THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

THE POTENTIAL ROLE OF CYBER-LIABLITY INSURANCE IN DATA BREACH LITIGATION

ERIC S. MCCOY
SPRING 2016

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree in Information Sciences and Technology
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

John Bagby
Professor of Information Sciences and Technology
Thesis Supervisor

Marc Friedenberg
Lecturer of Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

This paper aims to illuminate cyber-liability insurance's potential to alleviate the information asymmetry of the information security market, and to decrease defendants' liability in data breach litigation. To accomplish this end the paper elaborates the economic research undergirding the nature of the information asymmetry problem. The paper also discusses the precedential background of data breach litigation and the current cyber-liability insurance market to explore how innovations in cyber-liability insurance stand to take advantage of the existing legal landscape. Finally, the issues of relying on cyber-liability insurance to set standards are presented and the paper concludes with a balanced assessment of cyber-liability insurance's potential.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I want to thank my family for their support, and my thesis advisors Professor Bagby and Professor Friedenberg for providing guidance.

Chapter 1
Introduction

The threat of data breaches poses an unavoidable problem for any company utilizing personal information. An industry report noted that the average cost to companies dealing with the legal fallout of data breaches increased from $1.6 million to $1.64 million from 2014-2015. This sobering figure includes expenses such as compliance with state and federal data breach notification laws as well as lawsuits against the breached company by the owners of the breached personal information.[1] The claims that plaintiffs make against the breached parties vary from negligence, breach of implied contract, and violation of various federal statutes, but few claims succeed. Commonly, the plaintiffs claim that the defendant subjected them to an increased risk of identity theft via the breach, and thus owe the plaintiffs compensation for their credit monitoring expenses. These allegations rarely survive an analysis of whether the plaintiffs suffered an injury in fact sufficient to confer Article III standing, unless the plaintiff proves that they suffered an instance of identity theft as a result of the breach.[2]

Regardless of the legal standard applied to determine whether mitigation expenses produce standing, mandating increased security measures promises to reduce the defendant's liability in data breach cases. The issue remains of how to set standards which ensure a uniform level of information security across various businesses. Government standards for information security exist in the form of federal laws, state laws and the provisions of various standards

---

[1] Ponemon Inst., 2015 Cost of Data Breach Study: United States, 1 (2015).
[2] *See. In Re Hannaford Bros. Co. Customer Data Sec. Breach Litig*., 613 F. Supp. 2d 108 (D. Me. 2009).

setting bodies; however, applying these standards to a variety of organizations fails to guarantee uniform levels of information security. This arises from the fact that standards setting bodies suffer from a lack of information on cyber-attacks, due to the legal, reputational and competitive risks that sharing cyber-attack information poses.[3]

The burgeoning cyber-liability insurance industry potentially provides a third party able to aggregate and analyze cyber-risk information to mandate standards customized to the individual risk of each industry. This enables insurers to price risks accurately and security solution providers to design more effective security countermeasures. If cyber-liability insurers choose to fill this role they could incentivize companies to forfeit their cyber-risk information, because the insurers could make this condition of their contract for data breach insurance coverage, and their clients would benefit from the robust standards proposed by the cyber-liability insurers. Cyber-insurers would take on the cost of defending their clients in data breach litigation, so naturally they would aim to reduce their clients' liability for data breaches and offer incentives for clients to practice increased information security. The cyber-liability industry falls short of offering holistic information security, but further development of the industry in co-operation with government standard setting authorities or private voluntary consensus based standard setting bodies promises to increase information security while decreasing defendants' data breach liability.

---

[3] Eric Weiss, Cong. Research Serv., Legislation to Facilitate Cyber Security Information Sharing: Economic Analysis, 4-5 (2015).

Chapter 2
The Information Asymmetry Problem

The importance of research during the purchase of a used car highlights the basic concept behind the information asymmetry problem. Prudent consumers research information relevant to the car's value before stepping on the lot, to help them gain a conception of the car's monetary worth. Consumer word of mouth incentivizes the honesty of the car salesman, because if a consumer reports that a lot sold them a lemon, this forces the vendor to reduce the price on all cars, to compensate for the lost consumer trust.[4] Information security vendors enjoy immunity from this accountability, because consumers of information security solutions often lack the expertise to distinguish effective security solutions from ineffective ones. This lack of information enables vendors to sell sub-par solutions with impunity, because little risk exists of it besmirching their reputation if their customers are unable to discern that the vendors sold them an inferior product. The inability to discern the quality of a product is referred to as the information asymmetry problem and it hinders consumers' ability to make informed investments in information security. While substantive efforts have been made by economists such as Gordon Loeb to develop models which prescribe the level of investment for adequate information security,[5] researchers lament the lack of information to prove the efficacy of specific information

---

[4] Paulo Tilles et al. *A Markovian Model Market—Akerlof's Lemons and the Asymmetry of Information*, Physica A: Statistical Mechanics and its Applications 2562, 2562-2563 (2011).
[5] Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, ACM Transactions on Info. and Sys. Sec. 438, 438-457 (2002).

security solutions.[6] This asymmetric information market also promotes the purchase of security solutions on the basis of brand recognition instead of actual quality. Purchase of popular brands gives the appearance that a business practiced due diligence in information security when in reality, the countermeasures may or may not have had any preventative effect.[7] The fact that customers often fixate on irrelevant attributes of security software in determining its level of security means that solutions that appear to give adequate information security compete just as well as solutions which actually offer exemplary information security.[8] Information security's asymmetric information market depresses innovations through allowing the survival of solutions, which give the mere appearance of providing adequate security. This is because without sufficient information regarding the efficacy of cyber-security solutions customers are incentivized to pick security solutions based on brand recognition instead of their actual effectiveness in mitigating computer system breaches. Therefore, those wishing to develop new information security systems have little incentive to enter the market because it is unlikely that customers will abandon their preferred brand of security solution. Cyber-liability insurance's interest in reducing its clients' liability incentivizes it to remedy this information asymmetry, and to create a market which encourages real innovation.

Cyber-liability insurance promises to enable a more innovative market because it will act as a method of relieving individuals and corporations from accountability for non-diversifiable

---

[6] Ranjan Pal, *Cyber-Insurance in Internet Security A Dig into the Information Asymmetry Problem*, Cornell U. Libr. 1, 2 (2012).
[7] Ross Anderson, *Why Information Security Is Hard,* Annual Computer Security Applications Conf. 1, 5-6 (2001).
[8]Cho Byong Kim, & Park Yong Wan, *Security versus Convenience? An Experimental Study of User Misperceptions of Wireless Internet Service Quality,* Decision Support Sys. 1, 9 (2012).

risk, and reduce their susceptibility to diversifiable risk.[9] Non-diversifiable risks include the vulnerability to data breaches which a company might experience as a result of vulnerability in a widely used operating system or other issues which remain outside the company's capability to control. In contrast, diversifiable risks consist of risks within the company's ability to control such as software configuration, security policies and other risk mitigating countermeasures.[10] The cyber-liability insurers primarily promise to help companies reduce diversifiable risk as they can incentivize companies to improve their practices through lower premiums. Unfortunately this means that the cyber liability insurers would be left with responsibility for the non-diversifiable risk, thus making their policies less profitable because of the need to retain money to compensate their clients for the unpredictable occurrence of a non-diversifiable risk.[11] However, without protection from liability for non-diversifiable risk companies may be less incentivized to purchase cyber-liability insurance, as there would be less benefit in paying a third party to cover risks which one can control on their own. Thus the insurers' willingness to cover non-diversifiable risk incentivizes companies to adopt cyber-liability insurance, as without it they have little protection against instances of non-diversifiable risk.

---

[9] Symposium, *Should Cyber-Insurance Providers Invest in Software Security?* Lecture Notes in Computer Science, 483 (2015).
[10] *Id.*
[11] *Id.*

Chapter 3
The Precedential Background of Data Breach Litigation

The precedential background of data breach litigation helps to reveal cyber-liability insurers' incentives to create accurate metrics for the efficacy of information security solutions. In the aftermath of a data breach, some consumers seek compensation from the breached companies, arguing that there has been an increase to their risk of identity theft. The resulting litigation typically centers on whether a consumer's increased risk of identity theft from a data breach fulfills Article III's *injury in fact* requirement for standing.[12] Initially, courts found that an increased risk of identity theft fell short of an injury in fact; however, *Pisciotta v. Old Nat'l Bancorp*[13] broadened the definition of injury in fact to include a substantial increase in identity theft risk.[14] Courts disagreed about *Pisciotta*'s legitimacy causing a circuit split which *Clapper v.*

---

[12] Article III of the Constitution requires a plaintiff to show that, "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative that the injury will be redressed by a favorable decision." (*Thomas Robins v. Spokeo Inc.*, 742 F.3d 409, 412 (9th Cir. 2013) (citing *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. Inc.*, 528 U.S. 167, 180-81 (U.S 2000)). This paper exclusively deals with the injury in fact requirement for Article III standing and not its case or controversy clause. The history of the injury in fact requirement itself is complex, and here the author confines his analysis to its application to data breaches. For a more complete analysis of the injury in fact requirement See Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, Cornell L. Rev. 275, 289-306(2008) for a discussion of the injury-in-fact requirement in Article III standing.

