Mitigating Moral Hazard in Cyber-Risk Insurance

By Liam M. D. Bailey[1]

Abstract:

Over the last decade, electronically stored data has become both an indispensable asset and emergent liability for companies that transact business online. Almost weekly, data breaches and computer crimes make national headlines, compounding the public's demand for adequate protection of sensitive consumer information. Increasingly, entities doing business in the information age find that traditional commercial general liability insurance policies do not cover the loss or theft of electronic data, leaving those entities with a sizable gap in insurance coverage in the event of a data breach.

In response to this coverage gap, insurers have begun underwriting cyber-risk insurance policies to specifically address the perils of e-commerce. These policies range from coverage for losses and fines associated with data breach notification statutes, to comprehensive indemnity from consumer class action suits, infrastructure remediation costs and credit monitoring for affected individuals. Similar to more established types of insurance, however, cyber-risk coverage is not immune from the traditional vulnerabilities of the insurance marketplace, including moral hazard and adverse

[1] Liam Michael Driscoll Bailey is a third year law student at the University of Connecticut School of Law in Hartford, CT. Liam holds a B.A. in Classics from Gettysburg College and is a native of West Hartford, CT.

selection.

This Article seeks to provide insurers and policymakers with a suggestion for mitigating moral hazard in the cyber-risk insurance market. Through an analysis of information security regulation and public policy considerations, this Article proposes an information exchange that insurers and regulators may use to share loss data, claim costs, and compliance audits of insureds, in an effort to more effectively price cyber-risk coverage and thereby reduce the moral hazard presented by insureds that possess insufficient information security infrastructure. Admission to this information exchange is predicated on two conditions: First, an insurer must pledge to discount premiums for entities that employ information security infrastructure that sufficiently protects consumer custodial data as matter of public policy; and second, insurers writing cyber-risk coverage must contribute their own loss data to this information exchange.

The result of this proposal is a recommendation for an information-sharing platform, which encourages insurers to pool loss data and differentiate premiums for preferred risks. Because cyber-risk insurance is neither a market-driven private enterprise engaged in the unrestrained pursuit of profit, nor a tightly regulated, monopolistic public utility, this Article seeks to balance the autonomy of insurers with the public's need for adequately secured personal information to create a system that simultaneously mitigates moral hazard for insurers while encouraging the adequate protection of consumer data.[2]

[2] The author acknowledges and thanks Dr. David Thaw of the University of Connecticut School of Law, without whom this Article could not have been written, D. P. Stock, and the University of Connecticut Insurance Law Center.

I. INTRODUCTION

In April of 2011, Sony Corporation suffered one of the most prominent data breaches of the new millennium. Upwards of seventy-seven million users on the PlayStation® Network, a worldwide online service, were affected when unknown third parties accessed the PlayStation Network without authorization and absconded with the names, addresses, birth dates, passwords, and credit card information of Sony's subscribers. What made this particular data breach so remarkable, however, was neither the breadth of users affected nor the monetary value of the information that was stolen. Instead, what made the PlayStation Network breach so significant was the response of Sony's insurer, the Zurich American Insurance Company ("Zurich").

In July of 2011, Zurich filed an action for declaratory judgment in the Supreme Court of the State of New York, seeking "declaratory relief to settle important questions concerning Sony Defendants' claims for insurance coverage relating to numerous class action lawsuits, miscellaneous claims, and potential actions . . . arising out of one or more of the cyber-attacks perpetrated by computer 'hackers' on the PlayStation Network."[3] Zurich filed this action seeking an affirmative ruling that the insurer was not obligated to indemnify Sony under their commercial general liability or excess umbrella insurance policies for claims related to the PlayStation Network data breach. Zurich based its argument on the grounds that such claims "do not allege injury of damages covered under Coverage A—Bodily Injury of Property Damage Liability or Coverage B—Personal and Advertising Injury

[3] Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982-2011, 2 (N.Y. Sup. Ct., Jul. 20, 2011) (Complaint for Declaratory Judgment).

Liability."[4]

In this way, Zurich's action for declaratory judgment posed not only an issue for Sony, the corporation liable for the breach, but also underscored a fundamental issue at the center of the e-commerce industry: the duty of insurers for privacy, internet and network liability. As seen in the case of Zurich's 2011 action for Declaratory Judgment, insurers are increasingly willing to litigate the issue of whether commercial general liability policies provide insurance coverage for the theft of electronic data and harm to intangible property. Understandably, insurers are hesitant to indemnify corporations for data breach liability under many standard policies, due to the fact that the financial harm caused by a data breach is unpredictable and does not fall neatly within a defined policy coverage provision such as property damage, personal injury or bodily harm. In response to this evolving gap in coverage, many insurers have begun writing cyber-risk specific insurance policies to provide indemnity from liability for the unauthorized disclosure of sensitive consumer information.

The existence of cyber-risk insurance coverage, in and of itself, may not be enough to ensure that companies which compile sensitive consumer information adequately secure that electronic data as a matter of public policy. Accordingly, cyber-risk insurers face a moral hazard issue similar to traditional lines of property and causality insurance when underwriting adequately priced insurance premiums. As the costs resulting from a data breach continue to grow, firms with the greatest incentive to purchase insurance may be those with those with the greatest potential loss exposure, whether due to deficient

[4] *Id.* at 12.

information security infrastructure or participation in a highly-regulated line of business.

Assuming that firms who seek to purchase cyber-risk insurance coverage possess a fixed budget for information security, highly priced cyber-risk insurance provides an incentive for firms to purchase indemnity from data breach costs without making a corresponding investment in the information security infrastructure necessary to protect consumer data. In the short term, this asymmetry between the insurer's premium calculation and the insured's level of care may lead to inadequately priced cyber-risk insurance coverage. Should an insured devote an outsized percentage of its yearly security budget to high-cost insurance plans over corresponding infrastructure investments, the insurance carrier will be exposing itself to an increased risk of loss over the long term.

If this is the case, higher policy premiums reduce the funds available for information security infrastructure investment, thereby creating a corresponding increase in future risk of loss for the insurer and by extension the consumer. Should an insured purchase a yearly claims-made cyber-risk policy that indemnifies the insured against state sanctions, administrative fines, property damage, business interruption and consumer lawsuits arising from a data breach, the insured possesses little incentive to sufficiently secure its sensitive consumer information at the level required by public policy.[5] Thus, if the level of security infrastructure needed to price risk is lower than the level of infrastructure needed to adequately secure consumer data, firms with insufficient information security

[5] J. Wylie Donald & Jennifer B. Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board*, 18 ELEC. COM. & L. REP. (BNA) 44, 2953 (2013) (discussing the ability of insurers to require the adoption of information security standards that fit the needs of a diverse range of business endeavors).

possess an incentive to invest in infrastructure only up to the level that is required to purchase insurance coverage rather than investing to the level that is adequate for consumer protection.

In this scenario, an insured that allocates budget to cyber-risk insurance coverage over annual investments in information security infrastructure becomes insulated from the legal liability arising from a data breach, at the expense of consumers whose information remains inadequately protected from third party theft and misuse. In this way, the moral hazard problem in cyber-risk insurance presents an important public policy concern, wherein an insured is able to offset their own liability for failure to adequately secure consumer information, while leaving consumers to contend with the financial fallout of the insured's failure to adequately protect those same consumers' personal data.

