1-1-2021

Five Approaches to Insuring Cyber Risks

Christopher C. French
Penn State Law

FIVE APPROACHES TO INSURING CYBER RISKS

CHRISTOPHER C. FRENCH*

Cyber risks are some of the most dangerous risks of the twenty-first century. Many types of businesses, including retail stores, healthcare entities, and financial institutions, as well as government entities, are the targets of cyber attacks. The simple reality is that no computer security system is completely safe. They all can be breached if the hackers are skilled enough and determined. Consequently, the worldwide damages caused by cyber attacks are predicted to reach $10.5 trillion by 2025. Insuring such risks is a monumental task.

The cyber insurance market currently is fragmented with hundreds of insurers selling their own cyber risk insurance policies that cover different types of cyber risks. This means the purchasers of cyber insurance must be experts in both insurance and cyber security in order to make a knowledgeable purchase. And, even knowledgeable purchasers of cyber insurance can only obtain limited coverage for cyber risks. This is because the insurance is sold on a named peril, as opposed to all-risk, basis and the policies contain numerous exclusions. Cyber policies also have relatively low policy limits in comparison to other lines of insurance and the enormity of the risks presented.

This Article explores ways the cyber insurance market could be improved. In doing so, it analyzes the current cyber insurance market, including the history of cyber insurance and the challenges that insuring cyber risks present. The Article then offers five different approaches to insuring cyber risks moving forward that address many of the problems with the current cyber insurance market. Ultimately, the Article concludes the fifth approach, the novel "All-Risk Private-Public" approach, would be the best one.

* Christopher C. French is a Professor of Practice at Penn State Law; J.D., Harvard Law School; B.A., Columbia University. The author gratefully acknowledges the legal research contributions of Emory Robertson to this Article. The author also thanks Jay Feinman, Bob Jerry, Erik Knutsen, Dan Schwarcz, and Jeff Stempel for providing thoughtful comments on earlier drafts of the Article.

INTRODUCTION

Cyber risks have taken their place with climate change and natural catastrophes as some of the most dangerous risks of this century. The former FBI Director Robert Mueller has described the state of IT security as follows: "[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1] In short, no IT security system is completely safe. They all can be breached if the hackers are skilled and determined enough. Many types of businesses, including

1. Robert Mueller, Dir., Fed. Bureau of Investigation, Address at the RSA Cyber Security Conference (Mar. 1, 2012), https://www.americanrhetoric.com/speeches/robertmuellerrsacyberconference2012.htm.

retail stores, healthcare entities, and financial institutions, as well as government entities, are the targets of cyber attacks.[2]

Cyber attacks can take many forms. A few of the most common ones are: denials of service, ransomware, phishing scams, and computer hacks in which a third party gains unauthorized access to a computer system.[3] New types and means of cyber attacks are constantly emerging.

There are many potential negative consequences of a cyber attack. Intellectual property may be stolen. Customers' credit card information or social security numbers may be stolen. A company's computer system or website may be paralyzed, resulting in lost business. The reputations of the hacked companies are also often tarnished due to the public's loss of trust in the companies' security systems.[4]

The economic damage caused by cyber attacks is almost unfathomable. By 2025, the worldwide damage caused by cyber attacks is predicted to reach $10.5 trillion.[5] In the past few years, the annual damages associated with just ransomware claims have increased from $325 million to billions, with a projected amount of $20 billion in 2021.[6]

The number of impacted entities and the list of companies compromised by cyber attacks in recent years is incredible. In late 2016, for example, Uber Technologies suffered a system breach that resulted in hackers obtaining personal information for 57 million customers.[7] In 2017, the NotPetya malware caused more than $10 billion in estimated damages.[8] Also in 2017,

---

2. *See, e.g.*, Margaret A. Reetz, Lauren B. Prunty, Gregory S. Mantych & David J. Hommel, *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN ST. L. REV. 727, 732 (2018); Erik S. Knutsen & Jeffrey W. Stempel, *The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses*, 122 PENN ST. L. REV. 645, 649 (2018).

3. *See generally* Reetz et al., *supra* note 2, at 732–35.

4. *See id.*; Toni Scott Reed, *Cybercrime and Technology Losses: Claims and Potential Insurance Coverage for Modern Cyber Risks*, 54 TORT TRIAL & INS. PRAC. L.J. 153, 164 (2019) ("Target recorded a fourth-quarter profit down forty-six percent from the previous year and reported a significant decline in traffic and sales after the breach became public.").

5. *See* Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually By 2025*, CYBERSECURITY VENTURES (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

6. *See* Steve Morgan, *Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019*, CYBERSECURITY VENTURES (Nov. 14, 2017), https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/; Ivana Vojinovic, *Ransomware Statistics in 2020: From Random Barrages to Targeted Hits*, DATAPROT (Nov. 13, 2019), https://dataprot.net/statistics/ransomware-statistics/.

7. *See* Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html.

8. *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devasting Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Selena Larson, *The Hacks that Left Us Exposed in 2017*, CNN

the WannaCry malware crashed over 300,000 computer systems across 150 countries.[9] Equifax was also hacked in 2017, which compromised the data, including social security numbers, of 145 million people.[10] In late 2018, Marriott International, the world's largest hotel company, reported a data breach that affected 383 million guests.[11] With the constant stream of reports of new cyber attacks, the once widely discussed Target[12] and Sony[13] breaches that occurred just a few years ago are fading from memory. Reportedly, only a fraction of Sony's and Target's losses were covered by insurance.[14]

Much of the existing cyber insurance scholarship explores ways for cyber insurers to serve as private regulators of cyber security practices by creating premium incentives for certain system security practices and using insurers' third-party system security experts to provide security advice to insured businesses.[15] Insurers generally can have non-governmental, regulatory effects on policyholder behavior by, for example, providing premium incentives for risk-reducing behavior, so discussing insurance's potential role in that regard is certainly valuable.[16] Such scholarship does not, however, address the fundamental question facing the cyber insurance

MONEY (Dec. 20, 2017, 9:11 AM), https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

9. *See* Larson, *supra* note 8.

10. *Id.*

11. *See* Peter Holley, *Marriott: Hackers Accessed More Than 5 Million Passport Numbers During November's Massive Data Breach*, WASH. POST (Jan. 4, 2019), https://www.washingtonpost.com/technology/2019/01/04/marriott-hackers-accessed-more-than-million-passport-numbers-during-novembers-massive-data-breach/.

12. *See* Reuters, *Target Settles 2013 Hacked Customer Data Breach for $18.5 Million*, NBC NEWS (May 24, 2017, 10:49 AM), https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031 (stating Target had approximately $202 million in damages).

13. *See* Steve Kroft, *The Attack on Sony*, CBS NEWS (Apr. 12, 2015), https://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/ ("More than 3,000 computers and 800 servers were destroyed by the attackers after they had made off with mountains of business secrets, several unreleased movies, unfinished scripts, and the personal records of 6,000 employees . . . .").

14. *See* 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 29.01[2][a][ii] (2020).

15. *See, e.g.*, JOSEPHINE WOLFF, CYBER-INSURANCE POLICY: RETHINKING INTERNATIONAL RISK FOR THE INTERNET AGE (MIT Press, forthcoming) (manuscript at 231–32) (arguing insurers should serve as cyber security regulators to incentivize policyholders to increase system security); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417, 417 (2018) (arguing cyber insurers already are acting as regulators of cyber security); Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1534 (2017) (arguing cyber insurers are uniquely positioned to regulate cyber security).

16. *See generally* Omri Ben-Shahar and Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 196, 206 (2012) (discussing the use of insurance as a non-governmental regulator of policyholders' behavior).

market today, which is: What is the best approach to insuring cyber risks that will allow insurance to effectively transfer the risk of cyber losses from individual policyholders to entities that are financially able to bear the risk of those losses?

This Article addresses that fundamental question. In doing so, it discusses five different approaches to insuring cyber risks. Ultimately, the Article proposes a novel "All-Risk Private-Public" approach to insuring cyber risks that combines the best attributes of private cyber insurance with public insurance by proposing that private insurers sell "all-risk"[17] cyber policies with the federal government serving as an excess insurer or reinsurer above a stop-loss amount like it currently does for terrorism risks under the Terrorism Risk Insurance Program ("TRIA").[18]

The proposed "All-Risk Private-Public" approach would address the numerous challenges of insuring cyber risks. One of those challenges is that cyber risks are different from other risks in one significant way: Cyber attacks can come from anywhere in the world, at any time, and can impact thousands of businesses at approximately the same time, making cyber losses correlated risks.[19] If someone wants to steal the blueprints for an invention from a company's safe, for example, then a person has to show up where the safe is located in order to steal the blueprints. With a cyber attack, a hacker sitting in front of a computer in Latvia at 2:00 AM can break into the business's computer system in the United States and steal a copy of the blueprints.

Another challenge is that the legal obligations regarding cyber attacks for insured entities are ever-changing and increasing, so attempting to insure such obligations is akin to shooting a moving target. For example, although not required two decades ago, a hacked company now must notify the people potentially affected by a cyber attack, disclose the attack on its financial

17. "All risk" property insurance covers all risks of loss except for perils specifically excluded. *See* PETER J. KALIS, THOMAS M. REITER & JAMES R. SEGERDAHL, POLICY HOLDER'S GUIDE TO THE LAW OF INSURANCE COVERAGE § 13.02[B] (2009).

18. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002) (codified as amended in various sections of 15 U.S.C.) (TRIA is used in this Article to refer to the Terrorism Risk Insurance Act and the Terrorism Risk Insurance Program collectively); *see infra* Section III.D.