[13] *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 632 (7th Cir. 2007) (The case considered whether the plaintiffs' alleged increased risk of identity theft stemming from the theft of a laptop containing the plaintiffs' personal information constituted an injury in fact sufficient to confer Article III standing).

[14] *Id.*

Amnesty Int'l USA[15] partially resolved in requiring that future injuries be sufficiently concrete and imminent to constitute an injury in fact under Article III of the Constitution.[16] The *Clapper* standard leaves room for reasonable difference over imminence of the risk of identity theft. Some post-*Clapper* cases deemed an injury as imminent only if the plaintiffs prove the likelihood of the injury as certainly impending[17]; while others merely required proof that the breach substantially increased a plaintiff's risk of identity theft.[18] Whether one standard will prevail remains ambiguous; however cyber-liability insurance can take advantage of either rationale to reduce the risk of data breach litigation.

Building the Increased Risk Standard

An increased risk of identity theft is the chief harm alleged in data breach cases and initially plaintiffs' arguments that they suffered this harm generally fell short of an injury in fact in the courts' eyes. One can see this in a variety of data breach cases; however, *Hendricks v.*

---

[15]*Clapper v. Amnesty Int'l USA.*, 133 S.Ct. 1138 (U.S. 2013) (The case considered whether the **risk** of the government intercepting the plaintiffs' communications utilizing §1881a of the Foreign Intelligence Surveillance Act constituted an injury in fact sufficient to confer Article III standing).

[16] *Id.* at 1164 (The court makes an analogy to a case where plaintiffs gained standing, based on their allegation that the defendant's continued pollution of a nearby river would curtail their use of the body of water and thus cause them economic harm. In that case the plaintiffs acted reasonably in refraining from using the waterway because, its pollution practically guaranteed that they would be harmed by it. Therefore only plaintiffs able to prove that the exposure of their personal information guarantees that they will endure damages will be able to prove that their injury is concrete and imminent(*Id.* at 1153 (citing *Laidlaw, Messe v. Keene,* 481 U.S. 465, (U.S. 1987)).

[17] *See e.g. In Re: Sci. Applications Int'l Co. (SAIC) Backup Data Theft Litig.*, 45 F. Supp. 3d 14, 19-22 (D.C. 2014), *Polanco v. Omnicell*, 988 F.Supp.2d 451, 466 (D.N.J. 2013)., & *In re Horizon Healthcare Services, Inc. Data Breach Litig.*, 2015 WL 1472483 (D.N.J. Mar. 31, 2015).

[18] *See e.g. Moyer v. Michaels' Stores Inc.*, No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *14-15 (N.D. Ill. Oct. 14, 2014)., *Remijas v. Neiman Marcus Group, LLC,* 2015 4394814 at 4-6 (7th Cir. Jul. 20, 2015)., & *Galaria v. Nationwide Mut. Ins.*, 998 F. Supp.2d 646 (S.D. Ohio 2014).

DSW[19] serves as a good starting point to understand the rationale. *Hendricks* concerned a third party's compromise of personal information held by Discount Shoe Warehouse (DSW).[20] The plaintiff claimed that DSW breached its contract with its customers and credit/debit card issuers, causing them to seek an injunction against DSW to increase its security measures, and "damages 'in an amount sufficient to pay for the monitoring of [the plaintiff's] credit reports and accounts."[21] Before addressing individual claims, the court noted that the plaintiff's claim of the cost of credit monitoring as damages failed to "allege any cognizable damages or loss stemming from the data theft, as opposed to a mere risk of future damages".[22] The lack of *cognizable* damages resulted in the failure of the plaintiffs' breach of contract claim as these claims require proof that the defendant "breached the terms of the contract, and that the breach caused the plaintiff's injury".[23] A contract claim's dismissal "is warranted where damages are dependent upon the chances of business or other contingencies" and the claim "must be rejected where the breach… is *'damnum absque injuria'*".[24] The court determined that purchase of credit monitoring expenses to protect " against a risk that the stolen data will, in the future be used to

---

[19] *Teresa Hendricks v. DSW Shoe Warehouse Inc.*, 444 F.Supp. 2d 775, 776 (W.D. Mich 2006) (This case concerned whether the plaintiffs' increased risk of identity theft as a result of the breach of personal information from DSW's information processing system constituted an injury in fact sufficient to confer Article III standing).
[20] *Id.*
[21] *Id.* at 778.
[22] *Id.* at 779.
[23] *Id.* at 780.
[24] *Hendricks*, 444 F.Supp at 781. *Damnum absque injuria* encompasses acts which cause damage to another without violating their legal rights. A person possesses no legal recourse from *damnum absque injuria* actions even if they suffer damages (Andrew Hessick, *Standing, Injury in Fact, and Private Rights,* Cornell L. Rev. 275, 280-281(2008)).

(the plaintiff's) detriment" failed to constitute an injury in fact, and dismissed the claim due to lack of evidence of other injuries.

Key v. DSW[25] concerned the same breach as *Hendricks*, and thus discussed nearly identical factual and legal issues. The *Key* court determined that "an increased risk of financial harm by an unknown third party at an unidentified point in the indefinite future" too speculative to constitute an injury-in-fact for purposes of standing. The *Key* plaintiffs referenced *Sutton v. St Jude Medical S.C. Inc*[26]., which conferred standing upon a plaintiff for incurring medical monitoring expenses in response to speculative future injury from a defective medical implant, to attempt to gain standing.[27] The court noted that the *Sutton* plaintiff's speculative expenses constituted an injury in fact, because the plaintiff incurred actual and imminent risk of future injury. Unlike *Sutton*, the *Key* plaintiffs incurred preventative expenses to mitigate future injuries dependent on "the possible actions of unknown third parties at some point in the indefinite future".[28] Without proof that data thieves misused stolen information, data breaches posed an extremely hypothetical risk.

Hendricks's refusal to recognize an increased risk of identity theft as an injury in fact isolated companies from liability for all data breach victims besides those able to prove actual

---

[25] *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006) (This case concerned the same data breach which *Hendricks* addressed).
[26] *Sutton v. St. Jude Med., S.C. Inc.*, 419 F.3d 568, 571-76 (6th Cir. 2005) (This case decided that the preventative expenses which Sutton underwent to prevent future injury from a defective medical implant constituted an injury in fact sufficient to confer Article III standing).
[27] *Key v. DSW Inc.*, 454 F. Supp. 2d 684, at 690 (citing *Sutton v. St. Jude Med., S.C. Inc.*, 419 F.3d at 571-76).
[28] *Id.* at 685.

instances of identity theft stemming from the breach.[29] Data breach litigation before *Pisciotta* echoed *Hendricks'* rationale; however, *Key* and similar case law, provided grounds for *Pisciotta* to grant standing based on an increased risk of identity theft.[30]

Pisciotta and Krottner

Pisciotta v. Old Nat'l Bancorp allowed more data breach victims to attain Article III standing, in requiring proof that the data breach increased "the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions".[31] To justify this conclusion the court made analogies to various cases which conferred plaintiffs standing for incurring an increased risk of injury from the implant of defective medical devices.[32] The *Pisciotta* plaintiffs issued a negligence claim against Old National Bancorp Inc. (ONB) and sought compensation for their credit monitoring expenses, incurred in response to their increased risk of identity theft from the breach. The court found that because the breach increased "the risk of future harm that the plaintiff(s) would have otherwise faced absent the defendant's actions," the plaintiffs suffered an injury-in-fact and attained Article III standing.[33] This appears promising for the plaintiffs; however, a negligence claim under all states' laws requires "a

---

[29] Proving that a defendant's action proximately caused an instance of identity theft possibly requires the plaintiff to prove that their instance of identity theft arose *proximately* from the breach and not *coincidently*. As large data breaches become more common, it becomes more likely that the plaintiff's data was exposed in prior incidents. Proving that the present data breach directly resulted in a plaintiff's identity theft may prove an onerous task in the future.
[30] *See, e.g., Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 705-708 (D.C. Dec. 18, 2009).
[31] *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 632 (7th Cir. 2007).
[32] *Id.* at 634 (Noting that, "standing was present where a defective medical implement presented an increased risk of future health problems." (citing *Sutton v. St. Jude Med., S.C. Inc.*, 419 F.3d 568 (6th Cir. 2005)).
[33] *Id.*

compensable injury proximately caused by defendant's breach of duty".[34] The lower court determined that ONB complied with its duty to disclose the breach to customers, and that they held no duty towards the plaintiff beyond this.[35] Even if ONB had breached its duty the court determined that the credit monitoring expenses fell short of a *compensable* injury necessary for the negligence claim.