For the purposes of this Article the term "public policy" is not explicitly defined. The level of information security infrastructure that is needed to adequately protect consumer data as a matter of "public policy" is a normative debate and may depend on interrelated considerations including the scope and type of data insured. Accordingly, this Article does not seek to establish a single metric upon which to evaluate the efficacy of data protection infrastructure in all instances. Instead, this Article takes the position that data protection infrastructure is sufficient as a matter of "public policy" when a custodian of consumer data maintains infrastructure that reduces the likelihood of a security breach to minimum acceptable levels and retains only residual risk.

This Article seeks to address the problem of moral hazard in the cyber-risk insurance marketplace by proposing an independent, government funded information-sharing platform for insurers to anonymously pool historical loss data, claim histories, and compliance audits

of insureds in an effort to discount premiums for insureds that adequately secure consumer data at the level required for public policy. Similar to fire insurance and other property and casualty insurance lines, moral hazard in the cyber-risk insurance market can be mitigated by differentiated premiums based on discounts contingent on corresponding investments in information security infrastructure. Much in the same way that a physical storage facility may receive reduced premiums based on fire protections exceeding those required by building code regulations, so too can insurers predicate a corresponding reduction in cyber-risk policy premium on information security infrastructure benchmarks.

Developing these benchmarks as a technical matter will be challenging for insurers. Information security is a heterogeneous exercise across many lines of business. However, insurers may be in the best position to establish such a framework for information security benchmarks through the standard-setting and compliance functions of the insurance industry.[6]

By utilizing an information pooling system, insurers will be able to adjust premiums for firms that invest in information security infrastructure that reduces the insured's risk of loss while simultaneously increasing the protections afforded to consumers. Accordingly, insurers party to the information sharing agreement will reduce their own risk of loss while creating an economic incentive for insureds to adequately secure consumer information. As a secondary effect, this information-sharing regime may serve to lower the cost of entry into the cyber-risk insurance marketplace, allowing additional insurance

---

[6] TREAS. DEPT., SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 (2013).

companies to compete with current cyber-risk insurance carriers thereby creating a more competitive marketplace with a corresponding increase in risk adjustment and underwriting protocols with the end result of increasingly affordable cyber-risk insurance policies.

II. DEFINING CYBER-RISK

A. What Are Insurable Cyber-Risks?

E-commerce and online business are a defining economic characteristic of the modern era. While the risks borne by an entity doing business online are in some ways analogous to the traditional types of liability risks that many businesses' face, some aspects of cyber-risk "are unique, in terms of location, degree, and visibility."[7] Much in the same way that a brick-and-mortar storefront faces the risk of property damage and lost business in the course of a smash-and-grab robbery, so too do firms transacting business online. In the cyber-risk context, however, the perpetrator of the theft or property damage can commit their crime from the comfort of their home, thousands of miles away, thus challenging the application of traditional security measures.

Developing a comprehensive framework for analyzing an entity's potential for cyber-risk losses depends heavily on the type of businesses in which that entity is engaged. The complete prevention of security breaches in an interconnected network may be impossible and in many cases, undesirable due to the diminishing rate of return of information security infrastructure investment.[8]

---

[7] Lawrence A. Gordon et al., *A Framework for Using Insurance for Cyber-Risk Management*, 46 COMM. ACM 82 (2003).

[8] Hulisi Ogut et al., *Cyber Insurance and IT Security Investment:*

Accordingly, what makes cyber-risk management so unpredictable is the interdependency of cyber-risks among firms doing business within the marketplace.[9] Because the security of consumer data relies on interdependent risks in a networked system, the information security risks which one firm faces will depend not only on that firm's own security protocols but also the protocols of others with whom that firm's network is linked.[10] This phenomenon of a single security event in one insured's system affecting that insureds peers—even if those peers are under different administrative control[11]—has been called interdependent security risk.[12]

In a networked system, externalities arise because of interdependencies between communicating computers.[13] For example, should a malicious code breach an information security system through a compromised machine, that malicious code will have a lower barrier of entry to the other computers on that network, resulting in more damaged property and increased amounts of

---

Impact of Interdependent Risk, FOURTH WORKSHOP ECON. INFO. SEC. 1, 2 (2005), http://infosecon.net/workshop/pdf/56.pdf (discussing the idea that complete prevention of security breaches is "technologically impossible" and in many instances would be undesirable because of the high costs and diminishing returns of security investments).

[9] *Id.* (arguing that cyber-risk interdependence occurs in two ways: the physical link computers share via the internet and the logical interdependence that comes from the ubiquitous use of computer technology).

[10] *See generally* Howard Kunreuther & Geoffery Heal, *Managing Catastrophic Risk*, 52 ENCYCLOPEDIA OF ENERGY, NATURAL RES., & ENVTL. ECON. (2013).

[11] Jay P. Kesan et al., *Cyber-insurance as a Market-Based Solution to the Problem of Cybersecurity*, FOURTH WORKSHOP ECON. INFO. SEC. 1, 22 (2005), http://infosecon.net/workshop/pdf/42.pdf.

[12] *See* Kunreuther & Heal, *supra* note 10.

[13] Kesan et al, *supra* note 11, at 22.

compromised information.[14] Thus, "this externality problem often results in a security investment's private return that is lower that the social return."[15]

While the costs arising from any single data breach are unpredictable, the average total organizational cost of a data breach in the United States in 2013 was $5,403,644.00 or $188.00 per record.[16] This amount is subject to variance, however, based on the industry that a breached entity is engaged in. On average, data breaches in highly regulated industries such as healthcare, finance and pharmaceuticals were more costly than data breaches in the energy, retail, and public service sectors.[17]

Of this $5,403,644.00 average, the four primary cost centers of a data breach are: first, detection and discovery in the form of digital forensic investigations and audit services; second, escalation, including crisis management and communication to executive managers; third, notification costs in the pursuit of regulatory compliance; and finally *ex-post* response costs in the form of remediation activities, legal expenses and identity protection services for affected consumers.[18] In addition to these process-related activities, affected companies may also experience opportunity costs associated with a security event in the form of turnover of existing customers and diminished future customer acquisition.[19] In some case,

---

[14] *Id.*
[15] *Id.*
[16] Ponemon Inst., 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2, 6 (May 28, 2013), http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.
[17] *Id.* at 7.
[18] *Id.* at 21.
[19] *Id.*

these lost business costs may even be more than any single one of the "process-related" expenses described above. In 2013, the average lost business cost for a United States organizations resulting from a data breach was $3,030,814.00.[20]

Financial institutions and health care providers possess a very high duty to protect consumer data residing on their networks and therefore a serious potential level of loss exposure. Firms that collect and retain such statutorily protected data must comply with internal controls and reporting standards set by the state and federal government. Even entities that are not specifically covered by laws or regulations pertaining to their specific industry are charged with a general duty to safeguard the consumer data under their control.[21]

In the insurance context, cyber-risk losses can be divided into two broad categories: first-party and third-party losses. First-party losses occur when an insured faces lost profits and expenses due to property damage (lost data, software, hardware) in addition to business interruption costs as the direct result of a data breach.[22] Third-party losses, on the other hand, are losses that an insured incurs as a result of the damage caused, either directly or indirectly, to another firm or individual;[23] these risks can include state and federal notification statute compliance, credit monitoring, administrative fines or penalties, and as seen in the Sony case, consumer lawsuits against the insured.