19. Correlated risks are perils that cause numerous losses to the pool of insureds at approximately the same time. *See Correlated Risks*, WORLD FIN. (June 30, 2010), http://www.worldfinance.com/home/risk-encyclopaedia/correlated-risks [https://perma.cc/CQ3D-865A]; Véronique Bruggeman, Michael Faure & Tobias Heldt, *Insurance Against Catastrophe: Government Stimulation of Insurance Markets for Catastrophic Events*, 23 DUKE ENV'T & POL'Y F. 185, 187 (2012); J. David Cummins, *Should the Government Provide Insurance for Catastrophes?*, 2006 FED. RES. BANK ST. LOUIS REV. 337, 342–43 (2006); Adam F. Scales, *A Nation of Policyholders: Governmental and Market Failure in Flood Insurance*, 26 MISS. COLL. L. REV. 3, 10–11 (2006).

statements, defend claims asserted against it related to the company's failure to protect others' personal data, and respond to government investigations.[20]

Yet an additional challenge for insuring cyber risks is determining how to accurately price cyber insurance to make sure it is being sold at actuarially sound prices. Accurate claims data is the foundation of actuarially sound premium pricing but only a paltry amount of data exists for cyber risks and losses.[21] So, when attempting to price cyber insurance, insurers must do so without the benefit of the decades' worth of claims data that exists for other lines of insurance.[22]

Not only do they lack their own claims data, but insurers generally cannot even rely upon the claims data being generated by other insurers because, in the unlikely event that their competitors were willing to share such data—which generally is considered confidential and proprietary—the data would not be particularly useful.[23] Unlike other lines of insurance, cyber insurers have developed their own cyber policy forms instead of using a uniform industry-developed form, so the hundreds of insurers selling cyber insurance are not actually selling the same product.[24] With numerous policy forms using different policy language and providing different coverages, it is like comparing apples to oranges when it comes to the claims data—one type of cyber loss may be covered under one insurer's policy form, but it would not be covered under another's. Consequently, the claims data that one

20. *See, e.g.*, Reetz et al., *supra* note 2, at 733–34.

21. Insurers' actuaries use decades' worth of claims data related to other lines of insurance collected by the entire insurance industry through the Insurance Services Office, Inc. ("ISO") to create a risk profile for each prospective insured. *See, e.g.*, JAY M. FEINMAN, DELAY, DELAY, DENY, DEFEND: WHY INSURANCE COMPANIES DON'T PAY CLAIMS AND WHAT YOU CAN DO ABOUT IT 14 (2010) (explaining how insurers use claims data); Peter Siegelman, *Adverse Selection in Insurance Markets: An Exaggerated Threat*, 113 YALE L.J. 1223, 1245, 1248–49, 1251–52, 1263 (2004) (discussing the sources of informational asymmetry between insurers and insureds); Ben-Shahar & Logue, *supra* note 16, at 209–11 (examining insurers' informational advantages regarding insureds' risks).

22. *See* WOLFF, *supra* note 15, at 5 ("[I]nsurance firms lacked the decades of claims data that informed the actuarial models for their other insurance offerings . . . ."); Hurwitz, *supra* note 15, at 1544 ("A key reason that it is difficult to determine an accurate measure of damages is that there is a lack of actual data about the consumer costs of data breaches."); Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5(1) J. CYBERSECURITY 1, 12 (2019) ("[Insurers] have no historic or credible data upon which to make reliable inferences about loss expectations . . . .").

23. *See, e.g.*, FEINMAN, *supra* note 21, at 38–40 (discussing how insurance companies closely guard data on lawsuits for unfair claims practices); Daniel Schwarcz, *Transparently Opaque: Understanding the Lack of Transparency in Insurance Consumer Protection*, 61 UCLA L. REV. 394, 415–20 (2014) (discussing the need for the disclosure of insurers' claims payment practices in order to allow consumers to make more informed insurance purchasing decisions).

24. *See, e.g.*, 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[3][d] ("There is a large array of specialty cyber products on the market, with each policy varying greatly from insurer to insurer.").

insurer generates is nearly useless to other insurers because the data is not predictive of other insurers' likely claims experience.

An additional challenge is that, unlike the policy forms used in other lines of insurance—such as Commercial General Liability ("CGL") insurance, which has been sold since the 1940s and has been interpreted by numerous courts[25]—the policy language contained in cyber policies generally has not been interpreted by the courts because cyber policy forms are relatively new and, as mentioned, the coverages they provide are not uniform.[26] Without court decisions interpreting cyber insurance policy language, insurers do not know which cyber losses will actually be covered by their policies regardless of the insurers' intent with respect to the meaning of the policy language. Collectively, all these challenges result in insurers guessing to some extent when they establish the price of the premiums for cyber insurance.[27]

In the face of these formidable challenges, the existing cyber insurance market nonetheless is growing rapidly. In 2019, insurers collected approximately $2.5 billion in premiums.[28] Between 2015 and 2019, the number of insurers selling cyber insurance increased from 322 to 580.[29]

The dramatic growth of the cyber insurance market is due, in part, to the high profit margins associated with cyber insurance—the profit margin for cyber policies is approximately sixty-five percent, while the average profit margin for other lines of insurance is approximately thirty-eight percent.[30] These sizeable profit margins are generated by the high premiums charged in exchange for the relatively low amounts of coverage provided—the premium rates are three times higher than for other lines of liability insurance and six times higher than for other lines of property insurance.[31] Thus, as currently structured, the cyber insurance market works well for insurers by providing them high profit margins in exchange for the provision of limited insurance.

This Article discusses ways to fulfill the needs of both insurers and policyholders by considering the enormous challenges cyber risks present

25. *See, e.g.*, *infra* Section I.B.

26. Knutsen & Stempel, *supra* note 2, at 651 (describing the policy language in cyber policies as "untested"); 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[3][d] ("Because cyber policies are still relatively new, courts have only just begun to tackle the interpretive issues raised by these policies.").

27. *See, e.g.*, Romanosky et al., *supra* note 22, at 12 (some insurers basically "estimated or guessed" in establishing premium prices).

28. *See* FED. INS. OFF., U.S. DEP'T TREASURY, ANNUAL REPORT ON THE INSURANCE INDUSTRY 68 (Sept. 2020), https://home.treasury.gov/system/files/311/2020-FIO-Annual-Report.pdf [hereinafter FIO ANNUAL REPORT].

29. *Id.* at 69.

30. *See* WOLFF, *supra* note 15, at 229.

31. *See* Hurwitz, *supra* note 15, at 1537.

from a risk management perspective. In doing so, it proceeds in three parts. Part I discusses the history of cyber insurance.[32] Part II discusses the challenges associated with insuring cyber risks.[33] Part III provides five approaches the cyber insurance market could take moving forward: (1) maintain the status quo and let the market dictate the best approach to insuring cyber risks; (2) have traditional CGL policies and "all risk" property policies cover cyber risks; (3) sell cyber insurance as standalone insurance but use separate, uniform policy forms for third-party liability risks and first-party risks; (4) have the federal government serve as a stop-loss excess insurer or reinsurer for cyber risks by using the Terrorism Risk Insurance Program ("TRIA") as a template for structuring the program; and (5) sell cyber insurance as standalone insurance using separate, uniform policy forms for third-party risks and first-party risks, with the federal government providing excess insurance or reinsurance above established stop-loss points.[34] The Article concludes by arguing that the fifth approach, the novel All-Risk Private-Public approach, is the best one.[35]

I. THE CYBER INSURANCE MARKET

A. The Creation and History of Cyber Insurance

The first insurance policies that would be considered cyber insurance today were created in the mid-1990s by an insurance broker, Steven Haase, because his clients—the first online bank and a network security company—were doing a substantial amount of business on the Internet.[36] As the Internet became commercialized, Haase saw the need for a liability policy for companies doing business on the Internet.[37] So, Haase worked with American International Group, Inc. ("AIG") to develop a cyber risk policy, the Internet Security Liability Policy, which AIG began selling it in 1997.[38]

Early cyber policies often used Errors and Omissions ("E&O") policy forms for financial institutions as templates, and only provided coverage for third-party liabilities.[39] First-party coverage for a policyholder's own losses

32. *See infra* Part I.

33. *See infra* Part II.

34. *See infra* Part III.

35. *See infra* Conclusion.

36. *See* Andrea Wells, *What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now*, INS. J. (Mar. 1, 2018), https://www.insurancejournal.com/news/national/2018/03/01/481886.htm.

37. *Id.*

38. *Id.*

39. *See* Reetz et al., *supra* note 2, at 731; Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, 2 J. CYBER POL'Y 53, 53 (2017) ("Cyber insurance as a stand-alone product began to

caused by cyber attacks was not covered by the initial cyber policies.[40] Nor was coverage provided for cyber losses caused by a policyholder's own employees.[41] When studies revealed that approximately fifty percent of cyber hacks were caused by disgruntled employees, cyber coverage was expanded to cover employee-caused losses as well.[42]

The addition of coverage for losses caused by disgruntled employees is exemplary of how cyber insurance has evolved since its initial creation. Over time, cyber insurance has evolved to cover new cyber risks as they have emerged, and to cover new liabilities for data breaches as the laws in the area have developed.[43] For example, after significant network extortion events occurred in 2004, cyber coverage was expanded to cover such events.[44] After customer breach notification laws were created, with California being the first state to do so in 2003, cyber policies began covering the costs associated with complying with such laws.[45]

One of the challenges in the area of cyber security is that there is neither a general set of federal data security laws that apply to all businesses nor established standards for the best cyber security practices.[46] Instead, there is a patchwork quilt of data security laws that apply to specific industries to address specific concerns and a variety of sources that disagree on the best cyber security practices. For example, there are specific laws that apply to

take off in response to Y2K concerns and was designed to fill gaps in traditional property and casualty (P&C) products. The number of insurance providers offering the product gradually expanded, although it remained a niche speciali[z]ed market during these early days." (footnote omitted)); Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INS. J. (Sept. 22, 2014), https://www.insurancejournal.com/magazines/mag-eatures/2014/09/22/340633.htm ("[T]he original policies covered only third party suits arising from breaches originating from outside the company. . . . The markets offering coverage at that time responded by broadening coverage to cover loss to the entity . . . .").