The plaintiffs of *Krottner v. Starbucks* used *Pisciotta* to successfully gain standing in a data breach case. *Krottner* concerned the theft of a Starbucks laptop containing the names, addresses and social security numbers of several employees and the employees' resultant negligence claims against Starbucks.[36] The *Krottner* appellate court modified the *Pisciotta* standard to confer injury-in-fact standing for increased risk of future injuries which posed a "credible threat of harm" and were "not conjectural or hypothetical." The court applied this standard and concluded that the plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[37]

---

[34] *Id.* at 635.
[35] In determining the existence of a duty the court turned to Indiana's data breach notification statute and determined that it merely imposed a duty to, "disclose a security breach to potentially affected customers" which ONB upheld (*Pisciotta*, 499 F.3d 629, at 637 (7th Cir. 2007)). The statute also solely authorizes the state attorney general to enforce it and confers no private right of action, leaving no justification that it confers the defendant with a "duty to compensate affected individuals for inconvenience or potential harm to credit that may follow" (*Id.*).
[36] *Laura Krottner v. Starbucks Corp.*, No. C09-0216RAJ, 2009 U.S. Dist. LEXIS 20837, at *1-31, *1(W.D. Wash., 2009) *aff'd*, 628 F.3d 1139 (9th Cir. 2010).
[37] *Laura Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142.

A subsequent case, *Anderson v. Hannaford*[38] showcases some circumstances which give rise to substantial risk sufficient to confer plaintiffs with a compensable future injury. The *Anderson* plaintiffs suffered a breach of their personal information which resulted in actual identity theft, and an increased risk of identity theft. In Maine law a cognizable injury "must be both reasonably foreseeable" and plaintiffs must demonstrate that "efforts to mitigate (the injury) were reasonable and that those efforts constitute a legal injury, such as actual money lost, rather than time or effort expended".[39] The court noted that previous rulings which denied mitigation expenses occurred in response to a real threat of data misuse and not "inadvertently misplaced or lost data which has not been accessed or misused by third parties".[40] *Hannaford*'s breach consisted of "a large-scale criminal operation conducted…by sophisticated thieves intending to use the information (debit and credit card numbers) to their financial advantage" therefore, the court determined that the plaintiffs' credit monitoring expenses constituted a reasonable response "to a real risk of misuse."[41] In future data-breach litigation evidence of the data's theft and the

---

[38] *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (This case considered whether the increased risk of identity theft, inflicted on the plaintiffs through the breach of the Hannaford Brothers Company electronic payment system, constituted an injury in fact sufficient to confer Article III standing)

[39] *Id*. at 161.

[40] *Id.* at 164.

[41] *Id.* at 164, The court cited the breach's precipitation of 1,800 instance of identity theft, alongside the plaintiffs' banks' issuance of replacement credit and debit card as evidence of the reality of the threat of identity theft (*Id.* at 163). The case almost gained class action certification; however, "it failed to show that common questions of law or fact predominated over questions affecting individual members" (John Black, *Developments in Data Security Breach Liability*, The Business Lawyer 199, 204 (2013), http://plusweb.org/Portals/0/CHAPTER/CM2014/Developments_in_Data_Security_Breach_Liability.pdf). The court made this determination primarily because the plaintiff didn't have actual statistical evidence of the cost of the plaintiff's damages and merely proposed the possibility of the existence of this information (*Id.* at 205).

thieves' intent to misuse continued to play a central role in whether the plaintiffs gained standing. [42]

Reilly v. Ceridian

Reilly v. Ceridian[43] provides strong arguments against conferring standing for increased risk of identity theft in the absence of evidence which suggests its imminent misuse. *Reilly* concerned a hacker's theft of a law firm's employees' personal information which the payroll processing firm Ceridian hosted. The plaintiffs alleged that this breach increased their risk of identity theft, compelled them to incur credit monitoring costs, and subjected them to suffer from emotional distress.[44] The court dismissed these allegations as they assumed "the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants."[45] The court determined that the plaintiffs incurred credit monitoring expenses in response to a "hypothetical speculation concerning the possibility of future injury," and thus failed to suffer an injury-in-fact.[46]

---

[42] The *Hannaford* plaintiffs' attempts to gain class action certification also demonstrate the difficulties which data breach litigants encounter when seeking class action certification after their claims of future harm survive an Article III injury in fact analysis. See Richie Thomas, *DATA BREACH CLASS ACTIONS,* Brief 12, 27-48 (2015) For a concise discussion of these difficulties and a listing of cases which demonstrate this point.

[43] *Reilly v. Ceridian Co.*, 664 F.3d 38, 44 (3rd Cir. 2011) *cert. denied,* 132 S. Ct. 2395 (2012) (This case considered whether the increased risk of identity theft which the plaintiffs endured as a result of the breach of their personal information held by a law firm, constituted an injury in fact sufficient to confer Article III standing).

[44] *Id.*

[45] *Id.* at 42.

[46] *Id.* at 43.

Distinguishing Defective Medical Device Litigation

The plaintiffs relied on *Pisciotta* and *Krottner* to support their claim that their increased risk of identity theft conferred standing; however, the court rejected *Pisciotta*'s comparison of credit monitoring expenses to expenses incurred to reduce the risk of injury from defective medical devices. The court, argued that *Pisciotta* and *Krottner* failed to assess the different contexts of data breaches and defective medical device litigation in assessing the imminence of the injury.[47]

The *Reilly* court ruled that data breach plaintiffs failed to demonstrate an actual injury or increased risk of future injury comparable to defective medical device plaintiffs. The court noted that in "medical-device cases, a defective device has been implanted into the human body with a quantifiable risk of failure.", therefore "the damage has been done…"[48] On the other hand the *Reilly* court asserted that their plaintiffs suffered no injuries because their "credit card statements (were) exactly the same…as they would have been" if no hack occurred, and the breach exposed plaintiffs to "no quantifiable risk of damage in the future". [49]

The court also noted that defective medical device and data breach plaintiffs differed, because the latter retained the ability to recover damages after suffering from an instance of identity theft. The defective medical device cases, addressed an injury with the potential to kill

---

[47] *Id.* at 44.
[48] *Id.* at 45.
[49] *Id*. See Bruce Bublitz et. al. *On the Use of Market Derived Estimates of Contingent Losses: The Case of Data Breaches*, Journal of Business Cases and Applications 13 (2015). For an interesting discussion of how estimation of the future monetary loss resultant from a data breach may provide a means of proving compensable damages from the data breach itself.

the plaintiff if they declined to incur monitoring expenses.[50] Data breach plaintiffs lose "simple cash, which is easily and precisely compensable with a monetary award" while in defective medical device cases "The deceased… have little use for compensation."[51] Therefore, analogizing the risk of future injury in defective medical device cases to the risk of future injury in data breach cases ignores data breach plaintiffs' ability to seek recovery for their injury after they suffer it.

Reilly's criticism of Pisciotta and Krottner provides an important critical perspective; however, *Reilly* also reinforced these cases' evidence requirements. The *Reilly* court's attempt to distinguish the case from *Pisciotta* and *Krottner* noted that *Pisciotta* plaintiffs presented "evidence that 'the [hacker's] intrusion was sophisticated, intentional and malicious,'" and that in *Krottner* "someone attempted to open a bank account with a plaintiff's information following the physical theft of the laptop".[52] *Reilly* modified *Pisciotta*'s substantial risk requirement to require evidence of intent to misuse the data, *Clapper v. Amnesty International Inc.* overturned the substantial risk standard to install a stricter requirement for determining injury-in-fact for future injuries.

---

[50] *Id.*
[51] *Id.*
[52] *Id.* at 44.