---

[20] *Id.* at 18.

[21] Kesan et al, *supra* note 11, at 9; *see also* 15 U.S.C. § 45(a) (2006) (FTC power to prohibit unfair or deceptive trade act which may include the protection of consumer custodial data).

[22] Gordon et al, *supra* note 7, at 83.

[23] *Id.*

B. Indemnifying Cyber-Risks through Insurance

Traditional insurance in the form of Commercial General Liability, excess umbrella, Errors & Omissions, and Directors & Officers policies often do not cover losses for non-physical property damage and electronic data.[24] A review of traditional insurance policies demonstrates several gaps in coverage for potential cyber-risks. Among the most prominent of these gaps in traditional insurance policies for cyber-risk losses is the lack of a "trigger" provision that would create an insured occurrence in the event of a data breach.[25] Furthermore, coverage for third-party losses related to unauthorized access to protected consumer information may not be covered, due to the fact that affected consumers are not named insureds under the insuring agreement. Geographical limitations on an insurance policy also compound the applicability of cyber-risk insurance coverage as the harm caused to an insured may originate outside of the insured area. Finally, and perhaps most important, insurers' refusal to cover cyber-risk losses under traditional liability policies continues to drive companies toward cyber-risk specific insurance products.

With the development of the Internet-based economy, both federal and state governments have passed legislation to regulate the protection of nonpublic and personal consumer information.[26] Laws such as the Health

---

[24] Kesan et al, *supra* note 11, at 6.

[25] Creative Hospitality Ventures, Inc. v. United States Liability Ins. Co.,
655 F.Supp.2d 1316 (S.D. Fla. 2009) (holding that publication of credit card receipts triggered a CGL policy's advertising injury coverage provision), *rev'd* 444 Fed.Appx. 370 (2011).

[26] Kesan et al, *supra* note 11, at 6.

Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, Executive Order 13636, state data breach notification statutes, and FTC consent decrees have sought to impose a higher standard of information security compliance upon firms that gather and preserve sensitive consumer data.[27] As a result of these administrative burdens in conjunction with the increasing costs of data breach liability, insurers have begun offering products tailored to the specific risks associated with the data breach liability for many regulated industries.

Typically, cyber-risk policies provide coverage for both first-party and third-party losses. Generally speaking, first-party losses concern claims made by an insured for financial harm suffered directly by the insured organization as a result of an insured occurrence whereas third-party losses concern claims made against an insured, by a third-party, for losses related to an insured occurrence. In a data breach, an insured's remediation costs for damage to property owned by the insured entity composes the bulk of a first-party loss while claims against the insured, made by third parties harmed as the result of a data breach, compose a preponderance of third-party losses.

[27] *See generally* 45 C.F.R. § 164.512 (2013); 15 U.S.C. § 6801(a) (2013).

Insured First Party Losses	Insured Third Party Losses
Property damage to intangible assets (*e.g.* software and electronic data)	Damage to third party property
Theft of proprietary information or consumer data[28]	Denial of access
Business interruption	Insufficient measures to protect a third party from viruses, system failure or programming errors
Damages to company assets caused by viruses	Unauthorized use of confidential information
Crisis management expenses	Loss of expected goods and services
Restoration expenses (*e.g.* restoring damaged software and replacing hardware)	Failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing identity information[29]
Fraudulent transfer of money, securities, or other property	Defense expenses related to defending regulatory actions or third-party lawsuits

[28] MARSH, CYBER RISKS: UNDERSTANDING YOUR INSURANCE PROTECTION 7 (Apr. 2011), *available at*: http://usa.marsh.com/Portals/9/Documents/UnderstandingCyberRisks2011.pdf

[29] TRAVELERS, CYBER-RISK INSURING AGREEMENT, 1, 9 (Feb. 2014), *available at* https://www.travelers.com/business-insurance/management-professional-liability/cyberrisk-apps-mktg.aspx.

Categories of first-party claims that may be insured include: property damage to intangible assets such as software and electronic data; business interruption; the "theft of proprietary information or consumer data"[30] that occurs as the result of "hackers (external and internal); viruses; extortion; programming errors; power surges and the like leading to network or system failure."[31]

Third-party claims may include a company's liability for "damage to third party property consisting of intangible assets, namely software (programs) and data and or financial losses as a result of: denial of access, insufficient measures used to protect third-party from computer crime, spread of a computer virus, failure of software, and programming errors," any or all of which lead to "network or system failures or loss of expected goods and services."[32] Additionally, third-party liability coverage can indemnify an insured from "intellectual property infringements encompassing software patents, copyrights, trade secrets, trade markets; defamation, libel and slander; invasion of privacy; unfair competition or false and misleading advertising; unauthorized use of confidential information."[33]

Beyond the financial benefit of absorbing information security losses, cyber-risk insurance provides a number of distinct advantages over government regulation as a means of encouraging adequate protection of consumer data. Unlike fines and sanctions levied by Attorneys General or government agencies on entities that do not comply with a minimum set of information security regulations, insurers can positively reinforce consumer data protection through financial incentives based upon different

[30] MARSH, *supra* note 28, at 7.
[31] *Id*.
[32] *Id.*
[33] *Id.*

classifications of risk.[34] As a result of these financial incentives, information security infrastructure spending by an insured can be assessed on the basis of value added rather than the costs incurred.[35] Assuming that an insurance carrier is able to perform an *ex-ante* risk assessment of an insured's information security infrastructure, that insurer will be able to tie premiums to the level of the insured's security.[36] A moral hazard problem arises, however, in the event that an insured opts for greater (and more expensive) insurance coverage over a corresponding investment in security infrastructure.

III. MORAL HAZARD

A. Mitigating Moral Hazard in Traditional Insurance Lines

It is commonly noted that "protection from harm induces reckless behavior."[37] This phenomenon of increases in risky behavior, predicated on access to insurance, is known as moral hazard. Moral hazard is a systemic risk faced by all insurers. Generally, moral hazard consists of three categories of behaviors by insureds, all of which are unobservable by the insurer.[38] The first type of

---

[34] Rainer Böhme, *Cyber-Insurance Revisited*, FOURTH WORKSHOP ECON. INFO. SEC. 1, 22 (2005), *available at*: http://infosecon.net/workshop/pdf/15.pdf.

[35] *Id.*

[36] Kesan et al, *supra* note 11, at 13.

[37] Sasha Romanosky, *Comments to the Department of Commerce on Incentives to Adopt Improved Cybersecurity Practices, Docket Number 130206115-3115-01* 2 (2013), http://www.ntia.doc.gov/files/ntia/romanosky_comments.pdf.