40. Reetz et al., *supra* note 2, at 730–31.

41. *See* Brown, *supra* note 39.

42. *Id.*

43. *See, e.g.*, WOLFF, *supra* note 15, at 120–21.

44. *Id.*

45. *Id.*; Camillo, *supra* note 39, at 54. Today, all fifty states have customer breach notification laws. *See, e.g.*, 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[1]; Reed, *supra* note 4, at 162. The Securities and Exchange Commission ("SEC") now also requires companies to disclose major hacking incidents. *See, e.g.*, Reed, *supra* note 4, at 164; WOLFF, *supra* note 15, at 12.

46. *See, e.g.*, Hurwitz, *supra* note 15, at 1516 ("In the United States there is no general law of data security. Rather, there is a sector-by-sector approach to regulating specific security concerns."); WOLFF, *supra* note 15, at 13 ("[T]he federal government remained relatively hands-off when it came to mandating security best practices or clarifying the expectations for what companies must do to avoid liability for cybersecurity incidents.").

the security of personal financial data,[47] personal health data,[48] and consumer credit data,[49] but there are no general cyber security laws. Without a comprehensive set of cyber security requirements or standards, it is difficult for insurers and policyholders to know whether a policyholder is employing the best cyber security measures or taking the appropriate steps to comply with data security laws.

While the coverages under cyber policies have evolved to cover new cyber liabilities and risks as they have emerged, the insurance industry simultaneously has attempted to eliminate coverage for cyber risks under traditional liability and property policies, such as CGL policies and commercial all-risk property policies.[50] For example, over the past two decades, the Insurance Services Office, Inc. ("ISO")[51] has repeatedly revised its CGL policy form to eliminate coverage for "electronic data" losses.[52] In 2001, ISO changed the definition of what constituted covered "property damage" under CGL policies to make it clear that lost electronic data is not covered because:

> [E]lectronic data is not tangible property. . . . [E]lectronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CDROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.[53]

In 2004, ISO added an exclusion in CGL policies for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[54]

---

47. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (applying to the financial services industry).

48. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (applying to patients' health information).

49. *See* 15 U.S.C. § 1681 (2013) (setting forth the protections of consumers' rights to privacy under the Fair Credit Reporting Act).

50. *See infra* Section I.B.

51. ISO is an influential organization within the insurance industry that provides a variety of services to many insurers. *See* U.S. Fire Ins. Co. v. J.S.U.B., Inc., 979 So. 2d 871, 879 n.6 (Fla. 2007). One of ISO's primary functions is to draft policy forms that are then submitted to state insurance regulators for approval. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 772 (1993). As a provider of services to approximately 1,400 property and casualty insurers, ISO "is the almost exclusive source of support services in this country for CGL insurance." *Id.* As a result, "most CGL insurance written in the United States is written on [ISO] forms." *Id.*

52. *See, e.g.*, Reed, *supra* note 4, at 174.

53. *Id.* (quoting ISO form CG 00 01 10 01).

54. ISO Policy Form CG 00 01 12 04, Exclusion P.

ISO has also added other exclusions to its CGL policy form that were designed to eliminate coverage for the various types of cyber losses as they have emerged. For example, in 2014, ISO added an exclusion for liabilities due to the disclosure of confidential or personal information:

> This insurance does not apply to:
> . . .
> "Personal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of non public [sic] information.
> This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.[55]

ISO similarly has attempted to eliminate coverage for cyber losses under its commercial all-risk property policy form.[56] For example, since 2012, the ISO policy form has expressly disclaimed coverage for lost electronic data. Notably, the form states:

> Covered Property does not include:
> . . .
> Electronic data . . . . Electronic data means information, facts or computer programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), on hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other repositories of computer software which are used with electronically controlled equipment.[57]

Similarly, with respect to business interruption losses caused by cyber attacks (e.g., the lost revenues a company suffers because the company's website becomes paralyzed by a cyber attack), ISO's all-risk property policy form seeks to disclaim coverage for such losses, stating, "[c]overage for Business Income does not apply when a 'suspension' of 'operations' is

55. Reed, *supra* note 4, at 175–76; ISO Policy Form CG 21 07 05 14 (2014).

56. *See, e.g.*, WOLFF, *supra* note 15, at 125 ("[I]n 2003, the insurance industry developed the Institute Cyber Attack Exclusion Clause . . . [which] became popular with property insurers, enabling them to deny coverage for malicious cybersecurity incidents.").

57. ISO Policy Form CP 00 10 10 12, § A.2.n, https://www.propertyinsurancecoveragelaw.com/files/2017/05/CP00101012.pdf.

caused by destruction or corruption of electronic data, or any loss or damage to electronic data . . . ."[58]

In sum, insurers have increased the number and scope of the exclusions directed at cyber risks under traditional liability and property policies while they created and expanded the coverage provided under cyber policies. Doing so, of course, has allowed insurers to now sell an additional policy to cover losses that arguably would have been covered under either a CGL policy or an all-risk property policy before the data loss and other exclusions were added to them.

B. The Current Cyber Insurance Market

Today, cyber insurance is sold as either a standalone policy or as an add-on coverage to CGL and property policies.[59] There are now at least 580 insurers selling cyber insurance, but the top ten insurers account for approximately 64% of the market.[60] Between 2015 and 2018, premium sales for cyber insurance increased by 479%.[61] In 2019, insurers collected approximately $2.5 billion in cyber insurance premiums.[62] The worldwide cyber insurance market today is largely limited to sales in the United States, with the U.S. market accounting for 90% of cyber insurance sales and Europe accounting for between 5–9%.[63]

Cyber policies today typically provide both first-party and third-party coverage.[64] Coverage is provided on a "named peril" basis, as opposed to "all-risk,"[65] with the various coverages often sold à la carte. Under named

58. ISO Policy Form CP 00 30 06 07, § A.4.a, https://www.propertyinsurancecoveragelaw.com/wp-includes/ms-files.php?file=file/CP%2000%2030%2006%2007.pdf.

59. *See* 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[4][g]; Knutsen & Stempel, *supra* note 2, at 650; Reed, *supra* note 4, at 170; WOLFF, *supra* note 15, at 4.

60. *See* FIO ANNUAL REPORT, *supra* note 28.

61. WOLFF, *supra* note 15, at 155.

62. FIO ANNUAL REPORT, *supra* note 28, at 68.

63. *See id.* at 203.

64. *See, e.g.*, Reetz et al., *supra* note 2, at 738; WOLFF, *supra* note 15, at 157 ("The most commonly covered cyber-related losses . . . include[] the cost of legal claims, settlement costs, public relations services, notifying affected individuals about data breaches, computer forensic investigations, business income losses, data restoration, and data extortion expenses.").

65. Under all-risk policies, all risks are covered unless a risk is specifically excluded. *See* 3 NEW APPLEMAN INSURANCE LAW PRACTICE GUIDE § 31.06[2][d] (2020) (explaining the differences between "all risk" and "named perils" coverage); COUCH ON INSURANCE § 148:50 (3d ed. 2020) (discussing the increasing use of "all risk" policies and explaining that such policies cover all risks unless a risk is specifically excluded).

peril insurance, only the risks specifically listed are covered.[66] Available first-party coverages include: forensic investigation costs to discover the cause of a breach, costs to restore service and restore lost data, the costs of losses due to cybercrimes (e.g., ransomware, phishing, and denial of service attacks), and the replacement of lost revenue due to business interruptions.[67] Available third-party liability coverages include: costs to comply with breach notification laws, fines for failure to comply with breach notification laws, credit monitoring costs for affected customers, reimbursement costs paid to financial institutions for fraudulent purchases, and the costs to compensate third parties for stolen electronic data or intellectual property.[68]

Some scholars, such as Professor Josephine Wolff, have argued that, although some cyber policies currently provide such coverage, cyber insurance should not cover losses associated with certain cybercrimes (e.g., ransomware losses) because providing such coverage only encourages and rewards criminal behavior, such as kidnapping.[69] Yet, insurance already is available and allowed to pay ransoms for kidnappings.[70] Allowing cyber

66. *See, e.g.*, PETER J. KALIS, THOMAS M. REITER & JAMES R. SEGERDAHL, POLICYHOLDER'S GUIDE TO THE LAW OF INSURANCE COVERAGE § 13.02[A] (1st ed. 1997 & Supp. 2020).

67. *See* Reed, *supra* note 4, at 165 ("First-party risks include the cost of replacing data that are lost through corruption of the system, loss of stolen property, the cost of replacing systems that become inoperable, and the labor expenses from reentering data. . . . Finally, there may be risks of loss of the insured's money, as well as lost income, consequential damages, and crisis management costs." (footnotes omitted)); *see also* 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[2][a][ii] n.48; Romanosky et al*., supra* note 22, at 5.

68. *See* Reed, *supra* note 4, at 166 ("Third-party losses are losses that result when cybercrime damages or destroys data or steals information of a third party that is in the care, custody, or control of the victim of the breach, that is, the insured. These losses are typically sustained from the following general cybercrimes: intrusion into computer systems to steal bank account numbers, transmission of a computer virus through the insured's computer system into the system of a third party . . . and failure to give notice to a third party of the intrusion in violation of statute, regulation, or contract." (footnotes omitted)); *see also* 4 NEW APPLEMAN INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[2][b]; Romanosky et al., *supra* note 22, at 6–7.

69. *See* WOLFF, *supra* note 15, at 225–27; Gideon Parchomovsky & Peter Siegelman, *The Paradox of Insurance*, PENN L.: LEGAL SCHOLARSHIP REPOSITORY 1, 31 (Mar. 9, 2021) ("The bottom line is that while it's difficult to prove that kidnap insurance increases kidnappings, the limited available evidence is entirely consistent with that possibility, and some theoretical models predict it.").

