent data breaches and mitigate damages.”).

\textsuperscript{177} See supra notes 169-172.

\textsuperscript{178} See generally CHRIS JAIKARAN, CONG. RESEARCH SERV., R45127, CYBERSECURITY: SELECTED ISSUES FOR THE 115\textsuperscript{th} CONGRESS (Mar. 9, 2018) (outlining potential issues and priorities in cybersecurity for the last Congress).

\textsuperscript{179} An interesting counter to this point stems from a law-and-economics theory for why the problems of cybersecurity have proven difficult to solve. The standard model for why cybersecurity remains imperfect assumes it is due to flawed and fundamentally difficult and complex technical measures, deriving ultimately from the fact that the Internet as designed is inherently vulnerable to bad actors. This is the theory that this paper takes as a given. The economics theory, on the other hand, posits that it is actually because of perverse incentives: since cyber threats necessarily prey on a network of computers, the difficulty in meeting them can be better explained as problems of network externalities, asymmetric information, moral
Of course, the answer to this concern could be that insurers do not have to occupy the field in risk reduction research, as long as they join the other entities involved by adding their own valuable guidance. However, the second issue is that it is far from certain that cyber insurers could achieve any better access to information than their insureds or the government. As many experts on cybersecurity have noted, this is an area where the risks rapidly evolve, often in direct response to improved security measures. There is a widespread perception that changing cyber threats will continue to outpace increased cybersecurity. This is not to say that insurers cannot play some role in meeting these threats—many do see a place for cyber insurance in implementing more robust cybersecurity measures across a wider swath of organizations. However, at least given the current state of technology and projected trends, it seems as if the cyber sector does not lend itself well to complete or even substantial risk minimization. Rather, it is an area where incremental security improvements will be met with new threats to match them.

Third, as mentioned briefly in Part I, it is often the “human factor” that is the biggest weakness in an organization’s cybersecurity protections. Technical and administrative controls can only go so far when the success of an attack hinges primarily on the carelessness of employees (who might, for example, be tempted to click on a link in a phishing email or insert a USB drive they picked up outside). In these cases, for there to be effective risk reduction, there simply needs to be more effective training and education: employees need to know how to detect and react to potential cybersecurity attacks, and to not fall prey to common schemes.

Cyber insurers could certainly play a role in providing these trainings. But as any IT department in a large organization will explain, such training is already commonplace, often taking
creative forms in an effort to engage attention— and still worryingly ineffective. According to the Information Systems Audit and Control Association’s 2016 survey of cybersecurity professionals (most of whom work at organizations of over 1,000 employees), a significant majority of respondents had a training and awareness program in place (87%), but only 53% believed it to be effective. Notably, belief in such programs’ effectiveness has been trending down (from 71% in 2014)—perhaps a reflection of the increased sophistication of cyberattacks aimed at exploiting human vulnerabilities. As long as bad actors continue to find ways to take advantage of human frailty, and as long as it is impossible to make people hyper-vigilant for cyber threats that they do not understand, this may be an example of a risk that insurers cannot do much more to reduce. As such, cyber insurance’s potential for serving as a cybersecurity regulator may be limited.

D. Risk of Moral Hazard

The rise of cyber liability insurance also raises concerns about how organizations will handle consumer data going forward.

Some commentators worry that cyber insurance could lead to increased moral hazard in the implementation of cybersecurity. In broad strokes, their argument is that as long as organizations can offload the costs of potential liability to insurers, they will take less care with consumer data as they will have less incentive to invest in cybersecurity infrastructure when they expect potential losses to be recoverable. This moral hazard issue is very similar to the one present in discussions of traditional lines of property and casualty insurance.

However, this concern assumes two premises. First, that organizations have a fixed budget for cybersecurity spending, and that they will spend a portion of this on cyber insurance instead of investing it in improved cybersecurity measures internally. Second, that the funneling of such spending into cyber insurance will not result in improved security measures regardless.