The Clapper Standard

Clapper v. Amnesty Int'l USA concerned the interception of communications between Amnesty International employees and their foreign clients through §1881a of the Foreign Intelligence Surveillance Act, which authorized the federal government to attain communications between US citizens and foreigners affiliated with terrorist organizations.[53] To attain Article III standing Amnesty International asserted that §1881a subjected them to "an objectively reasonable likelihood," of the government intercepting their communications under §1881a "thus causing them injury".[54] They also maintained that their mitigation expenses in response the risk of surveillance constituted a "present injury that is fairly traceable to §1881a".[55]

The court rejected the contention that an "objectively reasonable likelihood" of plaintiffs suffering interception of their communication conferred standing, because it conflicted with the,

---

[53] This sounds like an admirable goal; however, depending what authority one consults a terrorist organization could range from legitimately hostile organizations to organizations engaging in non-violent civil disobedience.
[54] *Clapper,* 133 S.Ct. at 1146 (U.S. 2013).
[55] *Id.* at 1141.

requirement that "threatened injury must be certainly impending to constitute injury in fact".[56] The plaintiffs' allegations assumed that the government successfully executed the actions necessary to intercept their communications under §1881a.[57] Therefore, the court denied that the government inflicted plaintiffs with an injury in fact, because without evidence of the plaintiff's communications' interception under §1881a, their claims relied on speculation regarding the future acts of third parties.[58] *Clapper* also struck down Amnesty International's attempt to assert standing through the costs they undertook to avoid government surveillance. The court previously determined that surveillance under §1881a failed to qualify as "certainly impending", therefore the plaintiff's credit monitoring expenses failed to constitute an injury-in-fact, because the plaintiffs undertook them in response to the risk of future injury. The court denied classifying the credit monitoring expenses as an injury-in-fact because this potentially permitted plaintiffs to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[59]

Clapper replaced the substantial risk standard with the requirement that plaintiffs demonstrate an imminent risk of the future harm before the court deemed the future harm as an injury in fact. Like *Reilly*, *Clapper* required plaintiffs alleging that the risk of future injury constituted an injury in fact to present allegations which failed to rely on a third party's future actions. *Clapper* also affirmed *Reilly*'s judgment that a plaintiff's credit monitoring expenses failed to constitute an injury-in-fact unless the plaintiff incurred them in response to a certainly

---

[56] *Id.* at 1143.
[57] *Id.* at 1148.
[58] *Id.*
[59] *Id.* at 1151.

impending injury. The case greatly influenced future data breach litigation; however, a split remained between whether plaintiffs should attain standing based on a certainly impending future injury or a substantial risk of future harm.

The Certainly Impending Standard

Much post-*Clapper* data breach litigation precluded injury-in-fact status from future injuries unless the plaintiff alleged a "certainly impending" injury which failed to rely on "a highly attenuated chain of possibilities".[60] *In Re: Sci. Applications Int'l Corp. (SAIC) Backup Data Theft Litig.*[61] demonstrated a court's application of the certainly impending standard to analyze allegations that the theft of tapes which contained personal information precipitated an imminent risk of identity theft for the owners of the stolen data.[62] The plaintiffs alleged that their injuries included "an increased risk of identity theft….at 9.5 times their pre-theft risk….and, in at least one case actual identity theft".[63] Unfortunately for the plaintiffs the court determined that only those plaintiffs, who suffered identity theft, incurred an injury-in-fact. The plaintiffs' likely advanced their claim that the breach increased their identity theft risk by 9.5 percent to provide an example which disproved *Reilly*'s assertion that data breach plaintiffs "suffer no quantifiable risk of damage in the future".[64] The court refused to accept that the quantitative likelihood of identity theft constituted a certainly impending risk noting that "only about 19% of breach

---

[60] *Id.* at 1141.
[61] *In Re: Sci. Applications Int'l Co. (SAIC) Backup Data Theft Litig.*, 45 F. Supp. 3d 14 (The case concerns whether the plaintiffs' increased risk of identity theft resulting from the theft of data tapes from a truck constituted an injury in fact sufficient to confer Article III standing).
[62] *In Re: Sci. Applications Int'l Co. (SAIC) Backup Data Theft Litig.*, 45 F. Supp. 3d 14, 19-22 (D.C. 2014).
[63] *Id.* at 22.
[64] *Reilly*, 664 F.3d at 44.

victims actually experience data theft" therefore "injury is likely not impending for over 80% of the victims".[65] The *SAIC* court noted that the injury rested on speculation regarding the actions of a third party. For the thief to harm the plaintiffs, he would have to: recognize that computer tapes store information, find a tape reader, download the necessary software to read the tapes, decipher the encrypted portions of the data, interface with the company's database format, and misuse the plaintiff's personal information.[66] The *SAIC* court concluded that the theft of data tapes fell short of inflicting plaintiffs with a certainly impending increased risk of identity theft, because the other plaintiffs failed to prove that the thieve immediately intended to misuse their information. Other courts focused on whether the injury substantially increased the risk of the data's misuse in issuing their opinions.

Substantially **Increased Risk**

Moyer v. Michaels'[67] found *Clapper* compatible with *Pisciotta* and *Krottner*'s conclusion that a substantial increase in risk constituted an injury in fact. *Moyer* discussed whether Michaels' breach of personal information caused an increased risk of identity theft which constituted an injury-in-fact. The *Moyer* court found that the increased risk of identity theft constituted an injury-in-fact, because the plaintiff's faced a "credible non-speculative risk of harm" due to the fact that other plaintiffs suffered identity theft after the breach.[68] The court deemed the chain of causation separating the breach and possible identity theft scant enough to

---

[65] *In Re: Sci. Applications Int'l Co. (SAIC) Backup Data Theft Litig.,* 45 F. Supp. 3d at 26.
[66] *Id.* at 25.
[67] *Moyer v. Michaels' Stores Inc.,* No. 14 C 561 (This case considered whether the increased risk of identity theft which plaintiffs endured as a result of the breach of Michaels's point of sale systems constituted an injury in fact sufficient to confer Article III standing).
[68] *Id.* at *14-15. (The court referenced a catalog of cases which deemed a risk of future harm adequate to establish Article III standing from a previous case to justify its conclusion).

designate the injury as non-speculative, declining to enter into the chain of circumstances analysis present in *SAIC*.[69] Finally, the *Moyer* court called into question employing an "especially rigorous" standard developed to determine "whether the FISA Amendments Act of 2008, 122 Stat. 2436, was unconstitutional" to data breach cases which presented "neither national security nor constitutional questions". It concluded the rigorous application of *Clapper*'s certainly impending standard as warranted only in cases involving "national security and constitutional issues…"[70] This conclusion distinguished *Clapper* as applicable only in cases which presented issues of constitutional authority; this allowed *Moyer* to employ its increased risk standard in deciding whether an increased risk of identity theft constituted an injury in fact.[71]

---

[69] *Id.* at *17-19.
[70] *Id.* at *19.
[71] It is important to note the importance of case-law regarding the question of whether willful violation of a statute constitutes an injury-in-fact sufficient to confer Article III standing even though the plaintiffs suffered no actual harm. This question lies outside the scope of this article but See Bradford Mank & James Helmer, *Data Breaches, Identity Theft and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits,* 92 Notre Dame L. Rev. 35-46 (forthcoming Feb. 2016). For a thorough and well researched discussion of this issue and current trends in the case law.

Chapter 4
The Need for Cyber-Liability Insurance

Gaps in Traditional Insurance Coverage

Until recently the monetary harm that companies anticipated through computers arose from physical harm of the systems themselves. This assumption compelled companies to cover their computer assets under First Party Property (FPP) insurance which covers repair of damaged property. Companies also covered the loss of business which damage to computer systems precipitated with Business Interruption (BI) insurance, a subset of FPP which covers the loss of income from a business interruption and/or the expenses taken to continue business operations after the interruption.[72] Therefore FPP and BI insurance potentially exclude data breach damages. For example, if a virus interrupts business operations, a claim under FPP or BI insurance faces failure, as most viruses inflict no tangible damage on computers.[73] Media insurance covers harm to the policyholder if they published defaming statements or anything that infringes a person's right to privacy. This insurance often fails to cover data breach litigation damages, because the courts often determine that clients lack standing, and therefore no privacy claim arises.

As personal information becomes increasingly valuable, and litigation from data breaches more prevalent, the importance of FPP insurance has faded and third party liability (TPL) insurance, which covers the expenses of any litigation against the policy holder, has become

---

[72] Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists 176-177 (Thomas J. Shaw., 1st ed. 2012).
[73] *America Online Inc. v. St. Paul Mercury Ins. Co*., 347 F.3d 89, 96 (4th Cir. 2003) (concluding that although viruses altered a computers logic they failed to cause tangible damage because they left the computer's physical media unharmed).

incredibly important. TPL covers possible damages from a breach better than FPP; however, it still falls short of complete coverage. If a hacker steals personal information, and holds it for years before "publishing" it, the claims immediately following data breaches face denial of standing, without evidence of harmful publication. Commercial general liability (CGL) is a type of TPL insurance under which the insured obtains coverage for a fixed period after the injury occurred, or for a fixed period after filing the claim.[74] CGL policies provide coverage on claims made basis and this makes acquiring coverage difficult, because unless the insured filed their claim after the hacker published the information, the breach falls short of harmful publication under current law.[75] Cyber-liability insurance developed to fill the gaps left by traditional insurance.