70. *See* Amy Bell, *A Guide to Kidnap and Ransom Insurance Coverage*, INVESTOPEDIA (Sept. 19, 2021), https://www.investopedia.com/articles/personal-finance/062915/guide-kidnap-ransom-insurance-coverage.asp ("Kidnap and ransom coverage is often provided as part of a corporate insurance portfolio."); *What is Kidnap & Ransom Insurance?*, TRAVELERS INS. https://www.travelers.com/professional-liability-insurance/kidnap-ransom (last visited Sept. 28, 2021) ("Kidnap & Ransom insurance policies provide coverage typically for monies paid to kidnappers or extortionists, loss of ransom in transit and other expenses incurred as a result of a kidnapping."); *Kidnap, Ransom & Extortion Insurance*, AIG, https://www.aig.com/business/insurance/management-liability/kidnap-ransom-and-extortion (last

insurance to cover ransomware payment demands is conceptually no different. Indeed, society has a greater interest in discouraging kidnappings than computer hijacks, yet insurance is permitted to cover kidnapping ransom payments.[71] Further, the concern and argument that insurance should not be allowed to cover crimes because it incentivizes criminal behavior also applies to many other types of property insurance, including homeowners insurance and auto insurance, yet they too are allowed to cover a policyholder's losses caused by criminal behavior.[72]

Arguments against allowing coverage for the compensation of victims of crime also overlook the primary purpose of insurance, which is to compensate victims for their losses, not to indirectly regulate third parties' criminal behavior.[73] Forcing victims of crime to suffer losses at the hands of criminals for crimes such as ransom demands may have some deterrent effect on criminal behavior to the extent it removes a source of financial benefits available to pay for ransomed property, but there are better ways to deter criminal behavior. For example, one would expect that the risk of incarceration would be a stronger deterrent to crime than the risk the victim will not have adequate financial resources to make the crime worthwhile to the criminal if insurance proceeds are unavailable.[74] In short, the arguments in favor of treating cybercrimes differently than other crimes when it comes to insurance are not persuasive.

---

visited Sept. 28, 2021) ("Coverage for a range of crisis perils, including kidnapping, extortion, assault (known as active shooter or workplace violence) and more.").

71. *See* WOLFF, *supra* note 15, at 226 ("[T]he stakes of ransomware are often—though not always—lower than in cases of kidnapping, where individuals' lives are presumably at stake.").

72. *See, e.g.*, KENNETH S. ABRAHAM & DANIEL SCHWARCZ, INSURANCE LAW AND REGULATION 196, 645 (6th ed. 2015) (reproducing ISO's auto and homeowners insurance policy forms that cover losses caused by, among other things, "Malicious mischief or vandalism" and theft).

73. *See* Tom Baker, *Containing the Promise of Insurance: Adverse Selection and Risk Classification*, 9 CONN. INS. L.J. 371, 377 (2003) (explaining how the concept of insurance is predicated on the existence of a large number of fortunate insureds' premiums paying for the losses of the unfortunate few); Deborah A. Stone, *Beyond Moral Hazard: Insurance as Moral Opportunity*, 6 CONN. INS. L.J. 11, 16 (1999) (noting that the basic premise of insurance is collective responsibility for harms that befall individuals); Christopher C. French, *Debunking the Myth that Insurance Coverage is Not Available or Allowed for Intentional Torts or Damages*, 8 HASTINGS BUS. L.J. 65, 97 (2012) (discussing the lack of empirical evidence to support the argument that intentional misconduct would be deterred by the lack of insurance to cover the liabilities that arise from such misconduct); Ranger Ins. Co. v. Bal Harbour Club, Inc., 509 So. 2d 945, 947 (Fla. Dist. Ct. App. 1987) ("The proposition that insurance taken out by an employer to protect against liability under Title VII will encourage violations of the Act is . . . speculative and erroneous.").

74. *See, e.g.*, 18 U.S.C. § 1348 (authorizing prison sentences of as high as twenty-five years under Sarbanes-Oxley for misrepresentations regarding securities despite D&O insurance being allowed to cover shareholder fraud claims).

The issue of insuring cybercrimes raises another somewhat unusual aspect of the current cyber insurance market—some cyber policies cover crimes while other cyber policies do not.[75] Unlike many lines of insurance, such as CGL and auto insurance, there is no standard cyber risk policy form.[76] The cyber insurance market is fragmented with hundreds of insurers selling cyber policies using their own policy forms.[77] Despite being sold for more than twenty years, additional insurers continue to enter the cyber insurance market using their own policy forms, with many of them providing dramatically different coverages.[78]

Currently, insurers also offer only limited coverage under cyber policies in exchange for very high premium prices.[79] Insurers charge as much as $42,000 for $1 million in coverage.[80] To provide some context regarding how expensive that is, a person can buy $1 million of coverage under an umbrella insurance policy for auto and homeowners claims for between $150

75. *Compare The Hartford CyberChoice 2.0: Information Technology Liability and Risk Policy*, § I.E., HARTFORD (2008), https://safeguardme.com/wp-content/uploads/2013/10/PDF3.pdf [hereinafter *The Hartford CyberChoice 2.0*] (covering cyber extortion losses), *with Will Cyber Insurance Cover You After a Ransomware Attack?*, CONTINUUM GRC (Mar. 31, 2017), https://continuumgrc.com/cyber-insurance-ransomware/ ("[I]f a policy does not specifically include 'extortion coverage,' ransomware won't be covered at all.").

76. *See, e.g.*, 1 NEW APPLEMAN PENNSYLVANIA INSURANCE LAW PRACTICE GUIDE § 7.22[1] (2020) ("Cyber insurance is not standard. There is a wide variety of specialty cyber insurance on the market, with policies varying greatly from insurer to insurer."); 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.04[1][b][i] ("[T]here is little uniformity among cyber policies, and there is no such thing as a 'standard' cyber policy."); Reed, *supra* note 4, at 174 ("An important consideration with cyber-risk policies is that the policies are not standardized."); ABRAHAM & SCHWARCZ, *supra* note 72, at 437–54, 638–50 (reproducing ISO's standard CGL and auto policy forms used by most insurers).

77. *See supra* notes 24, 28–29 and accompanying text.

78. *See, e.g.*, 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[3][d] ("There is a large array of specialty cyber products on the market, with each policy varying greatly from insurer to insurer."); Reed, *supra* note 4, at 174 ("The policies provide similar coverage, but the policies can vary significantly from insurer to insurer in wording, format, and availability or treatment of certain coverages. The lack of uniformity among these policies will make interpretation and comparison difficult for insureds and insurers.").

79. *See* WOLFF, *supra* note 15, at 172 ("Given the threat of correlated, large-scale cyber risk hanging over the cyber-insurance industry, it's not surprising that policy limits are generally relatively low and premiums and deductibles are high."); Camillo, *supra* note 39, at 56 ("Of particular concern from an aggregation perspective are the activities of state-sponsored or terrorist attackers . . . . Major events, such as a cyberattack on the U.S. power grid . . . could trigger catastrophic and far-reaching losses. In this hypothetical scenario, which envisages hackers shutting down parts of the U.S. power grid . . . the total impact on the U.S. economy was estimated at $243 billion, rising to over $1 trillion in the most extreme scenario.").

80. *See* WOLFF, *supra* note 15, at 173; *see also* Romanosky et al., *supra* note 22, at 2 ("Average premiums are priced between $10,000 and $25,000 . . . .").

and $300.[81] Consequently, because the cyber losses paid by insurers thus far have been small compared to the premiums they have collected, cyber insurance is very profitable for insurers—they have been receiving a profit margin of approximately 65% for cyber insurance versus 38% for general property insurance.[82] Yet, some policyholders have been willing to pay the high price for cyber insurance, with about one-third of all companies buying it.[83]

It is somewhat understandable why insurers thus far have erred on the side of charging premium rates much higher than for other lines of insurance. Pricing cyber insurance involves a lot of guesswork because, unlike other lines of insurance, such as auto and life, insurers do not have fulsome databases regarding cyber claims.[84] This is because, as previously noted, cyber risks and cyber insurance are relatively new, and cyber risks are constantly changing.[85] It is also because many hacked companies do not disclose when they have been hacked due to reputational concerns and the lack of a legal obligation to report many types of cyber attacks.[86]

81. *See, e.g.*, Anna Baluch, *Best Umbrella Insurance Companies*, INVESTOPEDIA, https://www.investopedia.com/best-umbrella-insurance-4845653 (Feb. 26, 2021) ("According to the Insurance Information Institute, you may be able to lock in $1 million worth of umbrella coverage for anywhere between $150 to $300 per year."); *Should I Purchase an Umbrella Liability Policy?*, INS. INFO. INST., https://www.iii.org/article/should-i-purchase-umbrella-liability-policy-0 (last visited July 13, 2021) ("For about $150 to $300 per year you can buy a $1 million personal umbrella liability policy. The next million will cost about $75, and $50 for every million after that.").

82. *See* Hurwitz, *supra* note 15, at 1537 (explaining that premium rates for cyber insurance are three to six times higher than other types of insurance); WOLFF, *supra* note 15, at 229.

83. *See* Hurwitz, *supra* note 15, at 1536; WOLFF, *supra* note 15, at 229.

84. *See, e.g.*, Romanosky et al., *supra* note 22, at 12–13 ("[Insurers] have no historic or credible data upon which to make reliable inferences about loss expectations . . . . [I]n some cases, the carrier would appear to guess . . . ."); *Buffett Cautious on Cyber Insurance Because No One Knows Risks*, NEWSMAX FIN. (May 5, 2018, 12:14 PM), https://www.newsmax.com/finance/streettalk/buffett-cyber-insurancerisks/2018/05/05/id/858534/ (quoting Warren Buffet of Berkshire Hathaway Inc., "I don't think we or anybody else really knows what they're doing when writing cyber," and anyone who claims to be able to accurately predict cyber losses are "kidding themselves"); Reed, *supra* note 4, at 171 ("[T]here is little or no claims history and data to analyze, and little experience to use in order to know what information to gather from the insured to determine appropriate coverage."); WOLFF, *supra* note 15, at 158 ("One of the primary challenges insurers face is the lack of reliable, consistently collected data about the frequency and cost of cybersecurity incidents.").