Both of these are questionable.

The first seems like an oversimplification of IT budgets and spending. Organizations should

---

187 See, e.g., Everett Rosenfeld, New ITS Mascot Hooks Freshmen, YALE DAILY NEWS (Sept. 2, 2010), https://yaledailynews.com/blog/2010/09/02/new-its-mascot-hooks-freshmen/ (explaining how an Information Technology Services employee inside of a $800 fish costume called “Gil Phish” is on hand to teach Yale students not to fall for phishing attacks).

188 See, e.g., id. (noting that phishing attacks still successfully compromise Yale students’ accounts at a rate of two to three per week).

189 ISACA, supra note 186, at 16.

190 Id.


still have a vested interest in maintaining the security of their network systems even if they can expect to recover the costs of third-party liability in the event of a breach. The day-to-day operations of their businesses likely require a high level of functionality for their computer systems, and they probably have concerns beyond liability to third-parties that would require the protection of their data (most notably, first-party worries like trade secret protection or not wanting to lose work product, which may or may not have insurance coverage). As such, it is unlikely IT spending will be significantly diminished in response to organizations’ purchase of cyber insurance.

The second implicates the previously-discussed concerns over whether cyber insurance could effectively serve as an overall risk-reducer for the industry. In this scenario, where organizations actually are slowing their own work on improving cybersecurity—counter to the assumptions in Part IV(C)’s discussion of insurance-as-regulation—insurers would have a unique and increased incentive to invest in cybersecurity research themselves, and they could therefore issue more guidelines and requirements to the organizations they insure. Even if the moral hazard on the part of the insureds is real, then, the overall effect on the safety of consumer data might be minimal.

There are two further rebuttals to this traditional moral hazard argument.

First, cyber risks can result in harms outside of the first- and third-party liabilities that could be covered by insurance. For example, a major data breach might cause irreparable reputational harm to a company, even if it is able to recover for lost productivity time, property damage, and state sanctions and administrative fines (first-party losses) and settle any lawsuits brought by consumers (third-party losses). If, after that data breach, former customers choose to start doing business with a competitor whose security they trust more, that is a real loss to the business that goes unaccounted for in traditional categories of liability against which the business could insure. As such, most businesses will retain an incentive to keep their cybersecurity up to the state-of-the-art, even if they have comprehensive cyber insurance.

Second, as a purely practical matter, cyber insurance currently does not come close to fully compensating organizations for their losses in the case of a major data breach. As discussed in Part IV(B), the largest breaches of the decade thus far (e.g., Equifax, Target, Home Depot, etc.) came with costs exceeding the insurance coverage by tens or hundreds of millions of dollars. The reality of the marketplace and the severity of potential breaches are, in a sense, imposing a high deductible for this line of insurance. As a result, as it stands now organizations would not be able to offload all of the cyber risks they face onto cyber insurance, and thus concerns about moral hazard should be alleviated.

Still, there is another problem concerning how the mainstreaming of cyber insurance could lead to increased moral hazard, which has not yet garnered much attention.

This type of moral hazard springs from two principles. First, the need for cybersecurity protections does not scale in any meaningful way based on the amount of data a company is trying to protect: keeping one trade secret secure requires just as sound a network infrastructure as does
keeping 100 million customer records private. Second, on the other hand, the cost to a company of a data breach does scale—third-party liability in particular is felt on a price-per-record basis.193

There are good reasons why offsetting the cost of cyber risk through purchasing insurance should not reduce the incentives of a company to invest in strong cybersecurity, as discussed supra. However, it may be that it will reduce the incentive of companies to minimize the amount or value of personal data they collect on their employees or customers. As companies will now directly experience a lower cost of a data breach, the incremental risk-per-record will be lower, and the added value they could achieve from things like increased data mining or advertising capabilities by collecting more information may begin to look more appealing.