Cyber Liability Insurance Explained

Cyber liability insurance covers "customer-notification expenses; credit monitoring and identity theft monitoring; privacy and security liability; business interruption; cyber extortion; hacker damage costs; privacy regulatory defense and penalties; computer forensics investigation; and a privacy attorney".[76] Despite cyber liability insurance's novelty the National Association of Insurance Commissioners (NAIC) identified it as a top priority for the insurance industry in

---

[74] Lorelie S. Masters, *Insurance Protection for Security Breaches, in Data Breach and Encryption Handbook* 271, 272-273(Lucy Thomson ed., 2011).

[75] Although definitions of publication differ, some insurers designate that publication is "the 'communication (as of news or information) to the public,'" (*Recall Total Information Management Inc. v. Federal Ins. Co.*, 147 Conn. App. 450, 463 (Conn. App. Ct. 2014)). Thus theft of personal information does not necessarily imply publication, because the thief might not reveal the information publically.

[76] Matthew Sturdevant, Covering Online Terrorism: Sony, Target Cases Cloud Decisions; Cyber Insurance, Hartford Courant, Jan. 26, 2015 at A1.

2015. NAIC noted that although cyber-liability insurance is expensive, it possesses great growth potential as businesses realize that their current policies preclude coverage for most damages from data breaches.[77] This growth in the customer base possesses the potential to alleviate some of the problems the cyber insurance market suffers from its lack of cyber risk information.

Issues with the Cyber Liability Insurance Market

The cyber-liability insurance industry faces a variety of market issues arising from a lack of cyber threat information. All insurance companies set their premiums and coverage limits through statistical formulas which calculate the risk of the insured suffering from an injury. Insurers of traditional risks such as fire or automobile, easily set premiums and coverage limits reflecting the client's actual risk, through the analysis of readily available historical data. The cyber-liability insurance industry lacks the ability to project cyber-risk's probability, due to the dearth of documented cyber risk information. Unfortunately, few incentives exist for companies to document and share this information with cyber insurers, thus slowing the accrual of cyber risk information.[78] Uninsured companies are wary of sharing cyber-risk data with government bodies, as it may cause them negative publicity, or be used against them by rival companies. Companies with cyber-liability coverage primarily make claims after catastrophic incidents, biasing the risk data towards extreme cyber events.[79]

---

[77] Nat'l Ass'n of Ins. Comm'r(s) & The Ctr. for Ins. Policy and Research, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last visited Feb. 22, 2016).
[78] Christian Biener, Martin Eling, Jan Wirfs, *Insurability of Cyber Risk: An Empirical Analysis,* 40 Geneva Papers on Risk and Insurance: Issues and Practice 1, 9-12 (2015) (analyzes issues with the cyber-risk market in the U.S empirically).
[79] Rainer Böhme, & Galina Schwartz. *Modeling Cyber-Insurance: Towards A Unifying Framework,* 1, 17 (Workshop on the Economics of Information Security, Working Paper no. June: 1–36).

Insurers also utilize potentially inaccurate information as this scarcity of data enhances three fallacies inherent in the insurance business. The first, adverse selection occurs when insurers lack accurate metrics to measure the risk level of prospective clients. This leads to premiums which fail to reflect the increased risk that insuring the client poses to the insurer, an inaccuracy which threatens insurers' financial solvency in the event of repeated or catastrophic claims.[80] Although similar to the moral hazard fallacy adverse selection emphasizes the insurers' inability to determine the truthfulness of a client's self-reported risk level. Ordinarily insurers verify the client's veracity, via statistical analysis.[81] The lack of historical data in a cyber-risk environment forces, insurance companies to rely on the word of their policyholders. This incentivizes policyholders to misrepresent their risk level to attain lower but inaccurate premiums which spell disaster for the insurers' bottom line after repeated or monumental claims. Insurers engage in the practice of re-insurance to hedge themselves against this risk. In a market with widely available information, re-insurance enables endurance of the proverbial perfect storm. Unfortunately, the information scarcity in a cyber-risk environment makes this practice all but impossible because adverse selection and moral hazards greatly increase the likelihood of frequent claims from cyber-liability insurers.[82] Reinsurers shirk from insuring any cyber-liability insurance companies, thus further increasing the financial risk to the cyber-liability insurers.

---

[80] *Id.* at 17.
[81] *Id.* at 19-20.
[82] *Id.* at 17.

Chapter 5
The Promise of the Cyber-Liability Insurance Industry

Fortunately, increased cyber liability insurance enrollment holds the potential to decrease the asymmetric information problem's severity. The insurance provider Zurich conducted a survey in 2014 which found that fifty two percent of companies claim they will purchase some form of cyber-insurance in the future.[83] The resultant increase in cyber-attack claims that follows promises an increase in historical data available for analysis. As insurers develop more accurate measures to quantify cyber-risk, cyber-liability companies will set premiums reflecting their clients' risk level, and mandate security practices statistically proven to reduce the likelihood of cyber-attack conditions of insurance coverage. Networks which increase in value with the addition of members provide positive externalities to all members.[84] The cyber insurance market provides a network of information security knowledge, which yields increased utility to its membership as more companies purchase policies and report their security metrics to cyber-liability insurers.

Application to Litigation and Information Security Benefits

The wide adoption of cyber insurance will likely produce network externalities which benefit the internet's overall security, while reducing the insured's liability. Instead of prescribing a multitude of arbitrarily selected security practices, insurers could mandate security practices statistically calculated to minimize risk. Many cyber-liability-insurers currently

---

[83]Mary Miliken. *Insurance to Fully Cover Sony's Cyber Attack, Says CEO.* Insurance Journal (Jan. 12, 2015), http://www.insurancejournal.com/news/national/2015/01/12/353835.htm
[84] Rainer Böhme, & Galina Schwartz. *Modeling Cyber-Insurance: Towards A Unifying Framework,* 1, 10 (Workshop on the Economics of Information Security, Working Paper no. June: 1–36).

mandate that their policyholders undergo information security audits to ensure that they employ reasonable security practices.[85] The burden of data breach costs related to legal response to data breaches incentivizes, companies to provide information regarding cyber-attacks in order to maintain insurance coverage. The insurance companies hold an interest in controlling the costs of legal defense and would ensure that the practices which their audits tested for not only increased information security but decreased a plaintiff's ability to gain standing. This decreased ability to gain standing would result in an increased rate of settlements and decreased damages if the cases went to court. For example, an insurance company mandate that the insured offer free credit monitoring when it notifies customers of a breach, or employ standard encryption to lengthens the attenuated chain of circumstances leading to identity theft. If an insurer mandated enough countermeasures little likelihood exists of the plaintiff's claims prevailing.[86] These provisions would decrease the likelihood that the plaintiff's data would be used for identity theft, thus increasing the customer's welfare and decreasing the insurer's liability. Only claims where all security measures failed and actual identity theft occurred hold any potential of gaining standing. These security standards promise to decrease the insured's liability; however, if cyber-liability insurers mandate standards which comply with statutory safe-harbors plaintiffs might never bring litigation because they lack awareness of the breach.

---

[85] Ins. Journal, *CFC Partners With Cyber Security Ratings Firm to Evaluate Insureds' Cyber Risk* Ins. Journal (Jul. 20, 2015), http://www.insurancejournal.com/news/national/2015/07/20/375808.htm

[86] *See. e.g. Hendricks*, 444 F.Supp. 2d at 776, *Regina Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 705-708. & *Key v. DSW Inc.*, 454 F. Supp. 2d 684, 690.

What are Data Breach Notification Laws?

Cyber-insurance possesses the potential to mandate standards which take advantage of a variety of state data breach notification safe-harbors. To understand how this might work necessitates a brief review of the general outline of data breach notification laws. Data breach notification laws consist of state statutes mandating that collectors of personal information notify the information's owners after a data breach. Most data breach notification statutes indicate the definition of a breach, what type of information must be reported after a breach, who to notify, when to notify them, and what forms substitute notice can take.[87] Most state data breach notification laws define personal information as the combination of two or more types of personally identifiable information (PII) which usually consists of a person's first initial and last name, combined with their Social Security number, driver's license number, state ID number, or bank account number.[88] States usually define a data breach as the disclosure of PII to an unauthorized third party in a manner which compromises its confidentiality, integrity or availability. The laws define a loss of confidentiality as an "unauthorized disclosure of information," a loss of integrity as "the unauthorized modification or destruction of information"

---

[87] Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists 131-141 (Thomas J. Shaw., 1st ed. 2012).