[38] Ronen Avraham, *The Law and Economic of Insurance Law - A Primer*, 19 CONN. INS. L.J. 29, 66 (2012).

moral hazard, and the primary kind of behavior that this Article seeks to address, occurs when an insured takes less than optimal precautions against an insured risk.[39] This particular behavior is referred to as *ex-ante* moral hazard and appears when an insured engages in a riskier activity than that insured would ordinarily undertake, on the basis of insurance coverage for the resulting loss. The second type of moral hazard, *ex-post* moral hazard, occurs when an insured makes insufficient efforts to minimize potential liability in the event of an insured occurrence due to insurance coverage for the resulting loss. The third type of moral hazard, sometimes defined as fraud, is an embellishment of losses by an insured to secure larger reimbursements under an insurance contract.[40]

In all three of these cases, an insured externalizes the cost of their insurance claim to the insured risk pool.[41] When an insurer is unable to distinguish between insureds which take proper precautions to mitigate *ex-ante* moral hazard liabilities and insureds which do not, the insurer is forced to charge a higher premium to all insureds, leading to cross-subsidization of socially undesirable behaviors.[42]

On the front end of an insurance transaction, the insurer's "most basic tool for creating incentives to reduce risk is the setting of differentiated premiums."[43] This may be accomplished in one of three ways. First, underwriting cyber-risks, similar to underwriting traditional property and casualty insurance lines, requires an insurer to obtain

---

[39] *Id.*

[40] *Id.* (this type of behavior can be characterized as both *ex-post* moral hazard as well as fraud depending on the magnitude of losses embellished).

[41] *Id.*

[42] *Id.*

[43] Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 205 (2012).

detailed information regarding the risk characteristics presented by a particular insured. Information obtained during the underwriting process is strengthened by the use of verification methods in the form of yearly audits and/or on-site inspections to ensure that the information disclosed by an insured is accurate. The credibility of the underwriting process is further protected by "stiff sanctions on insureds who misrepresent information."[44]

Second, under the McCarran-Ferguson Act's exemption of insurers from federal antitrust law, insurance companies are allowed to pool and analyze risk-related information through a multitude of industry-owned risk rating agencies and bureaus. These information aggregation and sharing services assist in making insurance markets more stable and increasingly competitive by lowering the cost of entry into the insurance marketplace for insurers who would otherwise possess insufficient data to underwrite insurance coverage on their own. Thus, by sharing historical loss data and claims statistics, insurers are able to more effectively price risk, thereby ensuring stability in insurance markets.

Third, insurers who are privy to the information sharing schemes described above are able to alter underwriting protocols to modify premiums according to each policyholder's individual risk assessment based on current behaviors, in addition to loss data over time.[45] When underwriting individual property and casualty insurance policies, as opposed to group policies, "insurers can refine their premiums through the practice of 'feature rating,' in which they examine the insured's individual risk

[44] *Id.* at 206.
[45] *Id.*

characteristics and adjust premiums accordingly."[46] One example of this strategy from the property and casualty insurance context is the practice of discounting premiums for fire insurance, to more than offset the cost of added safety features, such as sprinklers and smoke detectors.

In addition to feature rating, insurers engage in "experience rating" by making "retroactive pricing adjustments or prospective pricing adjustments for future policy periods."[47] The combined goal of experience and feature rating is to created insured-specific premium adjustments over time so that an insured is made aware of what safety investments correlate with particular reductions in anticipated claim costs – and by extension, corresponding reductions in premium. In this way, differentiated premiums can affect the level of safety investment made by an insured. "Insureds from whom the activity provides a high utility will purchase insurance"[48] and engage in the risk-reducing activity while "others from whom the activity provides only a low utility, will be priced out altogether."[49]

Beyond differentiated premiums, two common devices employed by insurers to mitigate moral hazard are deductibles and copayments.[50] Together, deductibles and copayments force an insured to bear a portion of any claims made under an insurance contract. For many years, moral hazard scholarship has acknowledged the tradeoff between

[46] *Id.*
[47] *Id.*
[48] *Id.* at 207-8.
[49] *Id.* at 208.
[50] Romanosky, *supra* note 37, at 7.

"full insurance and optimal care incentives,"[51] the idea being that the most efficient insurance contracts ought to require partial sharing of a loss between the insurer and insured.

While deductibles and copayments serve an important purpose in mitigating moral hazard in the insurance marketplace, neither is as efficient as "premium differentials in creating optimal incentives for the insured."[52] Thus, deductibles and copayments present less attractive incentive for insureds to mitigate losses, due to the fact that an insured does not enjoy the full social benefit of making the additional safety investment.[53]

B. Moral Hazard in Cyber-Risk Insurance

As demonstrated above, differentiated premiums based on feature and experience risk-rating methodologies present arguably the most efficient method for mitigating *ex-ante* moral hazard in individual insurance policy contracts. In the cyber-risk context, however, *ex-ante* moral hazard presents an additional public policy concern wherein an insurer is subject to increased liability in the form of additional consumer harm. For example, should an insured inadequately secure consumer data, an insurer may be liable not only for property damage remediation losses incurred by an insured but also for the legal liability arising from the insured's unauthorized exposure of statutorily

[51] Ben-Shahar & Logue, *supra* note 43, at 208-9. *See generally* Steven Shavell, *On Moral Hazard and Insurance*, 93 Q. J. ECON. 541, 546 (1979) (discussing the advantage of incentive effects to purchase insurance, where the low cost of obtaining partial insurance coverage will outweigh the imposition of risk).
[52] Ben-Shahar & Logue, *supra* note 43, at 209.
[53] *Id.*

protected consumer data.

In this way, *ex-ante* moral hazard in the cyber-risk marketplace presents an important concern for consumers. If an entity that invests primarily in cyber-risk insurance products rather than information security infrastructure is able to offset data breach liability for the resulting consumer harm, that entity possesses little incentive to pursue additional investments in security infrastructure, thereby creating both an increased risk of loss for the insurer as well as an increased risk of harm to the consumers.[54]

Hence, a cyber-risk insurance policy which indemnifies an insured (who does not adequately secure consumer data) from the liability arising out of unauthorized access to that data will create an incentive for an insured to retain only the level of information security infrastructure needed to purchase insurance coverage sufficient to offset their own potential liability without ensuring additional consumer protection. Assuming that a company which seeks to purchase cyber-risk insurance possesses a fixed yearly budget for information security investments (both insurance and infrastructure) and assuming that the level of information security infrastructure required for an insurer to adequately price

[54] While this Article does not specifically address the reputational harms that a breached entity may face as the result of unauthorized access to consumer data, it is important to note that both statutory data breach notification compliance and cyber-risk claim reporting carry inherent reputational risks for the breached entity. By publicly reporting a data breach, an organization risks economic harm in the form on diminished future customer acquisition in addition to reduced consumer confidence in the organization itself. For a more detailed analysis of how such secondary loss exposure may affect an insured's behavior when reporting data breach incidences to insurers, see Tribid Bandyopadhyay et al., *Why IT Managers Don't Go for Cyber-Insurance Products*, 52 COMMUNICATIONS OF THE ACM 68 (2009).

risk is lower than the level of infrastructure required to adequately secure consumer data, a rational purchaser will invest in infrastructure only up to the point of obtaining insurance coverage to the detriment of the consumer. Thus, an insured's reliance on insurance coverage rather than infrastructure investment may insulate an insured from the legal liability resulting from a data breach, while simultaneously leaving consumers to deal with the financial and administrative fallout of that insured's risky behavior.