85. *See supra* Introduction; note 26 and accompanying text.

86. *See, e.g.*, Reed, *supra* note 4, at 161 ("[A]ttempts to calculate the actual cost of cybercrime are often hindered by the fact that organizations are unlikely to be willing to share exactly how much cybercrime has cost them for fear of reputational damage."); *Ransomwar*e, NAT'L ASS'N INS. COMM'RS (June 23, 2020), https://www.naic.org/cipr_topics/topic_ransomware.htm ("[M]any ransomware attacks go unreported."); Camillo, *supra* note 39, at 59 ("The reputational impact of a data breach or cyber intrusion is also of growing concern to risk managers . . . ."); WOLFF, *supra* note 15, at 198 (explaining that cyber attacks resulting in only first party losses can "be caused by

Consequently, there is a spectrum regarding how insurers calculate premiums. On one end, some insurers make relatively sophisticated actuarial projections based upon the policyholder's industry, the size of the policyholder in terms of annual revenues or number of employees, and the policyholder's answers to a system-security questionnaire.[87] On the other end, some insurers simply use flat rates for all policyholders or use the premium rates charged by other insurers.[88] Thus, for many insurers, premium rates are not tied to the policyholder's security measures in place.[89]

Regardless of the price of a cyber policy, however, the amount of risk actually transferred to insurers under most cyber policies is somewhat limited because insurers typically are willing to provide relatively low limits of coverage for policies that have large deductibles and numerous exclusions.[90] Some of the exclusions even appear to remove coverage for the very cyber risks the policies purport to cover under the insuring agreement portion of the policy.[91]

For example, although policyholders buy cyber insurance to protect themselves against their failure to prevent successful cyber attacks, some cyber policies exclude coverage for "an Insured's failure to take steps to use, design, maintain or upgrade a Computer System in order to prevent or avoid a Network Security Wrongful Act"[92] or the "[f]ailure to ensure that the computer system is reasonably protected by security practices and systems

incidents that companies had no obligation to report, leaving insurers even more in the dark about how to build accurate risk models . . . .").

87. *See* Romanosky et al., *supra* note 22, at 15–16; WOLFF, *supra* note 15, at 173–75.

88. *See* Romanosky et al., *supra* note 22, at 13–14; WOLFF, *supra* note 15, at 173 (explaining that some insurers "looked to the premiums set by their competitors to help determine their own prices").

89. *See* WOLFF, *supra* note 15, at 172 (noting it is surprising "how little [premium rates] seem to be influenced by the insured entity's actual security posture").

90. *See* WOLFF, *supra* note 15, at 172 ("Given the threat of correlated, large-scale cyber risk hanging over the cyber-insurance industry, it's not surprising that policy limits are generally relatively low and premiums and deductibles are high."); Hurwitz, *supra* note 15, at 1499 ("[C]yber insurance . . . policies are written narrowly."); Knutsen & Stempel, *supra* note 2, at 663 ("Policies providing coverage for a data breach or data loss have very narrow definitions of what type of loss is covered."); Camillo, *supra* note 39, at 62 ("Due to concerns over aggregation, many insurers are currently reluctant to offer substantial limits for cyber terrorism, or cyberattack[s] . . . ."); 1 NEW APPLEMAN PENNSYLVANIA INSURANCE LAW PRACTICE GUIDE, *supra* note 76, at § 7.22[4][a] ("The ISO Cyber Policy contains 30 exclusions.").

91. *See, e.g.*, Erica J. Dominitz, *To Err Is Human; To Insure, Divine: Shouldn't Cyber Insurance Cover Data Breach Losses Arising (in Whole or in Part) from Negligence?*, BRIEF, Summer 2017, at 32, 33 ("[A] number of cyber insurance policies contain certain exclusions that, if interpreted broadly, could significantly limit, or eliminate altogether, coverage . . . ."); Hurwitz, *supra* note 15, at 1537 ("[I]nsurers are pushing . . . for broad construction of these policies' exclusions . . . ."); WOLFF, *supra* note 15, at 237 ("[T]he short history of the past cyber-insurance market suggests . . . an expanding set of exclusions and no clear decrease in premium payments.").

92. *See The Hartford CyberChoice 2.0*, *supra* note 75, at § IV(A)(9)(b) (emphasis omitted).

maintenance procedures that are equal to or superior to those disclosed in the proposal."[93] Such exclusions are particularly problematic because there are "no clear, codified industry standard[s] for cybersecurity."[94] Consequently, when presented with cyber loss claims, insurers may argue these exclusions eliminate coverage for cyber losses that occur due to the policyholder's negligent computer security practices and systems.[95] Yet, that is the very reason policyholders purchase cyber insurance—to protect against cyber losses caused by, among other things, negligent computer security practices and systems. If cyber policies do not even cover cyber losses that result from a policyholder's negligent protection of its computer system, then the policies arguably provide only illusory coverage for many, if not most, cyber losses.[96]

Similarly, although many cyber policies purport to provide coverage for policyholders' liabilities to financial institutions for the reimbursement of the costs associated with fraudulent transactions resulting from a security breach (e.g., credit card charges on a stolen credit card number), the policies often also contain a "contractual liability" exclusion.[97] A contractual liability exclusion precludes coverage for "[a]ny contractual liability or obligation or any breach of contract, including any liability of others assumed by you, unless such liability would have attached to you even in the absence of such contract."[98] Insurers have successfully argued to courts that such exclusions apply to situations where, for example, MasterCard or Visa seek reimbursement from the victimized policyholder for fraudulent credit card charges as result of a successful cyber attack on the policyholder's computer

93. PHILA. INDEM. INS. CO., CYBER SECURITY LIABILITY COVERAGE FORM § IV.D., https://www.phly.com/files/Cyber%20Security%20Liability%20Policy%20Form36-8835.pdf.

94. WOLFF, *supra* note 15, at 64.

95. *See, e.g.*, Dominitz, *supra* note 91, at 33 ("By interpreting such exclusions broadly, insurers could argue that there is no coverage for virtually any data breach event by arguing that the breach resulted, at least in part, from system failures, negligent adoption of inadequate cybersecurity protocols . . . ."); Knutsen & Stempel, *supra* note 2, at 667 ("[A] surprising number of cyber-insurance policies incorporate various pre-loss cyber-security requirements to which a policyholder must adhere in order to obtain coverage post-loss.").

96. *See* Dominitz, *supra* note 91, at 33–34 ("[W]hile the insurance industry commonly markets cyber insurance products to companies as comprehensive protection from the full breadth of cyber-related risks, in actuality, many cyber policies are written on insurance forms that insurers might argue exclude coverage for more than 50 percent of the traditional and common data breach scenarios . . . ."); Knutsen & Stempel, *supra* note 2, at 668 (criticizing policy provisions that only allow non-negligent policyholders to recover, arguing that "the pre-loss computer security requirements demanded by the insurer are acting as post-claim underwriting opportunities for the insurer. . . . After the loss, if the policyholder has not met the insurer-specified behavioral standards, that insurer can back out of coverage. This is akin to an attempt by the insurer to eliminate substantially all risks . . . . If a policyholder had perfect compliance with computer security, the risk of loss should be zero.").

97. PHILA. INDEM. INS. CO., *supra* note 93, at § IV.P.

98. *Id.*

system because the credit card companies' contracts with the policyholder require the policyholder to reimburse the credit card companies for losses caused by the policyholder's loss of its customers' credit card numbers.[99] So, an unwary policyholder may think it has purchased cyber insurance for losses due to stolen credit card numbers as a result of system security breaches, but the policy it actually purchased may contain an exclusion that takes away that very coverage.

Cyber policies also typically exclude coverage for claims arising out of "war" or "acts of foreign enemies."[100] Insurers may interpret these exclusions to mean policyholders do not have coverage for the losses associated with many cyber attacks because some of the major cyber attacks are believed to have been launched by hostile foreign countries such as Russia, China, and North Korea.[101]

II. THE CHALLENGES OF INSURING CYBER RISKS

Creating a robust market for cyber insurance where policyholders can obtain real coverage for the cyber risks they are facing at actuarially sound and fair prices has several obstacles to overcome. Some of the primary ones have been touched upon, but they will be highlighted and discussed in more detail in this part.

99. *See, e.g.*, P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1, *8 (D. Ariz. May 31, 2016) (applying contractual liability exclusion in cyber policy to eliminate coverage for policyholder's losses associated with reimbursing credit card processing company for credit card costs and fees associated with a security breach).

100. *See, e.g.*, *The Hartford CyberChoice 2.0*, *supra* note 75, at § IV(A)(8), https://safeguardme.com/wp-content/uploads/2013/10/PDF3.pdf. (excluding coverage for losses in any way related to "war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not) . . . ."); Reed, *supra* note 4, at 192 ("[T]he policies often include exclusions for claims based upon or arising out of war, invasion, acts of foreign enemies, etc.").

101. *See* Reed, *supra* note 4, at 192; 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[2][a][ii]; WOLFF, *supra* note 15, at 121. The strength of insurers' argument regarding the applicability of war exclusions is questionable, however, because it often is unclear who precisely launched the cyber attacks and the attacks may be made for reasons other than as acts of war. *Id.* Indeed, such exclusions have been narrowly interpreted in other contexts to apply only to actions by "sovereign" nations. *See, e.g.*, Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1015 (2d Cir. 1974) (holding that war exclusions did not apply where a Pan American Airlines plane was hijacked and destroyed because the actors were "a radical political group, rather than a sovereign government"); Universal Cable Prods., LLC v. Atl. Specialty Ins. Co., 929 F.3d 1143, 1158 (9th Cir. 2019) (finding that the costs to move the production of a movie due to rocket fire by Hamas into Jerusalem were not excluded by war exclusions because "Hamas did not constitute a de facto or de jure sovereign during the July 2014 conflict between Hamas and Israel").