The moral hazard, then, will be that companies will put larger amounts or more types of individual data at risk. Of course, this concern is only relevant to certain types of cyber-insured companies, but it does present a unique spin on the problem of moral hazard that has not arisen in traditional lines of insurance.

V. Cyber Insurance Merits More Critical Study Than It Has Attracted to Date, and Questions of Intervention and Regulation Should Not Be Considered in a Vacuum.

In the short term, I believe the first change that needs to come for the cyber liability insurance sector is simply a change in the surrounding discourse. Indeed, one of the primary goals of this paper was merely to move us in that direction. It is a hallmark of pieces written on the cyber insurance topic to bemoan the lack of scholarly attention it has attracted, and this piece has been no different.194 The emerging cyber insurance market merits further study simply because it has the potential to impact so many aspects of our society,195 and the implications of that alone are worth understanding. But beyond that, if the scholarly discussion on cyber insurance becomes more sustained, more nuanced, and perhaps more critical, we may see more data and in-depth studies emerge on some of the issues I raise in Part IV.

There have already been several studies and reports on the state of the cyber insurance market196 (and in light of the nascent and rapidly evolving state of this sector, such studies should and no doubt will continue), but little on the purported benefits of cyber insurance. We should be able to start assessing: Now that more companies have cyber insurance, are best practices in cybersecurity appreciably changing (i.e., are the insurers performing their regulatory role)? If so, are these changed practices resulting in fewer, less severe, or less costly data breaches (i.e., are they performing it effectively)? Are the overall impacts of cybersecurity threats to the economy lower as a

193 See, e.g., PONEMON, supra note 36, at 8.
194 See supra note 6 and accompanying text.
195 See supra notes 7-15 and accompanying text.
196 See supra note 5.
result of cyber insurance’s widespread use (i.e., is it effectively performing its role as a risk-spreader)? Are the pricing schemes and expected profits of cyber insurance companies becoming more standardized or predictable (i.e., is the prospect of relying on actuarial data becoming any more realistic over time)? If the problems in the cyber insurance space start to attract more critical scholarly attention, we should start to be able to answer some of these questions based on actual data.

Such further study is a prerequisite for my second suggestion, which has to do with whether and how to ensure the cyber insurance market’s survival. As discussed in Part IV.B, the world of cyber liabilities suffers from both correlated risks and enormous losses—two features that may make it impossible for a thriving insurance market to survive. If cyber insurance attracts sustained scrutiny and lives up to its cheerleaders’ promises—organizations do need it to effectively manage cyber risks, it does improve standards of cybersecurity for covered insureds—then given cybersecurity’s importance for economic stability and national security, this may be a line of insurance that requires government intervention to guarantee its stability and survival.

Government intervention in insurance markets can take many forms (for example, government-provision, government-subsidies, or various other regulatory mechanisms), and there is ample precedent for state and federal government involvement in various lines of insurance: health insurance, flood insurance, terrorism insurance, crop insurance, deposit insurance in the financial services industry, liability insurance for nuclear power generation, political risk insurance for certain international business exports, crime insurance for certain properties in designated urban areas, hurricane insurance, and earthquake insurance.197 The common thread in all these disparate areas are that their risk regulation has been deemed important to the public interest, but purely private insurance systems cannot operate profitably within them while offering insurance products at an affordable cost. Cyber risks, with their high correlation and potential for enormous losses, may represent another such area. If it becomes clear that cyber insurance really is as socially beneficial a product as its proponents suggest, then, this suggests government intervention to keep the cyber insurance market stable may be desirable and necessary.

As a third and final suggestion, from a consumer-protection standpoint, further work should be done to ensure the moral hazard concern expressed in Part IV.D does not come to fruition or worsen. As cyber insurance becomes more widely available—even assuming it succeeds as an insurance product and the other issues discussed here are dealt with in due course—we need to bring it into the conversation on data collection and consumer privacy.