At present, cyber-risk insurance is hampered in this regard by a number of practical and unresolved research challenges related to underwriting cyber-risk coverage. One of the most prominent of these challenges is the information asymmetry between the insured and insurer.[55] Because an insurer underwriting cyber-risk coverage possesses finite resources to monitor an insured's actions that affect the probability of loss after an insurance contract has been signed, it may be difficult to determine whether an insured has engaged in behaviors that increased the likelihood of a covered loss. Examples of some behaviors by an insured which may create additional risk of loss to the insurer include: "vital information regarding applications, software products installed by internet users, and security maintenance habits, which correlate to the risk types of users."[56]

Of the current cyber-risk insurance policies available, many incorporate provisions which are designed to address potential moral hazard problems.[57] One example of such a provision states that an insured "cannot claim

---

[55] Ranjan Pal, *Cyber-Insurance in Internet Security: A Dig into the Information Asymmetry Problem*, 2 (2012), http://arxiv.org/pdf/1202.0884v1.pdf.

[56] *Id.*

[57] Kesan et al, *supra* note 11, at 14.

payment for a loss or claim associated with failure to take reasonable actions to maintain and improve their security."[58] While such a provision provides sound protection for the insurer from an insured's failure to mitigate *ex-ante* moral hazard, the coverage exclusion may not sufficiently address consumer harms resulting from a data breach other than to place the *onus* of the resulting loss upon the insured rather than the insurer. For example, if an insured suffers a data breach after failing to update critical infrastructure software, the insurer may dispute coverage but the affected consumers have still suffered harm. For this reason, other methods such as heightened self-retained policy limits and/or deductibles may serve to encourage "self-protection,"[59] in light of the fact that self-insurance and market insurance can "both redistribute income toward hazardous states."[60] Accordingly, tying a firm's insurance premiums to that firm's investment in self-protection may help to mitigate moral hazard.[61] If an insured's level of information security infrastructure can be observed by the insurer on an *ex ante* basis, the presence of cyber-risk insurance may increase the amount an insured spends on self-protection as an economically rational response to the corresponding reduction in insurance premiums.

At its heart, the fundamental problem of *ex-ante* moral hazard in cyber-risk insurance rests upon the fact that an insured may be able to achieve sufficient information security infrastructure to purchase cyber-risk insurance without first obtaining the level of protection needed to

---

[58] *Id.*

[59] *See id.* at 20 (discussing insurance, self-protection, and complements, where the insurer can observe the level of protection of the insured and price is negatively related to the amount of self-protection).

[60] Isaac Ehrlich & Gary S. Becker, *Market Insurance, Self-Insurance, and Self-Protection,* 80 J. POL. ECON. 623, 637-8 (1972).

[61] Kesan et al, *supra* note 11, at 20.

adequately secure consumer data. Assuming that the level of security required for adequate protection of consumer custodial data as a matter of public policy is greater than the cost of the information security infrastructure necessary for insurers to properly price risk, an insured will possess an incentive to retain only the level of infrastructure that is required to obtain coverage which indemnifies that insured from data breach liability. Thus, the infrastructure cost of achieving sufficient consumer data protection may be greater than the cost of obtaining insurance coverage for indemnification of data breach liability, resulting in an *ex-ante* moral hazard issue with direct consequences for consumers.

IV. INSURANCE REGULATION & INFORMATION SHARING

A. Information Sharing Under the McCarran-Ferguson Act

Federal antitrust law historically has curtailed the extent to which private corporations are legally allowed to share information regarding the costs and profits of their business. Traditionally, sharing of information between competitors has led to cartelization and decreased competition within a competitive marketplace. Insurance, however, poses a unique problem when subject to federal antitrust law, as insurance itself is neither a traditional area of private enterprise in which "unrestrained capitalist rivalry ought to prevail,"[62] nor is it a purely public utility with monopoly privileges subject to "rigid rate-making."[63]

---

[62] Banks McDowell, *Competition as a Regulatory Mechanism in Insurance*, 19 CONN. L. REV. 287, 292 (1987).
[63] *Id.*

Instead, insurance has been described as a business "clothed in a public interest,"[64] which affects the community at large and therefore requires regulation that is not traditionally employed for private enterprise businesses.

Historically, the authority to regulate information sharing among insurers has been a product of state law. Insurance regulation is unique in the sense that very few areas of law expressly assign the states' supervisory power over commerce in the same way that the McCarran-Ferguson Act does for insurance regulation. Broadly, the extent to which a state may regulate the insurers doing business within its jurisdiction – the "business of insurance" – is fundamentally tied to the sovereign power of the state itself. Each state, with the assistance of the National Association of Insurance Commissioners, sets the legal regulations specifying how insurers may legally share claims costs and historic loss data without running afoul of each state's antitrust laws. This section begins with a brief overview of court cases and decisions leading up to the McCarran-Ferguson Act's antitrust exemptions for to insurers, and seeks to illuminate the types of information sharing platforms that insurers utilize under both state and federal law.

Today, insurance continues to be primarily regulated by states. The McCarran-Ferguson Act of 1945 provides that state regulation and taxation of the insurance industry best serves the public interest and that no federal law shall be "construed to invalidate, impair or supersede any law enacted by any state for the purpose of regulation the business of insurance."[65] In this way, the insurance industry has been exempted from the Sherman, Clayton,

[64] Bentley v. Allstate Ins. Co. 227 Ga. 708, 709 (1971).
[65] 15 U.S.C. § 1011 (1945).

and Federal Trade Commission Acts,[66] applicable to the extent that the so-called "business of insurance" is not regulated under the laws of the several states.[67]

Section 2 of the McCarran-Ferguson Act specifies the criteria to be used in determining whether an insurer's activity falls within the scope of the antitrust exemption afforded to insurance companies generally. Section 2 of the Act states in part that if an activity is within the "business of insurance," that activity will be exempt from federal antitrust law.[68] While precisely what constitutes the "business of insurance" may be an undefined and ambiguous term under the McCarran-Ferguson Act, the Supreme Court has crafted a three-prong test for determining whether an activity of an insurer falls within the "business of insurance."

Because insurance is regulated at the state level, many states have differing interpretations as to what the "business of insurance" entails. One reading of the McCarran-Ferguson Act's exemption for insurers from federal antitrust law might include all activities that are "regularly conducted by those firms which have as their principal purpose and effect the passage of risk from one party to another."[69] A broad interpretation such as this may include any transaction which assists in the passage of risk from one party to another, even third parties such as insurance agents, brokers, and information aggregation services within the business of insurance. Currently,

---

[66] Alan M. Anderson, *Insurance and Antitrust Law: the McCarran-Ferguson Act and Beyond*, 25 WM. & MARY L. REV 81, 88 (1983).
[67] *Id.*
[68] *Id.* at 89.
[69] Jonathan R. Macey & Geoffrey P. Miller, *McCarran-Ferguson Act of 1945: Reconceiving the Federal Role of Insurance Regulation*, 68 N.Y.U. L. REV. 13, 21 (1993).

however, this patchwork of state regulation has largely been supplanted by NAIC Model Acts, draft laws suggesting how states ought to regulate insurance companies within their jurisdiction.