A. Correlated Catastrophic Risks

One of the principal challenges to insuring cyber risks is that cyber risks can be correlated.[102] Correlated risks are perils that cause numerous losses to the pool of insureds at approximately the same time.[103] Because the losses to many policyholders occur at approximately the same time, correlated risks can cause catastrophic losses for insurers. Consequently, for most types of correlated risks, such as the natural catastrophes of floods and earthquakes, private insurers generally refuse to insure them.[104] Private insurers avoid insuring correlated risks because of insurers' alleged inability to accurately predict when and where losses associated with correlated risks will occur, which in turn makes it difficult to establish actuarially sound premiums and spread the risk of loss across a large enough pool of insureds with diverse risk profiles.[105]

If an insurance company is not well-capitalized and is exposed to correlated risks, then the insurer may become insolvent in the event the risk is realized. For example, after Hurricane Andrew hit Florida in 1992, numerous insurers became insolvent.[106] In 2018, a California insurer similarly became insolvent after a wildfire known as the "Camp Fire" destroyed ninety percent of the homes in Paradise, California.[107] Consequently, because most private insurers generally refuse to insure correlated risks, the losses associated with correlated risks are often uninsured or underinsured.[108]

With respect to cyber risks, the insurance industry understandably is wary of providing large amounts of insurance for them because some cyber

102. *See* WOLFF, *supra* note 15, at 14 ("Prior work on cyber-insurance includes significant theoretical modeling of the cyber-insurance industry and the challenges it presents, such as correlated losses."); Hurwitz, *supra* note 15, at 1538 ("[M]any risks relating to cybersecurity are correlated.").

103. *See supra* note 19 and accompanying text.

104. *See* Cummins, *supra* note 19, at 342–43; Bruggeman et al., *supra* note 19, at 187.

105. *See* Bruggeman et al., *supra* note 19, at 187.

106. *See* LYNNE MCCHRISTIAN, HURRICANE ANDREW AND INSURANCE: THE ENDURING IMPACT OF AN HISTORIC STORM 5 (Aug. 2012), https://www.iii.org/sites/default/files/paper_HurricaneAndrew_final.pdf; Cassandra R. Cole et al., *The Use of Post-Loss Financing of Catastrophic Risk*, 14 RISK MGMT. & INS. REV. 265, 266 (2011).

107. *See* Dale Kasler & Michael Finch II, *Insurer Goes Bust From Camp Fire With Millions in Claims Unpaid. How Will It Affect Paradise Homeowners?*, SACRAMENTO BEE (Dec. 3, 2018), https://www.sacbee.com/news/state/california/fires/article222563185.html; Kristin Lam, *Northern California Town of Paradise Lost 90% of its Population After Camp Fire, Data Shows*, USA TODAY (July 14, 2019), https://www.usatoday.com/story/news/nation/2019/07/11/paradise-california-population-camp-fire-california-wildfire-fund/1710525001/.

108. *See Facts + Statistics: U.S. Catastrophes*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-us-catastrophes (noting that in 2018, there were approximately $33 billion in uninsured losses caused by natural catastrophes).

risks may result in correlated losses.[109] For example, in a matter of days, NotPetya caused $10 billion in losses worldwide, and WannaCry impacted 300,000 computers in 150 different countries.[110] To avoid being bankrupted by massive, correlated cyber losses, insurers currently limit the amount of cyber insurance they are willing to sell to individual policyholders.[111] Insurers also purchase reinsurance to transfer some of their losses to other insurers.[112] As discussed further in Section II.D, insurers' decisions to provide only limited cyber coverage due to correlated risk concerns, however, leave policyholders uninsured or underinsured for many cyber risks.

B. Too Little Risk and Loss Data

Another significant challenge facing cyber insurers is the fact that cyber insurance has only been around for a little more than two decades, so robust

109. *See supra* note 102 and accompanying text; *see also* WOLFF, *supra* note 15, at 5 ("But cyberattacks like NotPetya were not restricted to any single location or industry sector. For insurers, that meant potentially facing a massive number of claims simultaneously with no obvious path to diversifying their customer base in a way that would reliably prevent correlated losses."); LLOYD'S, CLOUD DOWN: IMPACTS ON THE US ECONOMY 5 (2018) ("[R]eliance on a relatively small number of [cloud services] companies has resulted in systemic risk for businesses using their services. In the event of sustained downtime of a top cloud service provider, simultaneous damage for all its clients and dependents could lead to catastrophic financial losses.").

110. *See supra* notes 8–9.

111. *See, e.g.*, WOLFF, *supra* note 15, at 5 ("[T]o avoid correlated losses . . . insurers deliberately diversif[y] their customers to be certain they [are] not all concentrated in any one place . . . ."); Camillo, *supra* note 39, at 62 ("Due to concerns over aggregation, many insurers are currently reluctant to offer substantial limits for cyber terrorism, or cyberattack[s] . . . .").

112. Reinsurance is a worldwide business wherein global reinsurers insure all, or portions, of another insurer's portfolio of business. *See, e.g.*, BARRY R. OSTRAGER & THOMAS R. NEWMAN, HANDBOOK ON INSURANCE COVERAGE DISPUTES § 15.01[a], [b] (19th ed. 2019) (generally discussing reinsurance). Most reinsurance is sold by European and Bermuda companies. *See, e.g.*, FED. INS. OFF., U.S. DEP'T TREASURY, THE BREADTH AND SCOPE OF THE GLOBAL REINSURANCE MARKET AND THE CRITICAL ROLE SUCH MARKET PLAYS IN SUPPORTING INSURANCE IN THE UNITED STATES 5 (2014), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/FIO%20-%20Reinsurance%20Report.pdf ("[I]n 2013 approximately $46 billion in total (P/C) reinsurance premiums were ceded by U.S.-based insurers to unaffiliated reinsurers; of this amount, approximately $28.4 billion of premiums were ceded to non-U.S. reinsurers and approximately $17.6 billion of premiums were ceded to U.S. professional reinsurers."); Daniel Schwarcz & Steven L. Schwarcz, *Regulating Systemic Risk in Insurance*, 81 U. CHI. L. REV. 1569, 1615 (2014) ("[R]einsurance is an international business—the largest companies are located in Europe and Bermuda . . . ."). In fact, reinsurance paid 60% of the insured losses related to the September 11th terrorist attacks, 65% of the insured losses resulting from Hurricanes Katrina, Rita, and Wilma, and 40% of the insured Hurricane Sandy losses. *See* FED. INS. OFF., *supra*, at 15.

claims databases regarding cyber losses do not yet exist.[113] Without accurate claims data, actuarially accurate premium pricing is not possible.[114]

In addition, because cyber insurance is sold by hundreds of insurers with numerous different policy forms, the claims information of one insurer may not be particularly useful to another insurer using a different policy form.[115] Even if it would be useful, however, insurers generally do not share their own claims data because they view it as proprietary and confidential information.[116]

Another impediment to creating robust cyber risk databases is that, aside from system breaches where consumers' private information is compromised, victimized companies historically have not been required to report or disclose most cyber breaches.[117] If system hacks are not reported or disclosed, then insurers can only guess as to how many are actually occurring.

Unlike other risks, cyber risks are also constantly changing because cyber criminals are continually creating new means and ways of attacking or hacking into computer systems.[118] This, in turn, means cyber insurers also must predict how many, and how severe, future cyber losses will be from previously unknown types of cyber attacks. Collectively, these uncertainties regarding the frequency and scope of future cyber losses make it extremely difficult to accurately price premiums for cyber insurance.

C. Untested Policy Language

Cyber insurers also must price cyber policies with somewhat of an information void regarding how courts will interpret the policy language contained in cyber policies.[119] Although some of the policy language has been cut and pasted from other lines of insurance and courts have interpreted that language in other contexts, cyber policies are new enough, and have varying policy language, such that cyber policy language generally has not

113. *See supra* notes 21–22, 84 and accompanying text.

114. *See supra* note 21 and accompanying text.

115. *See supra* notes 24, 28–29 and accompanying text.

116. *See supra* note 23 and accompanying text.

117. *See supra* note 86 and accompanying text; *see also* WOLFF, *supra* note 15, at 47, 167 (explaining that under state breach notification laws, only thefts of personal identifying information must be reported, while "[a]ll other cybersecurity incidents, from online extortion to theft of intellectual property and denial-of-service attacks, could still go unreported").

118. *See, e.g.*, WOLFF, *supra* note 15, at 230–31 ("[N]either carriers nor policy-holders are necessarily able to anticipate the kinds of cyber risks that will emerge even one or two years into the future."); Hurwitz, *supra* note 15, at 1538 ("[T]here is dramatic uncertainty as to the actual risk exposure associated with cyber-incidents.").

119. *See supra* note 26 and accompanying text.

been tested in the courts.[120] Therefore, much of the policy language does not have court-established meanings.[121] The lack of interpretation by courts of the policy language and the coverage provided under cyber policies means that neither insurers nor policyholders can be confident regarding what coverage cyber policies actually provide. This information void is another factor that adds to the complexity of establishing actuarially sound premium prices.