Debate on the privacy issue has been raging for years, with academics, businesspeople,

---

policymakers, concerned members of the public, and more weighing in with proposed solutions.\footnote{This is the subject of countless other articles, and to adequately canvas them here would be a herculean task. For a sampling, merely to provide a sense of the diversity of concerns and proposed solutions in this space, see, e.g., Jack M. Balkin, \textit{Information Fiduciaries and the First Amendment}, 49 U.C. DAVIS L. REV. 1183 (2016); Leila Javanshir, \textit{The GDPR: It Came, We Saw, But Did It Conquer?}, 42 SEATTLE U. L. REV. 1019 (2019); Michael L. Rustad & Thomas H. Koenig, \textit{Towards a Global Data Privacy Standard}, 71 FL. L. REV. 365 (2019); Pamela Samuelson, \textit{Privacy as Intellectual Property?}, 52 STAN. L. REV. 1125 (2000); Alexander Tsesis, \textit{Marketplace of Ideas, Privacy, and the Digital Audience}, 94 NOTRE DAME L. REV. 1585 (2019); Anne Logsdon Smith, Note, \textit{Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data}, 27 CATHOLIC U. J.L. & TECH. 187 (2018); Nathan Heller, \textit{We May Own Our Data, but Facebook Has a Duty to Protect It}, NEW YORKER (Apr. 12, 2018); David N. Ciciline & Terrell McSweeney, \textit{Competition Is at the Heart of Facebook’s Privacy Problem}, WIRED.COM (Apr. 24, 2018).} Insurance, not particularly surprisingly, has not been a part of that discourse to any appreciable degree. But cyber insurance is lurking in the background for all of the companies that hold consumers’ personal data, and it is possible that its continued availability will affect the amount or the character of the personal data the companies choose to hold. The solutions being put forward focus, again not particularly surprisingly, on the companies holding the data. If these solutions are to encompass the full scope of the problem, then they need to consider the effects of cyber insurance as part of their calculus. This is true across the board. If we are looking to further regulate the companies holding personal data, we must consider how that regulation should address the insurance providers behind the companies. If we opt for adopting an information fiduciary system, we must query whether we should and if so how we can bring insurance companies under that umbrella. If we ask the companies for self-governance and transparent standards, we must ensure the insurance providers are involved as well. In short, no matter where the conversation on data privacy goes, it is time that some of the discourse on cyber insurance starts to come with it.

\textbf{Conclusion}

Cyber insurance is still so new that even basic facts about its future remain unclear. What kind of market coverage can it achieve? Will its pricing become more data-driven and consistent? Will its presence bring down the overall costs of cyber risks going forward? Will there be litigation over the scope of its coverage? These are practical questions, and undoubtedly the passage of time will provide more data and more clarity.

Depending on the answers to these questions, insured companies stand to gain economically from the availability of cyber insurance—though likely not enough to completely offset or even put a significant dent in the staggering cyber liabilities companies now risk.

For those individuals whose personal data is held by the insured companies, the effects will be indirect and perhaps intangible. For them, the questions are broader. Is this a market that can survive? Will cyber insurance have any effect on cybersecurity at all? Will individuals’ data be better protected? Might it only encourage companies to take more liberties with third-party data? Will it
change anything about how data breach claims are litigated in court?

As of now, hopes are high for the impact cyber insurance could have on the economy and on cybersecurity. Its promise, however, should not be oversold. As an insurance product, it is different enough from traditional lines of insurance that one should not take its emergence as a guarantee of its success. As cyber insurance continues to establish itself, there should be further study of the realism of its pricing, the viability of its operation given correlated and consistently large risks, its ability to reduce cyber risks overall through standards-setting and compliance-monitoring, and the possibility of its encouragement of morally hazardous data-collection practices on the part of large companies. At the very least, these potential areas of concern will make the cyber insurance market an interesting one to watch in the years to come.

199 See, e.g., JAIKARAN, supra note 179, at 15 (identifying cyber insurance as one potential mechanism for strengthening cybersecurity in the U.S.).