In antitrust case law, courts have tended to favor a view that federal antitrust laws are displaced by state regulation when state laws regulate the same conduct that federal antitrust law seeks to control.[70] Perhaps the clearest case of a federal antitrust act exemption for insurers comes from plenary rate-setting in states which require insurance premium rates to be filed with the Insurance Commissioner before an insurer can issue policies within that jurisdiction. The strongest argument for an antitrust exemption for insurance companies, however, is that such an exemption facilitates economically efficient sharing of information thereby permitting insurers to evaluate and price risk more effectively.[71]

Cooperation between insurance companies is necessary to achieve accurate risk pricing within the industry.[72] Proper evaluation of risk requires extensive sampling of past occurrences as well as analysis of sample data to predict future losses. Without information sharing, each insurer would underwrite coverage based on only its own historical loss data, making accurate underwriting nearly impossible for all but the largest and oldest insurers. Furthermore, collaboration in the form of information sharing also achieves economies of scale, as an industry-rating bureau can perform the data sampling and analysis used by all insurance firms underwriting a certain type of risk, thereby reducing the cost of acquiring information for all insurers within a particular jurisdiction or line of

[70] *Id.* at 28.
[71] *Id.* at 47.
[72] *Id*. at 48.

business.

"The strength of this argument for information sharing depends substantially on the type of information that is being shared."[73] In the past, ratings bureaus have provided three general types of information to the insurance industry: historical loss costs, prospective loss costs, and advisory rates. Thus, the argument for information sharing among insurers centers on the transaction costs associated with antitrust regulation. Were an independent third party to purchase loss data from multiple insurers, then analyze, compile and sell that data on the annual results of specific insurance lines back to the insurers, the transaction costs associated with such a system would be higher than if insurers were allowed to directly share information among themselves.

Accordingly, collective investment in shared information produces economic efficiency in the insurance industry. If information sharing were prohibited, numerous inefficiencies would arise. Pooling and sharing loss data is efficient because it treats information as a public good: that is, the use of information by one firm does not preclude the use of the same information by another. Given expenditures for information, increased access to loss data ensures that premiums will more accurately reflect the aggregate information that all firms share, thus avoiding replication of information expenditures and keeping costs low.[74] Furthermore, a decrease in the ability to share claims data will result in firms using less information to set premium rates, thereby exacerbating adverse selection problems caused by informational asymmetry in the insurance

---

[73] *Id.* at 49.

[74] Ralph A. Winter, *The Liability Crisis and the Dynamics of Competitive Insurance Markets*, 5 YALE J. ON REG. 455, 497 (1988).

marketplace. Finally, the cost of information in the insurance industry is fixed and any reduction in access to information for rate setting purposes would affect smaller firms more adversely than larger firms, increasing the market concentration, and resulting in a less competitive insurance market.[75]

In some states, the Department of Insurance designates a State Rating Bureau to serve as a consumer representative in hearings related to the appropriateness of insurance premium rates. The State Rating Bureau "collects and analyzes statistical data in order to provide technical advice to the Commissioner on oversight of auto, workers' compensation, health and other insurance markets."[76] In addition to State Rating Bureaus, the NAIC model acts also allow for "Insurance Support Organizations" which are organizations that collect loss data and claim costs from insurers "for the purpose of providing the information to an insurance institution or agent for insurance transactions."[77] Examples of some well-known Insurance Support Services are: A.M. Best, ISO – the Insurance Services Office, and CLUE – the Comprehensive Loss Underwriting Exchange.

The NAIC's Insurance Information and Privacy Protection Model Act establishes "standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance support organizations."[78]

---

[75] *Id.* at 498.

[76] Office of Consumer Affairs & Business Regulation, State Rating Bureau, http://www.mass.gov/ocabr/government/oca-agencies/doi-lp/doi-departments/state-rating-bureau.html (last visited Mar. 17, 2014).

[77] NAT'L ASSC. INS. COMM'RS, NAIC INS. INFO. & PRIVACY PROT. MODEL ACT § 2(M) (1992).

[78] NAT'L ASSC. INS. COMM'RS, NAIC INS. INFO. & PRIVACY PROT. MODEL ACT Preamble (1992).

Insurers are then able to request reports from Insurance Support Organizations and use the historical loss data, projected future claim costs and advisory rates in their own underwriting, decision-making, and strategies. Historically, Insurance Support Organizations have been the predominant way in which insurers pool information without running afoul of state law. More recently, however, a federal alternative to the NAIC's Insurance Support Organization information-sharing regime has been proposed in the context of health data collected by recipients of Veterans Benefits, Medicare and Medicaid.

B. Information Sharing and the Federal Government

The Affordable Care Act proposed a number of new incentives and methods for health insurers to share information in ways that substantially differ from the Insurance Support Organization and state rating bureau information collection methodologies. The Centers for Medicare and Medicaid Services are tasked with establishing a national program that collaborates with treating physicians across care settings, aggregating data and sharing information regarding managed health care cost and quality.[79] According to this proposal, Medicare beneficiaries will be eligible to have their claims data shared among industry participants to better serve beneficiaries. This system, proposed at the federal level, offers an alternative to the state level information-sharing platform currently in place.

Such a system of information sharing, regulated by

[79] *New ACO Proposed Rule: Shared Data Could Lead to Privacy, Security Concerns for Participants*, 10 No. 4 GUIDE TO MED. PRIVACY & HIPAA NEWSL. 4, May 2011.

the federal government and authorized under the Affordable Care Act, provides a new way for government and physicians to pool claims data to positively affect a public policy concern. 42 CFR Part 425 proposed the Medicare Shared Savings Program: Accountable Care Organizations. This proposed rule implements § 3022 of the Affordable Care Act and relates to payment of providers participating in Accountable Care Organizations ("ACOs.") It relies on the participation of ACOs in the Shared Savings Program to report claim data and receive feedback from healthcare providers. While such a program is quite dissimilar to the Insurance Support Organization and State Rating Bureau methods detailed above, a federal information-sharing platform possesses some unique advantages unavailable to Insurance Support Organizations and state rating bureaus.

In addition to the Affordable Care Act, the Health Information Technology for Economic and Clinical Health Act ("HITECH") has encouraged healthcare providers to move to electronic health record-keeping systems.[80] The benefits of the HITECH Act include: quicker and more accurate patient information availability, enabling healthcare providers to more easily spot possible health problems; the easy sharing of information among doctors, hospitals and systems, thereby allowing better coordination of care; and increased patient engagement, allowing patients and families to view their own health information.[81] Perhaps most importantly, the HITECH Act provides federal grants to assist states in developing Health Information Exchanges ("HIEs.")[82] These HIEs are intended to capitalize on the ease of access and efficiency

[80] Barry R. Furrow, *Cost Control and the Affordable Care Act: Cramping Our Health Care Appetite*, 13 NEV. L.J. 822, 859 (2013).
[81] *Id.* at 860.
[82] *Id.*

conditions that the electronic medical records provide, as outlined above.