D. Lack of a Uniform Policy Form

For policyholders, it is currently very difficult to compare cyber insurers, cyber policies' coverages, and the prices of cyber policies because cyber insurers are not selling the same product.[122] There are hundreds of insurers selling cyber policies using different policy forms that provide different coverages and use different policy language.[123] Thus, a policyholder currently needs to be very sophisticated regarding both insurance and cyber security, or employ sophisticated intermediaries, in order to procure an appropriate cyber policy to cover the types of cyber risks the policyholder's particular business faces.[124]

That is not the case for other lines of insurance, such as CGL policies, where insurers all sell the same product, so policyholders can compare insurers based upon the price of the insurance and the claims handling reputations of the insurers.[125] Indeed, despite ever-increasing cyber risks, one of the reasons only one-third of businesses currently purchase cyber insurance is because many businesses lack knowledge regarding the cyber risks they face and the various cyber coverages being sold that is necessary to make an intelligent purchase of cyber insurance.[126] Yet, most policyholders do not employ the sophisticated cyber risk and insurance

120. *See supra* note 26 and accompanying text. Some scholars have argued that insurers reuse policy language year after year once the language has been interpreted by courts because the court-established meaning of the language aids in the actuarial process. *See, e.g.*, Michelle E. Boardman, *Contra Proferentem: The Allure of Ambiguous Boilerplate*, 104 MICH. L. REV. 1105, 1113 (2006) (arguing that the predictability in the interpretation of policy language by courts incentivizes ISO not to change policy language).

121. *See supra* note 26 and accompanying text.

122. *See supra* notes 24, 28–29 and accompanying text.

123. *See supra* notes 24, 28–29 and accompanying text.

124. *See, e.g.*, 4 NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION, *supra* note 14, at § 29.01[4] ("Given the complexity of assessing the potential losses and determining how best to cover those risks, it may be helpful [for policyholders] to engage insurance brokers, consultants or outside attorneys before purchasing [cyber] insurance."); Reed, *supra* note 4, at 171 ("[T]he research and analysis required by an individual potential insured are currently substantial.").

125. *See supra* note 76 and accompanying text.

126. *See supra* note 83 and accompanying text.

intermediaries needed to purchase cyber insurance as it currently is being offered.[127] Consequently, two-thirds of American businesses are largely uninsured with respect to cyber risks.[128]

E. Too Little Actual Coverage

Another problem with the usefulness of cyber insurance from the policyholders' perspective is that the policies only cover specifically listed types of cyber risks and losses instead of all types of cyber risks and losses, and the policy language granting coverage is narrowly written with numerous exclusions.[129] This means a lot of policyholders' cyber risks and losses are not covered, which leaves policyholders uninsured for those risks.[130] Thus, under current cyber policies, policyholders, not insurers, generally bear the risk of losses from new forms of cyber attacks. Because cyber attacks are constantly evolving, the cyber insurance currently being sold may not be a very valuable asset for many policyholders if it leaves policyholders uninsured for new forms of cyber attack. Such insurance also is not serving the purpose for which businesses buy cyber insurance—to transfer the risk of expensive, or even catastrophic, cyber losses from policyholders to insurers.[131]

Even for cyber risks that are covered, the coverage provided is limited because cyber policies typically have low policy limits and high deductibles.[132] According to some reports, insurers generally are unwilling to sell more than $10 million to $25 million in limits of coverage to a single policyholder.[133] The most cyber insurance that currently can be purchased, even when it is purchased from numerous insurers in various amounts, collectively only totals approximately $300 million.[134]

The potential losses from a cyber attack for some companies, however, far exceed the amount of available cyber insurance. For example, the NotPetya malware attack knocked out 30,000 computers and 7,500 servers at

127. *See supra* note 83.

128. *See supra* note 83.

129. *See supra* notes 65–66, 90–93, 98, 100 and accompanying text; *see also* WOLFF, *supra* note 15, at 156 ("[A]s exclusions of cyber risk grew broader over time . . . the definitions of covered cyber risks in stand-alone policies grew narrower and more specific.").

130. WOLFF, *supra* note 15, at 156. Target, for example, reportedly was only able to purchase $100 million in coverage despite trying to purchase more than that before its well-publicized cyber attack which cost Target more than $200 million. *See* WOLFF, *supra* note 15, at 170; Reuters, *supra* note 12.

131. *See supra* note 73 and accompanying text.

132. *See supra* note 90 and accompanying text.

133. *See* Romanosky et al., *supra* note 22, at 2.

134. *See id.*

Merck & Co. and allegedly cost the pharmaceutical company $1.3 billion.[135] Even if Merck had $300 million in coverage, it still would have had a $1 billion uninsured loss, which is a staggering amount.

Other policyholders think they are covered for cyber losses under the policies they purchased, but when they present claims, they are surprised to learn that the cyber policies they purchased do not actually cover the cyber losses at issue due to exclusions in the policies. For example, the restaurant chain P.F. Chang's China Bistro, Inc. paid an annual premium of $134,052 for a cyber policy that specifically covered losses due to "cyber attacks" into the "insured's system."[136] P.F. Chang's was hacked and 60,000 credit card numbers of its customers subsequently were posted on the Internet.[137] MasterCard assessed P.F. Chang's credit card processing company, among other costs, a charge of $1,716,798.85 to reimburse MasterCard for the fraudulent credit card charges that resulted from the hack.[138] In turn, P.F. Chang's credit card processing company charged P.F. Chang's for that amount pursuant to its credit card processing agreement, under which P.F. Chang's agreed to reimburse the company for any assessments that credit card companies imposed as a result of P.F. Chang's acts or omissions.[139]

P.F. Chang's tendered the claim to its cyber insurer, which, in turn, denied coverage based on a contractual liability exclusion similar to the one discussed in Section I.B.[140] The court agreed with the cyber insurer that the exclusion applied.[141] Thus, a policyholder that processed a lot of credit card transactions as part of its business and purchased cyber insurance to cover cyber attacks into its system did not actually have coverage for cyber attacks into its system for one of the primary risks it faced (i.e., theft of customers' credit card numbers) because the policyholder had a contractual obligation to reimburse another party that was injured by the hack. So, just how effective was the cyber risk transfer that P.F. Chang's purchased for $134,052?

In short, for cyber insurance to be a meaningful source of risk transfer for some businesses, cyber insurance will need to provide much more robust coverage than it currently does. Cyber insurance also needs to be available

135. *See, e.g.*, Riley Griffin, Katherine Chiglinsky & David Voreacos, *Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question.*, INS. J. (Dec. 3, 2019), https://www.insurancejournal.com/news/national/2019/12/03/550039.htm.

136. P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1, 6 (D. Ariz. May 31, 2016).

137. *Id.* at *2.

138. *Id.*

139. *Id.*

140. *Id.* at *7; *see also supra* note 98 and accompanying text.

141. *Id.* at *8.

with much higher limits of coverage because the potential losses facing some companies far exceed the limits currently available for purchase.

III. POTENTIAL APPROACHES TO INSURING CYBER RISKS

Moving forward, how should the creation and sale of cyber insurance policies change, if at all, to address the problems discussed in Part II? This Part addresses that question and provides potential answers to it.

A. Maintain the Status Quo—Let the Market Solve the Problems

One option is to stay the course and let the process that has been unfolding over the past two decades continue to unfold. The principal argument in support of the status quo is that markets are more efficient than the government at solving problems, so the market should be allowed to address the problems in the cyber insurance market.[142]

Under this approach, market forces would be left alone to work out the most efficient solution to the problems facing the cyber insurance market. That essentially has been the government's position thus far.[143] The government has been content to let the cyber insurance market cover policyholders' cyber losses to the extent insurers are willing to do so with little regulation.[144] According to Professor Wolff, "governments across the world appeared to be convinced that insurers could figure out how to build better risk models and strengthen cybersecurity practices in industry better than policy-makers."[145]

Although there are some statutes, such as HIPPA and the various state notification laws, that require hacked policyholders to advise their customers

142. *See generally* Alan Kirman, *Economic Theory and the Crisis*, VOXEU (Nov. 14, 2009), https://voxeu.org/article/economic-theory-and-crisis ("[T]he efficient markets hypothesis . . . has ruled the roost for some years in finance. Its originator was, by common accord, Louis Bachelier, who developed the notion of Brownian motion at the turn of the twentieth century."); Baruti Kafele, *Can The Free Market Solve Society's Problems? Hell Yes!*, BEING LIBERTARIAN, (Dec. 18, 2016), https://beinglibertarian.com/can-free-market-solve-societys-problems-hell-yes/ ("[H]istory continually proves that when people autonomously and organically solve problems in the free market, then progress is unquestionable. Alternatively, government intervention and intrusion into the private affairs of citizens often causes more confusion, stagnation, and inefficiency in the long term . . . ."); David Brooks, Opinion, *I Was Once a Socialist. Then I Saw How It Worked.*, N.Y. TIMES, Dec. 6, 2019, at A31 ("Socialist planned economies . . . interfere with price and other market signals in a million ways. They suppress or eliminate profit motives that drive people to learn and improve.").

143. *See* WOLFF, *supra* note 15, at 13 ("Subscribing to the view that the private sector knows best how to handle these risks, the federal government remained relatively hands-off . . . .").

144. *See id.* at 162 ("[T]he U.S. government seemed hesitant to take any tangible steps toward establishing any formal data repository or collection system.").

145. *Id.*, *supra* note 15, at 196.

when their customers' personal information has been compromised, to date, the government has not developed any mandatory cyber security requirements or best practices.[146] Indeed, "there is no authoritative source for cyber risk assessment."[147]

Consequently, insurers, to some extent, have become the de facto regulators of cyber security practices through the coverages they provide and the cyber risk management counseling services they sell to their policyholders for a separate fee.[148] Thus far, however, insurers filling the role of cybersecurity regulators have not translated into lower premium rates for policyholders or more coverage for policyholders. As a result, the primary beneficiaries of the current approach appear to be insurers and the cyber security service providers with whom they have partnered.[149]

As for the actual coverage provided by cyber policies and the limits of coverage sold, insurers can defend the status quo by noting that insurers historically have avoided insuring correlated risks that could result in catastrophically large losses for insurers which could jeopardize their financial solvency.[150] As discussed in Section II.A, correlated risks are situations where numerous people have essentially the same risk of the same type of loss occurring at approximately the same time.[151] Correlated risk concerns are greatest when an insurer sells insurance to a limited pool of insureds that face the same risks at the same time.[152] For example, people who live in the same neighborhood generally face similar risks of natural catastrophes.[153] Insurers generally attempt to avoid insuring correlated risks due to actuarial and capitalization concerns.[154]

146. *See* Hurwitz *supra* note 15, at 1516 ("In the United States there is no general law of data security."); *see also* WOLFF, *supra* note 15, at 158 ("[T]here is relatively little consensus about the most effective baseline security practices and risk management techniques for organizations to reduce their risk exposure . . . .").