[88] Interestingly enough there has recently been a push in state legislatures for the definition of personal information to include geolocation information, insurance provider information, user names, email addresses and unique biometric data. As the internet of things continues to grow, the success of these sort of laws may be vital to ensuring privacy (Nat'l Conf. of St. Legislatures, 2015 Security Breach Legislation, http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx (last visited February 22, 2016)).

and the loss of availability as the "disruption of access to or use of information or an information system".[89]

The stringency of the notification standards varies, but generally the statutes will require notification:

1. If a third party *acquires* the data;

2. If a third party *acquires* the data and proof exists of the data's *disclosure* to the third party;

3. Under condition 1 and/or 2 only if the breach poses a substantial threat to the data owner.[90]

The first condition requires notification after the theft of a laptop containing PII, without requiring evidence of the thief's ability to misuse the PII. For example if an employee dropped a flash drive containing unencrypted PII into a river whose current carried the drive away, no duty exists to notify consumers of a data breach due to the low likelihood of a third party acquiring the data. The second category of data breach notification requires notification only if evidence exists that an unauthorized party acquired both the data and means of accessing it. For example, evidence that a recently discharged employee downloaded unencrypted PII from the company's database before his departure warrants notification, because the employee acquired the data and

---

[89] Nat'l. Inst. of Standards and Tech., FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (2004).

[90] It is important to note that employees who need to access PII in the course of their job duties do not trigger data breach notification laws unless they use the information they gain over the course of their job duties maliciously.

likely possesses a means of accessing it via his personal computer. However, if a thief acquired heavily-encrypted PII without any evidence that he possesses the encryption key, the incident may not warrant notification, as no evidence of the thief's ability to access the data exists. The third notification criterion mandates an investigation to determine if the breach poses a substantial risk to victims if the breach meets the first and/or second criteria.

The first criterion warrants notification only if an investigation determines that a substantial risk exists of the third party acquiring the data. For example, if a few unlabeled data tapes containing unencrypted PII fell off of a transport truck on a deserted stretch of highway the investigation may determine notification unnecessary because little evidence exists that anyone acquired these tapes. Under the second data breach notification criterion it would be necessary to prove that there is a sufficient risk of the PII being acquired, and then disclosed to an unauthorized party. Tweaking the data tape example, notification would be required if the unencrypted PII was contained in clearly labeled paper files which were stolen by a roadway bandit during transit. On the other hand notification of the breach may not be required if the thief merely absconded with a truck which contained unlabeled and encrypted data tapes of PII, because although the thief acquired the information there would be little evidence that the PII had been disclosed to him in a manner which allowed it to put it to malicious use.

Whenever the notification criterion is triggered, holders of PII must disclose the breach to any affected party as well as the state attorney general. This must be done as soon as possible except where the needs of law enforcement require a delay, or other measures to ensure the

integrity of the entity's system before revealing the breach to the public.[91] Many data breach notification statutes contain safe harbors which allow companies to forego notification if they comply with various security standards.

The Problem with Data Breach Notification Laws

The ambiguities of Massachusetts and Nevada's data breach notification statutes illustrate how these laws lead companies to report data breaches despite their compliance with the safe-harbor, or allow companies to comply with the safe-harbor despite providing sub-standard security. The notable differences between these states' definition of encryption illuminate the issues arising from data breach notification statutes' opaqueness. Nevada's statute defines encryption as:

> "The use of any protective or disruptive measure, including without limitation, cryptography, enciphering, encoding or a computer contaminant, to:
>
> 1. Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; 2. Cause or make any data, information, image program, signal, or sound unintelligible or unusable; or 3. Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network." [92]

---

[91] Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists 94-96 (Thomas J. Shaw., 1st ed. 2012).
[92] Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists 106 (Thomas J. Shaw., 1st ed. 2012).

On the other hand Massachusetts defines encryption as a "processes which assign a low probability to the likelihood of an unauthorized party assigning meaning to the acquired information". [93] These definitions' vagueness confer companies in both states the ability to use sub-standard security practices. In Nevada plaintext information accessible only if one enters a five digit employee ID number fulfills the definition of encrypted information because the ID number constitutes a measure which makes the data "unintelligible or unusable" and "delays access to…data". This provides sub-par security because any hacker with an automated script possesses the ability to easily foil this security measure.[94] Massachusetts's definition of encrypted also leaves room for sub-par security because it potentially classifies, plaintext PII accessible only after entering a lengthy password, as having a "low likelihood of an unauthorized party assigning meaning to the acquired information". Although a lengthy password decreases the likelihood of someone cracking the password via automated software with enough computing power, little stands between them and the plaintext PII.[95] Data breach notification statutes adequately ensure that companies notify breached parties of their situation; however, they fail to ensure data security beyond compliance with the safe harbor requirement. The safe harbor they provide suffers from a bias for encryption, which poses merely one of the many information security practices available to companies.[96] Massachusetts's data breach notification statute

---

[93] *Id.*
[94] Aaron L.-F. Han, Derek F. Wong & Lidia S. Chao, *Password Cracking and Countermeasures in Computer Security: A Survey*, Cornell U. Libr., http://arxiv.org/ftp/arxiv/papers/1411/1411.7803.pdf (last visited February 22, 2016).
[95] *Id.*
[96] Justin C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 Wm. & Mary L. Rev. 975, 987 (2016) (Article argues that Congressional legislation poses the best method of

acknowledges this reality through requiring companies to maintain comprehensive information security plans which establish minimum standards and practices.[97] Other states fall short of requiring such stringent security countermeasures; however, cyber-liability-insurers may increase information security, while simultaneously decreasing their client's liability through mandating compliance with these safe-harbors as a condition of coverage. Data breach victims primarily gain awareness of their plight, from the data breach notification notices companies produce to comply with data breach notification statutes.[98] Therefore cyber-liability insurers stand to defray expenses from a significant amount of data breach cases if they mandate compliance with these standards as a condition of coverage.

---

allocating liability for data breaches, also references stagnating effect which encryption safe harbor of data breach notification statutes have on security).

[97] Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists, 110 (Thomas J. Shaw., 1st ed. 2012).

[98] Sasha Romanosky, David Hoffman &Alessandro Acquisti *Empirical Analysis of Data Breach Litigation* J. Empirical Legal Stud. 1, 1-27 (2013) (An empirical analysis of the common causes for data breach litigation and common outcomes).

Chapter 6
Potential Problems with Cyber-Liability Insurance

Although cyber liability insurance holds potential as a liability reducing tool, it potentially suffers from some legal vulnerability resulting from the sharing of cyber-risk information. Companies could claim that cyber-liability insurers cannot access certain security information due to intellectual property concerns. For example, an insurance firm with a cyber-liability policy understandably might shirk from sharing a customer list protected as a trade secret due to this sharing's ability to dilute the trade secret's value. On the policy drafting side the insurer must also ensure that they employ warranties wisely to achieve the maximum risk reducing effect for their clients, as otherwise clients may be improperly incentivized to reduce risk. Cyber-liability insurers should employ promissory warranties to mandate standards with the greatest potential to reduce risk and exclusions to address less dangerous risk categories.[99] If one fails to comply with promissory warranties insurers do not have to prove a connection between the breaking of the promise and the loss for which the insured makes a claim.[100] Thus promissory warranties are appropriate means to incentivize companies to strictly comply with conditions which dramatically decrease the risk of a cyber incident occurring. Cyber-liability insurers should use the conditions of exclusions to mandate standards which do not reduce risk as dramatically as those mandated in promissory warranties. Exclusions are more forgiving than promissory warranties because if the insured fails to honor its conditions they risk losing

---

[99] A promissory warranty "is a statement about future facts or about facts that will continue to be true throughout the term of the policy." (The Free Dictionary by Farlex, http://legal-dictionary.thefreedictionary.com/warranty (last visited Apr. 4, 2016)).

[100] Travis Wall, *How Not to Void Your Cyberinsurance Policy*, Risk Management (Mar. 2, 2015, 9:29pm) http://www.rmmagazine.com/2015/03/02/how-not-to-void-your-cyberinsurance-policy/

coverage for that particular risk and not the whole policy.[101] This potentially poses a problem to the insurer if insured chooses not to comply with an exclusion whose conditions substantially increase the probability of other covered risks occurring. On the upside, exclusions may allow insurers to appeal to a wider range of clients by allowing them to choose to not comply some conditions without risking losing coverage on the whole policy. Therefore, it is important cyber-insurers to carefully choose how they cover risk so that they can exert the maximum amount of pressure to incentivize clients to adopt risk reducing countermeasures, while appealing to the widest audience. Cyber-liability insurers to accurately assess the risk their clients face they will likely need to maintain databases of their clients' security information. Unfortunately, this means that a breach of a cyber-insurer entails devastating consequences as it could expose their clients to increased risk of attack by hackers and the insurers to the threat of expensive lawsuits. This makes it of paramount importance that the cyber-liability insurers also employ state of the art information security countermeasures, and that they notify their customers immediately after a breach. The cyber-liability-insurers should consider adopting data retention and destruction policies which ensure that the insurer retains no security information for longer than needed for analysis. These conventional methods of reducing liability may help cyber-liability insurers; however, developments in sharing technology also promise to reduce all parties sharing liability.