In the healthcare context, a national network of aggregate claims data for rate-calculation may be preferable to Insurance Support Organizations and state rating bureaus due to the fact that a centralized risk adjustment agency can better ensure the integrity and consistency of statistical data and reporting among competing insurance companies.[83] If data from one ACO beneficiary population demonstrates high rates of hospital readmission, that ACO can consider actions to improve discharge coordination among attendant physicians. In the same way, if an HIE is able to determine that a particular set of health care providers in one state's jurisdiction are responsible for inefficient or even negligent medical care, the HIE may be able to identify those concerns more quickly than previously possible.

While the implications of such a federal information sharing system have not yet been fully explored, these systems present a viable alternative to State and Insurance Support Organization information sharing. From a regulatory standpoint, a single government agency or contractor will be able to centralize risk adjustment as well as ensure the integrity of claim data and risk scoring among competing insurers.[84] Similar to the "economies of scale" argument for insurance support organizations and rating bureaus, a federally centralized system of insurance loss data and claim costs avoids duplicative reporting, collection expenses, and storage expenses.

Arguments against a government agency or

---

[83] Mark A. Hall, *Risk Adjustment Under the Affordable Care Act: Issues and Options*, 20 KAN. J.L. & PUB. POL'Y 222, 223 (2011).
[84] *Id.*

contractor for risk calculation and data collection, however, focus primarily on the concerns of insurance companies. Should a government data collection or risk-scoring algorithm inaccurately predict current or future claim costs, insurers may lose profits in the risk-adjustment process.[85] Thus, maintaining the trust of insurance companies that agree to a government sponsored information sharing and risk-calculation program will be of the utmost importance.

V. HOW INFORMATION SHARING MITIGATES MORAL HAZARD

A. Economic Efficiency of Information Sharing

The leading argument for information sharing among insurers is that a federal antitrust exemption facilitates an economically beneficial exchange of information by permitting insurance companies to better evaluate risk and thereby to price premiums more accurately.[86] Despite concerns regarding the potential anticompetitive and price-fixing effects of information sharing among insurers, the social cost of information sharing's reduction in competition within the insurance marketplace is outweighed by the net benefit of more accurately priced insurance premiums, resulting in more insurers competing for the same business.[87]

Any argument which favors information sharing among insurers begins with the basic observation that faulty pricing of insurance products causes harmful economic distortions and inefficiencies in the insurance marketplace. When rates are set too low, harmful behavior by an insured is subsidized through insurance coverage,

---

[85] *Id.*
[86] Macey & Miller, *supra* note 69, at 47.
[87] *Id.* at 48.

resulting in a social burden.[88] Furthermore, excessively low premium rates may result in some firms leaving the insurance industry, thereby creating a residual market wherein many parties who desire insurance find themselves unable to obtain insurance coverage at all.

Conversely, if premium rates are set too high, insurance firms will profit while policyholders pay too much, causing the socially desirable activity that insurance incentivizes to be discouraged. A secondary effect of excessive premiums is that some consumers will be unable to afford insurance at all and will be forced to either self-insure or to cease the activity for which they desire insurance coverage. Finally, high premium rates reduce insurers' incentives to operate efficiently, as the regulated pricing environment of shared loss data forces insurers to resolve claims at a level of efficiency that is beneficial to both the company and the policyholder.[89]

Thus, cooperation between insurance companies facilitates the accurate pricing of risk within the insurance industry.[90] Achieving proper evaluation of risk requires extensive sampling of past occurrences as well as analysis of sample data to predict future losses. When insurers are unable to share loss data, companies are forced to rely solely on historical data they have collected. Such a rule effectively denies smaller insurers the benefits of actuarially sound loss data for ratemaking purposes.[91] It then follows that smaller insurers would be unable to set adequate or competitive premium rates, meaning those

---

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] Francis Achampong, *The McCarran-Ferguson Act and the Limited Insurance Antitrust Exemption: An Indefensible Aberration?* 15 SETON HALL LEGIS. J. 141, 167 (1991).

small insurers risk insolvency or being priced out of the insurance market altogether. Thus, the inability to share data would not only reduce the level of competing companies within the insurance marketplace but may also harm the policyholders of smaller insurance companies that are driven to insolvency.[92]

Of course, evaluation of past occurrences and historical losses can only occur if insurers are willing to share claim data with one another. Information sharing services provide two important functions within the insurance industry. First, information sharing "makes historical loss data available in a sufficiently large sample to provide a high degree of statistic reliability in the analysis."[93] Second, cooperation in the form of loss information sharing achieves economies of scale. The arguments for sharing information within the insurance industry are most persuasive, however, when applied to property and casualty insurance lines where the economic justifications for sharing loss data extend beyond historical claims.[94]

Information sharing among competing insurance companies creates a public benefit by ensuring the accurate assessment of insurance premiums within the industry.[95] Because the price of insurance premiums reflects an insurer's "evaluation of the probable costs of paying claims, as well as the other costs of doing business and a reasonable provision for profit,"[96] knowledge of historical claims data is of the utmost importance for predicting the costs of future losses in property and casualty lines. For

---

[92] *Id.*

[93] Macey & Miller, *supra* note 69, at 48.

[94] *Id.* at 49.

[95] *Id.* at 48 (discussing the need for accurate assessment of insurance premiums especially in property and casualty insurance lines).

[96] *Id.*

many insurance companies with insufficient data, however, the cost of future payable claims may be difficult to assess at the time that an insurance policy is written. Therefore, a proper evaluation of downstream risk must include the "sampling of past occurrences of [the] event insured against, as well as analysis of the historical sample in order predict losses in the future."[97]

Data collection services in the form of insurance rating bureaus typically provide insurers with advisory rates and historical loss data in addition to prospective loss analyses to project the cost of future claims. This makes the data collection function of insurance rating bureaus important for three reasons. First, prospective loss analysis utilizes information sharing to estimate the future cost of claims made on past loss data. Second, trend analysis takes into account the economic and legal changes, which may affect the future cost of claims and forecasts future losses based on information that historical loss data alone may be unable to predict.[98] Finally, the dissemination of historical and projected loss data through insurance rating bureaus achieves economies of scale by performing the data sampling and analysis functions for all insurance companies underwriting a certain type of coverage, thereby reducing the cost of acquiring information for all insurers within in particular jurisdiction and or line of business. [99]

Therefore, collective investment in shared information is economically efficient within the insurance industry. If information sharing were prohibited, numerous inefficiencies would arise. Pooling and sharing loss data is efficient because it treats information as a public good, as

---

[97] *Id.*
[98] *Id.* at 50.
[99] *Id.* at 48.

the use of information by one firm does not preclude the use of the same information by another. Given expenditures for information, increased access to loss data ensures that premiums will more accurately reflect the aggregate information that all firms share, thus avoiding replication of information expenditures and keeping costs low.[100] Second, a decrease in the ability to share claims data will result in firms using less information to set premium rates, thereby exacerbating adverse selection problems caused by informational asymmetry in the insurance marketplace. Finally, the cost of information in the insurance industry is fixed and any reduction in access to information for rate setting would affect smaller firms more adversely than larger firms, increasing the market concentration, and resulting in a less competitive insurance market.[101]