The Parallel between Cyber-Liability Insurers and Information Sharing and Analysis Centers (ISACs)

---

[101] *Id.*

The legal risks of information sharing pose one of the greatest hurdles for cyber-liability insurers. Information Sharing and Analysis Centers (ISAC) s which facilitate information sharing among critical infrastructure sectors, exemplify the legal issues which cyber-liability insurers may face.[102] The ISACs "are private sector, nonprofit entities that collect analyze and share information on cybersecurity threats and best practices".[103] Private organizations purchase subscription levels which confer various services aimed at increasing their information security. Both ISACs and cyber-liability insurers share the mission of quantitatively measuring and reducing their client's risk.[104] ISACs also suffer from a lack of cyber-threat information because legal and business concerns increase the temptation for companies to reap the rewards of the ISAC's analysis without contributing their cyber-threat information. ISACs lack information because they fail to require their members to share it; however, cyber-liability insurers can require their clients to share information as a condition of coverage, and use specialized sharing technology to reduce the risk of sharing related legal battles.

Relief from Liability

One of the simplest legal hurdles which face cyber-liability insurers are negligence based lawsuits. Negligence generally occurs if the court proves, that the defendant had a duty which they breached causing the plaintiff actual damages.[105] The foreseeability of something happening

---

[102] *Id.*
[103] Eric Weiss, Cong. Research Serv., Legislation to Facilitate Cyber Security Information Sharing: Economic Analysis., 8 (2015).
[104] For example, for five thousand dollars annually, the Financial Services ISAC's allows access to a trusted email registry, a listing of industry security practices, and various other services meant to help members increase their cybersecurity (*Id.*).
[105]Cornell Legal Information Institute, https://www.law.cornell.edu/wex/negligence (last visited Mar. 9 2016).

generally determines the scope of the defendant's liability. If the court finds that defendants knew of a risk and its preventative measures before the injury, this generally increases their liability. Therefore, companies are incentivized against voluntarily sharing attack information with cyber-liability insurers or ISACs, because of the act's potential to inflict them with increased negligence liability.[106] Cyber-liability insurers and ISACs also face the prospect of lawsuits alleging that the analysis they produce, based on their members' information, breached the member's confidentiality or intellectual property.[107] Finally, both organizations likely fear their liability under the Sherman Antitrust Act which outlaws "every contract, combination or conspiracy in restraint of trade". ISACs and cyber-liability insurers dole out their analysis exclusively to their members, which possibly compete with each other. Therefore, a plaintiff might issue a claim that an ISAC or cyber-liability insurers' analysis indirectly revealed competitive information about their organization thus restraining their ability to compete.[108] This prospect discourages cyber-liability insurers from providing their clients with the benefits of their information because of the risk of anti-trust lawsuits. While some of these issues require legislative resolution, cyber-liability insurers stand to minimize the risk of legal action if they employ methods of information sharing which only relay relevant cyber-threat information.

Technical Minimization of Sharing Liability

---

[106] Robert Palmer, Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor." *Virginia Journal of Law & Technology,* 318, 319 (2014).
[107] ITI Council, ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing, 5 (2012).
[108] *Id.* 3-4.

Cyber-liability insurers can minimize their sharing liability through adopting the intelligence community's XML markup languages theoretically unable to accept any information but cyber-threat data. A lexicon of languages exists to accomplish this end; however, the MITRE Corporation's Structured Threat Information Expression language (STIX) serves as an apt example. STIX's design communicates technical information solely related to the assets the security incident affected, and the nature of the threat arising from the incident. STIX generates this information automatically after the security software employing STIX detects the incident. STIX defines the incident element and its attributes using the variant of XML schema shown below.

```
1 <stix:Incident id="example:incident-081d344b-9fae-d182-9cc7-d2d103e7c64f" xsi:type=
'incident:IncidentType' timestamp="2014-02-20T09:00:00.000000Z">
 2     <incident:Title>Exfiltration from hr-data1.example.com</incident:Title>
```

Figure 1: STIX Excerpt

(MITRE Corp., Assets Affected in an Incident, STIX (2012), http://stixproject.github.io/documentation/idioms/affected-assets/)

The "<stix: Incident…" tag defines the incident's element's ID number, its type, and its timestamp. The "<incident:Title>" tag defines the incident element's title attribute as a human readable string, identifying exfiltration from the HR server as the security incident. [109] The HR database's breach prompts STIX to create a new incident and set its attributes to a preset value describing the incident. In this example, the breach only harmed the HR database's

---

[109] "Data exfiltration is the unauthorized transfer of sensitive information from a target's network to a location which a threat actor controls." (Macky Cruz, *Data Exfiltration in Targeted Attacks,* TrendLabs Security Intelligence Blog (Mar. 9, 2016, 8:05 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/).

confidentiality, prompting STIX to define the incident's property attribute as "Confidentiality".[110] The incident element fails to reflect any confidential information but rather creates meta-data regarding the security incident. This simplifies inter and intra-organizational information sharing through greatly reducing the risk of accidently revealing private information. If a plaintiff issues a negligence claim, STIX's status as a standard form of information sharing unable to accept any harmful information, promises to bolster the defendant's ability to claim that they exerted the upmost effort to avoid collecting confidential information. STIX's acceptance of only cyber-threat information also greatly reduces the risk of claims that the automated information sharing breached the plaintiff's confidentiality or intellectual property. The language lacks the ability to share PII; therefore the only intellectual property which the language could breach would be the plaintiff's security configuration.

STIX and other XML languages facilitate information sharing; however, a few problems demand solutions before the languages' universal adoption. International information sharing standards differ drastically, causing XML languages compliant with requirements in one jurisdiction to violate regulations in another.[111] While this initially poses a hurdle to universal adoption it also poses an opportunity for standards creating organizations to request grants to develop sub-languages which uphold the requirements of each jurisdiction. While STIX's

---

[110] The property element indicates the main threat the incident poses, defined in terms of Confidentiality, Integrity and Availability. The data breach left the equipment and data unharmed, therefore STIX sets the property to "Confidentiality" (MITRE Corp., *Assets Affected in an Incident*, STIX (2012), http://stixproject.github.io/documentation/idioms/affected-assets/). STIX helpfully denotes the data's encryption and classifies the data as public or non-public. This feature likely aims to aid companies' decision of whether to issue data breach notifications.
[111] Panos Kampanakis, *Security Automation and Threat Information-Sharing Options* IEEE Security and Privacy, 42, 50-51 (2014).

automation provides security professionals with timely updates of security events the sheer volume of information possibly makes the information security staff unable to differentiate relevant and irrelevant reports.[112] Although problematic at first, this also creates opportunity for software companies to develop solutions which parse reports and search for meaningful patterns. Finally, STIX fails to completely foreclose the possibility of anti-trust litigation, because plaintiffs may be able to claim that cyber-liability insurers revealed competitive information about their organizations' security configurations; however, it does confine the risk to revealing client's information security configuration and thus makes it easier to control.

---

[112] *Id.*

Chapter 7
Conclusions

Cyber-liability insurance occupies an ideal position to alieve the asymmetric information market which currently prevails in information security. Cyber-liability insurers' mission to reduce their client's liability from data breaches using methods which they can hold up as quantitatively sound in a court of law incentivizes them to develop quality methods of determining the efficacy of information security solutions. Incentive programs such as reduced premiums for adopting recommended security countermeasures, or precluding coverage for data breach lawsuits unless countermeasures are adopted incentivizes companies to rely on cyber-liability insurers' advice. Unlike ISACs whose free rider problem is magnified by the legal risks of sharing cyber-threat information, cyber-liability insurers can mandate sharing as a condition of insurance coverage, and can minimize their legal risks through deploying technical countermeasures. Most importantly, the cyber-liability insurers' recommendations will reduce liability for data breach litigation through recommending countermeasures which actually increase the security of the personal information. Some argue that the desire for convenient internet services is gradually eroding the public desire for privacy. One may debate this conclusions' truth endlessly, but the fact remains data breach litigation rarely prevails and wastes defendants' and plaintiffs' resources. Privacy's utility is a question for economists; however, businesses must realize the utility of the decrease in data breach liability promised by cyber-liability insurance and of an internet where people can securely share their PII.