B. Information Sharing to Mitigate Consumer Harm in Cyber-Risk Insurance

As outlined above, differentiated-premium based risk-adjustment and information sharing are two of the primary ways in which insurers are able to provide adequately priced polices to consumers. In the formation of an insurance contract, information flows between both the insurer and insured.[102] Ideally, each party supplies information regarding the factors of risks that affect the insurability of the would-be-consumer.[103] In traditional fire insurance, a company with smoke detector and sprinkler systems that hopes to purchase a fire insurance policy will be eligible for a lower-cost premium based on the

---

[100] Winter, *supra* note 74, at 497.
[101] *Id.* 498.
[102] W. F. Young, *Is Insurance a Niche Business? Reflections on Information as an Insurance Product*, 1 CONN. INS. L.J. 1, 19 (1995).
[103] *Id.*

composite knowledge of the insurance industry that sprinkler systems reduce the likelihood of fire losses and therefore warrant a corresponding reduction in premium.[104] Most importantly, this sharing of information from insurer to insured gives the insurance consumers a financial incentive to achieve reduced risk of loss based on the collective experience of the insurance industry.

In the cyber-risk insurance context, however, the financial incentive to bolster security infrastructure in order to reduce the likelihood of loss achieves a consumer protection goal beyond that raised by fire insurance alone. If an insured possesses a financial incentive to invest in additional information security infrastructure in the form of a reduced policy premium, the insurer will be able to reduce its own likelihood of future loss while the non-party consumer, whose data is stored by the insured, benefits from the increased protection of the insured's additional information security investments.

Unlike fire insurance or other traditional lines of property and casualty insurance, one of the most prominent issues in underwriting cyber-risk coverage is the lack of information regarding frequency, magnitude, and claim costs of both actual and potential data breach incidents.[105] Carriers may be reluctant to share information among one another—or with the government—due to the fact that additional reputational risks may follow any disclosure of a company's data breach claim expenses. Thus, if an independent body were created for insurers to anonymously share information regarding data breaches claim costs, the

---

[104] *Id.*

[105] U.S. DEPT. OF HOMELAND SEC., CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT 18 (Nov. 2012) http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

insurance industry may then be able to offer increasingly industry-specific cyber-risk products that are priced precisely for the levels and types of risk which they cover.

This Article proposes creating an independent, government-sponsored cyber-risk service bureau to collect claims and loss data, identify effective information security measures, and promote the development of increasingly accurate premium rates that will "reward" companies which choose to invest in security infrastructure that adequately protects consumer custodial data as a matter of public good. In this way, a cyber-risk rating bureau creates a market-based incentive to adopt security protocols that permit risk managers to trade off infrastructure investments with insurance premium reductions, thus lowering the cost of a cyber-risk loss for an insured while simultaneously reducing the likelihood and magnitude of those losses for the insurer. By allowing insurers to anonymously share loss data, and by requiring those insurers who do share such data to issue corresponding reductions in premium based on experience-rating adjustments for security metrics that reduce the risk of harm to consumers, insurers will be able to encourage data protection sufficient for public policy.

If cyber-risk insurance carriers are able to rate an insured's cyber-risk policy premiums based on that insured's continuing investments in information security infrastructure, insurers will occupy a unique space in the information security market, with the ability to create a market-based incentive for information security metrics that adequately secure consumer data. In this way, insurers may be in a better position than legislatures and government agencies to promulgate standards which serve to protect not only the financial interests of the risk-bearing insurer but also the consumers who have personal information stored by the insured. Thus, a cyber-risk rating bureau will aid this function of cyber-risk insurance by promoting higher levels of security investments, increasing

the overall levels of safety for information security infrastructure; facilitating standards for best practices to reduce consumer harm as cyber-risk insurance carriers benchmark proper security levels for risk management and consumer protection decision making;[106] and creating an insurance market that results in a greater net social benefit than government regulation alone could produce.[107]

Based on the assumptions outlined in § III.B of this Article, the level of information security infrastructure which a firm needs to retain in order for an insurer to accurately price cyber-risk coverage may be lower than the level of infrastructure needed to adequately protect the consumer information which that firm stores. If this is the case, and insurers writing cyber-risk coverage indemnify an insured for liability resulting from the exposure of protected consumer data, both insurers and consumers will be subject to increased levels of financial harm if an insured chooses to allocate information security funds primarily to insurance coverage rather than to security infrastructure. A cyber-risk rating bureau accomplishes this, and corrects this market failure, by allowing cyber-risk insurance carriers to share information which precisely

---

[106] Kesan et al, *supra* note 11, at 35.

[107] There is a potential for industry capture of any risk rating organization, and a cyber risk rating system should contain a safeguard mechanism to properly serve the interests of both consumers and insurers. The safeguard's purpose would be to ensure that the process of cyber-risk rating itself does not become a function of the industry, subject to the external pressures of the marketplace, and independent of the insured risk. A detailed analysis of how such a safeguard would operate in practice not presented here, but for an analysis and proposal addressing this problem in the mortgage lending context see Jeffrey Manns, *Rating Risk after the Subprime Mortgage Crisis: A User Fee Approach for Rating Agency Accountability*, 87 N.C. L. REV. 1011 (2009).

addresses the relevant risks presented by each insured when underwriting policies. Thus, the availability of loss data and rate-setting information available to insurers though the cyber-risk rating bureau encourages insureds to allocate optimal levels of investment toward infrastructure rather than relying on insurance coverage to offset data breach losses, to the benefit of both the insurer and the consumer.

VI. CONCLUSION

The expansion of the cyber-risk insurance market is likely to continue in the coming years. While the gross written premiums for cyber-risk insurance policies currently stand at the $1 billion dollar mark (up from $800 million in 2011) the cyber-risk insurance market still represents only a tiny fraction of the $247 billion in total direct premiums written in the United States commercial insurance lines market for 2012.[108] As insurers continue to limit cyber-risk coverage under existing policy lines, insurance carriers will be able to move insureds towards comprehensive cyber-risk-specific insurance plans, establishing consistent standards and best practices that improve the ability of insurers to price coverage and underwrite insurance. This Article recommends a government sponsored but independent cyber-risk rating bureau to assist insurers and benefit consumers through the sharing of historical loss data, claim costs, and projected future claims in order to ensure the accuracy of cyber-risk coverage pricing and to reward the adoption of security standards that benefit consumers. In this way, insurers may

[108] TREAS. DEPT., REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 at 26 (2013); BETTERLEY RISK CONSULTANTS, INC., CYBER/PRIVACY INSURANCE MARKET SURVEY – 2012, 6 (Jun. 2012), http://betterley.com/samples/cpims12_nt.pdf.

be able to implement safety standards to encourage consumer protection of electronic data in the rapidly evolving landscape of information security's diverse risk sectors in a manner that government regulation alone is unable to achieve.[109]

[109] Donald & Strutt, *supra* note 5, at 2953.