BIBLIOGRAPHY

1. Aaron L.-F. Han, Derek F. Wong & Lidia S. Chao, *Password Cracking and Countermeasures in Computer Security: A Survey*, Cornell University Library, http://arxiv.org/ftp/arxiv/papers/1411/1411.7803.pdf (last visited February 22, 2016).
2. *America Online Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003).
3. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011).
4. Andrew Hessick, *Standing, Injury in Fact, and Private Rights,* Cornell L. Rev. 275 (2008).
5. Bradford Mank & James Helmer, *Data Breaches, Identity Theft and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits,* 92 Notre Dame L. Rev. (forthcoming Feb. 2016).
6. Bruce Bublitz et. al. *On the Use of Market Derived Estimates of Contingent Losses: The Case of Data Breaches*, Journal of Business Cases and Applications 13 (2015).
7. Cho Byong Kim, & Park Yong Wan, *Security versus Convenience? An Experimental Study of User Misperceptions of Wireless Internet Service Quality*, Decision Support Systems 1 (2012).
8. Christian Biener, Martin Eling, Jan Wirfs, *Insurability of Cyber Risk: An Empirical Analysis,* 40 Geneva Papers on Risk and Insurance: Issues and Practice 131 (2015).
9. *Clapper v. Amnesty International USA.*, 133 S.Ct. 1138 (U.S. 2013).
10. Cornell Legal Information Institute, https://www.law.cornell.edu/wex/negligence (last visited Mar. 9 2016).
11. Eric Weiss, Cong. Research Serv., Legislation to Facilitate Cyber Security Information Sharing: Economic Analysis (2015).
12. *Galaria v. Nationwide Mut. Ins.*, 998 F. Supp.2d 646 (S.D. Ohio 2014).
13. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108 (D. Me. 2009).
14. *In re Horizon Healthcare Services, Inc. Data Breach Litig.*, 2015 WL 1472483 (D.N.J. Mar. 31, 2015).
15. Insurance Journal, *CFC Partners With Cyber Security Ratings Firm to Evaluate Insureds' Cyber Risk* Insurance Journal (Jul. 20, 2015), http://www.insurancejournal.com/news/national/2015/07/20/375808.htm
16. ITI Council, ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing (2012).
17. John Black, *Developments in Data Security Breach Liability,* The Business Lawyer 199 (2013),http://plusweb.org/Portals/0/CHAPTER/CM2014/Developments_in_Data_Security_Breach_Liability.pdf
18. Justin C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 Wm. & Mary L. Rev. 975 (2016).
19. *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006).

20. *Laura Krottner v. Starbucks Corp.*, No. C09-0216RAJ, 2009 U.S. Dist. LEXIS 20837, at 1-31 (W.D. Wash., 2009).
21. *Laura Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).
22. Lorelie S. Masters, *Insurance Protection for Security Breaches in Data Breach and Encryption Handbook* 271 (Lucy Thomson ed., 2011).
23. Macky Cruz, *Data Exfiltration in Targeted Attacks*, TrendLabs Security Intelligence Blog (Mar. 9, 2016, 8:05 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/
24. Mary Miliken. *Insurance to Fully Cover Sony*'s *Cyber Attack, Says CEO.* Insurance Journal (Jan. 12, 2015),
25. Matthew Sturdevant, Covering Online Terrorism: Sony, Target Cases Cloud Decisions; Cyber Insurance, Hartford Courant, Jan. 26, 2015 at A1.
26. http://www.insurancejournal.com/news/national/2015/01/12/353835.htm
27. MITRE Corp., *Assets Affected in an Incident*, STIX(2012), http://stixproject.github.io/documentation/idioms/affected-assets/
28. *Moyer v. Michaels' Stores Inc.*, No. 14 C 561, 2014 U.S. Dist. LEXIS 96588 (N.D. Ill. Oct. 14, 2014).
29. Nat'l Ass'n of Ins. Comm'r(s) & The Ctr. for Ins. Pol'y and Res., http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last visited Feb. 22, 2016).
30. Nat'l Conf. of State Legislatures, 2015 Security Breach Legislation, http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx (last visited February 22, 2016).
31. Nat'l. Inst. of Standards and Tech., FIPS PUB 199, Standards For Security Categorization of Federal Information and Information Systems (2004).
32. Panos Kampanakis, *Security Automation and Threat Information-Sharing Options* IEEE Security and Privacy, 42 (2014).
33. Paulo Tilles et al. *A Markovian Model Market—Akerlof*'s *Lemons and the Asymmetry of Information*, Physica A: Statistical Mechanics and its Applications 2562 (2011).
34. *Pisciotta v. Old Nat'l Bancorp.*, No. 06-3817, 2007 U.S. App. LEXIS 20068, at *1-11 (7th Cir. Aug. 23, 2007).
35. *Polanco v. Omnicell*, 988 F.Supp.2d 451 (D.N.J. 2013).
36. Ponemon Inst., 2015 Cost of Data Breach Study: United States (2015).
37. Rainer Böhme, & Galina Schwartz. *Modeling Cyber-Insurance: Towards A Unifying Framework*, 1 (Workshop on the Economics of Information Security, Working Paper no. June: 1–36).
38. Ranjan Pal, *Cyber-Insurance in Internet Security A Dig into the Information Asymmetry Problem*, Cornell U. Libr. 1 (2012).
39. *Regina Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702 (D.C. 2009).
40. *Recall Total Information Management Inc. v. Federal Ins. Co.*, 147 Conn. App. 450 (Conn. App. Ct. 2014).
41. *Reilly v. Ceridian Co.*, 664 F.3d 38 (3rd Cir. 2011).
42. *Remijas v. Neiman Marcus Group, LLC*, 2015 4394814 (7th Cir. Jul. 20, 2015).

43. Richie Thomas, *DATA BREACH CLASS ACTIONS*, Brief 12 (2015).
44. Robert Palmer, Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor." *Virginia Journal of Law & Technology*, 318 (2014).
45. Sasha Romanosky, David Hoffman &Alessandro Acquisti *Empirical Analysis of Data Breach Litigation* J. Empirical Legal Stud. 1 (2013).
46. *In re Science Applications Int'l Co. (SAIC) Backup Data Theft Litigation.*, 45 F. Supp. 3d 14 (D.C. 2014).
47. Symposium, *Should Cyber-Insurance Providers Invest in Software Security?* Lecture Notes in Computer Science, 483 (2015).
48. *Teresa Hendricks v. DSW Show Warehouse Inc.*, 444 F.Supp. 2d 775 (W.D. Mich 2006).
49. The Free Dictionary by Farlex, http://legal-dictionary.thefreedictionary.com/warranty (last visited Apr. 4, 2016).
50. Thomas J. Shaw et al., Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists (Thomas J. Shaw., 1st ed. 2012).
51. Travis Wall, *How Not to Void Your Cyberinsurance Policy*, Risk Management (Mar. 2, 2015, 9:29pm) http://www.rmmagazine.com/2015/03/02/how-not-to-void-your-cyberinsurance-policy/

Academic Vita of Eric S. McCoy

emccoy432@gmail.com

Education:

Major(s) and Minor(s): Bachelor of Science in Information Sciences and Technology, Minors in Security and Risk Analysis and History

Honors in Security and Risk Analysis

Thesis: The Potential Role of Cyber-Liability Insurance in Data Breach Litigation

Thesis Supervisor: Professor John Bagby

Work Experience:

Application Development Intern,

Highmark Insurance Solutions *Pittsburgh, Pennsylvania*

May 2015-August 2015

Developed additional functionality for Highmark's insurance claims processing application used daily by employees. To ensure that the added functionality addressed the user's desires I sought input throughout the organization. In response to a lack of orientation material I authored a document to aid new hires. At the internship's conclusion I gave a brief presentation on the knowledge I gained to several executives.

Learning Assistant,

The Pennsylvania State University *State College, Pennsylvania*

August 2015-Present

Assisted professor in administering a class on the architecture of electronic payment systems by addressing student needs, and giving supplemental lectures. Created detailed diagrams demonstrating the legal implications of payment systems and found readings on payment systems, for classroom use.

Jr. Software Test Engineer

Compunetix Inc.,

Monroeville, Pennsylvania

Summers 2013 & 2014

Tested critical conferencing systems used by governmental and private entities. I began with responsibility for testing of a single system, and transitioned into testing a variety of the

company's products. After exemplary editing of test plans authored by senior employees I transitioned into authoring test plans independently.

Awards: Meyer Honors Scholarship Recipient 2013 & 2015.

Dean's List 2012-2015.

Schreyer Gateway Scholar admitted Spring 2013.

Alpha Phi Omega Gold Award

Community Service:

Treasurer, Historian, and Webmaster Alpha Phi Omega.

Treasurer for St. Paul's Wesley Student Fellowship