147. WOLFF, *supra* note 15, at 187 (quoting Romanosky et al., *supra* note 22).

148. WOLFF, *supra* note 15, at 183 ("I wouldn't say that we have data to suggest that the money . . . our customers have spent on prevention partners has improved the security performance . . . .") (quoting the Chief Underwriting Officer of XL Catlin); Talesh, *supra* note 15, at 429 ("Insurance companies either have in-house departments or contract with third-party organizations that offer a series of services aimed at preventing data breaches and violations of privacy laws from ever occurring.").

149. *See* WOLFF, *supra* note 15, at 180 ("Insurers . . . did not have sufficient confidence in [their cyber risk management] partners to link their pricing schemes to those companies' services or assessments, and policy-holders therefore received no clear value from engaging with those partners.").

150. *See supra* notes 104–108 and accompanying text.

151. *See supra* note 103 and accompanying text.

152. *See supra* note 105–107 and accompanying text.

153. *See supra* note 107 and accompanying text.

154. *See supra* note 105 and accompanying text; *see also* Cummins, *supra* note 19, at 342–43.

Insurers limiting the amount of coverage they are willing to underwrite and limiting the actual coverage provided under their policies by drafting cyber policies as named peril policies, as opposed to all-risk policies, and then adding dozens of exclusions could be viewed as a prudent way of protecting against catastrophic losses in the event of a correlated cyber loss event. If cyber risks are correlated risks, then policyholders should be grateful there is a private cyber insurance market at all because private insurance generally is not available for other types of correlated risks, such as flooding and earthquakes.[155]

With that said, just because a cyber threat can impact numerous entities at the same time does not mean that a large percentage of an individual insurer's policyholders will suffer correlated losses. This is because different industries face different types of cyber risks. For example, P.F. Chang's and Merck both face cyber risks, but they are not the same cyber risks. P.F. Chang's is a retail restaurateur that processes thousands of credit cards on a daily basis, while Merck is a pharmaceutical company that does not process thousands of credit card purchases daily. Consequently, their risks from a cyber attack are not correlated. Similarly, although malware, such as WannaCry, could impact thousands of computers around the world, that does not mean that all the owners of the computers impacted would be insured by the same insurer. Accordingly, to reduce the correlation of cyber losses, insurers need to sell cyber policies to policyholders in diverse industries to ensure their insureds are not all vulnerable to the same cyber risks.

Further, reinsurance and catastrophe bonds are two additional ways that insurers can mitigate and spread correlated risks of loss. Reinsurance is a worldwide business wherein global reinsurers insure all of, or portions of, another insurer's portfolio of business.[156] For example, as a result of insurers' purchase of reinsurance, reinsurers paid 60% of the insured losses related to the September 11th terrorist attacks, 65% of the insured Hurricane Katrina losses, and 40% of the insured Hurricane Sandy losses.[157]

By purchasing reinsurance, cyber insurers can spread the risk of catastrophic cyber events to other insurers throughout the world. Thus, through reinsurance, cyber losses effectively become less correlated with respect to the losses any individual insurer faces because the losses are insured by multiple insurers worldwide and spread across worldwide pools of insureds with diverse risk profiles.

155. *See supra* note 104 and accompanying text.

156. *See, e.g.*, OSTRAGER & NEWMAN, *supra* note 112, at § 15.01[a], [b]; Christopher C. French, *The Role of the Profit Imperative in Risk Management*, 17 U. PA. J. BUS. L. 1081, 1109 (2015).

157. *See* FED. INS. OFF., *supra* note 112, at 15.

Catastrophe bonds are bonds that are issued for specific types of catastrophes, such as natural catastrophes, and they are sold to institutional investors.[158] Catastrophe bonds emerged in the 1990s following Hurricane Andrew in Florida and the Northridge Earthquake in California as a new way to diversify insurers' risks with respect to catastrophic events.[159] Typically, institutional investors receive interest payments on the bonds and the return of their principal at the end of the bond term unless the specified catastrophe occurs, in which case the investors forfeit their rights to the return of the principal and any additional interest payments.[160] The retained money is then available to pay the insured losses, which means the true risk of loss is transferred from the insurer to the institutional bondholders. As of August 2020, $41.5 billion in catastrophe bonds were outstanding.[161]

Cyber insurers could use catastrophe bonds to reduce their risks of suffering correlated, catastrophic cyber attack losses. For example, a catastrophe bond could be issued to cover any named malware event that impacted an established number of computer systems (e.g., 10,000) or a specified dollar amount of loss (e.g., $1,000,000). By doing so, the insurer effectively could create a stop-loss point that triggers the forfeiture of the institutional investors' catastrophe bonds, thereby creating a pool of capital to pay the losses.

In fact, Aon plc, a global insurance broker, and Hudson Structured Capital Management Limited, a Bermuda-based reinsurer, recently introduced a cyber risk catastrophe bond product in November 2020.[162] This development further buttresses the argument that cyber risks can be insured in large amounts. It also weakens the argument in favor of the status quo to the extent the argument is based upon the premise that cyber risks are uninsurable in high amounts due to correlated risk concerns.

As discussed in Sections II.C, II.D, and II.E, maintaining the status quo is also problematic from policyholders' perspectives.[163] Cyber insurance currently is very expensive for the amount of coverage being provided.[164]

158. *See Facts + Statistics: Catastrophe Bonds and Other Insurance-Linked Securities*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-catastrophe-bonds (last visited Oct. 1, 2021) [hereinafter *Catastrophe Bonds*].

159. U.S. GOV'T ACCOUNTABILITY OFF., GAO-02-941, CATASTROPHE INSURANCE RISKS: THE ROLE OF RISK-LINKED SECURITIES AND FACTORS AFFECTING THEIR USE 15–16 (2002), https://www.gao.gov/assets/gao-02-941.pdf.

160. *See* Scales, *supra* note 19, at 46.

161. *See Catastrophe Bonds*, *supra* note 158.

162. *See Aon Secures $70 Million Alternative Capital Capacity Led by HSCM to Transfer Systemic Cyber Risk*, AON (Nov. 19, 2020), https://aon.mediaroom.com/news-releases?item=138033.

163. *See supra* Sections II.C–E.

164. *See supra* note 31 and accompanying text.

There also are dozens of different cyber policy forms being sold that are so dense that one needs to retain experts in both cyber security and insurance to even attempt to make an educated purchase.[165] The cyber policies currently being sold also provide inadequate actual insurance coverage because the coverage grants are narrowly written and then subject to a prolix of exclusions.[166]

The insurance industry has had more than twenty years to consolidate the policy forms being sold, to make the policies understandable and affordable, and to provide meaningful coverage. It has not done so. Consequently, although markets theoretically should be efficient ways to solve problems, sometimes they fail to do so.[167] After twenty years of trying, the cyber insurance market appears to be a market that is incapable of solving its problems on its own. Indeed, insurers have even acknowledged the cyber insurance market cannot solve the problems it is facing without legislative or regulatory intervention.[168] The potential forms of that intervention will be discussed in the next four Sections of the Article.

B. Cover Cyber Risks Under Commercial General Liability and All-Risk Property Policies

Instead of maintaining the status quo, one potential solution to some of the cyber insurance market's current problems is for all-risk property and CGL policies to cover cyber losses, just as they do for most physical injuries and losses.[169] Professors Jeff Stempel and Erik Knutsen are champions of this approach. They refer to it as the "techno-neutral" solution.[170] Under this approach, cyber risks are not considered materially different from other types of risks insured by CGL policies and property policies.[171] For example, using cyber attacks to steal credit card numbers is just a new form of theft. The fact that the physical credit cards have not been stolen is not important. And property insurance has long covered theft.[172] Similarly, since the 1940s, CGL

165. *See supra* notes 24, 29 and accompanying text.

166. *See supra* notes 90–93, 97–98, 100 and accompanying text.

167. *See infra* notes 196–198 and accompanying text.

168. *See* WOLFF, *supra* note 15, at 238 ("The idea that cybersecurity can be handled solely, or even primarily, through a market-driven approach led by insurers is a flawed one—something that insurers themselves, to their credit, have been pointing out to policy-makers for years.").

169. *See* Knutsen & Stempel, *supra* note 2, at 647 ("The long-term solution is for insurers to simply fold cyber-loss coverage into traditional coverage products and not differentiate a loss based on its particular or peculiar property characteristics.").

170. *See* Knutsen & Stempel, *supra* note 2, at 673–74.

171. *See id.* at 655 ("Cyber losses due to crime or fraud are also no different in end result than losses due to crime or fraud in the physical world.").

172. *See supra* note 72 and accompanying text.

policies have covered policyholders' liabilities to third parties for injuries caused by policyholders' negligence.[173]

Much of business and personal life today is conducted on computers and the Internet. People now download or stream movies and music instead of buying DVDs and CDs. People now pay bills online instead of using checks or cash and buy countless items online from Amazon.com that are directly delivered to their homes instead of going to stores. Consequently, the risk of physical injuries, such as the physical theft of a credit card, is likely far lower today than the risk of a cyber theft of a credit card number. That, in turn, means the need for insurance to cover many types of physical injuries and losses today is also likely lower than it was twenty years ago because many assets now reside in cyber space, not physical space.

When viewed in this light, insurers' attempts to exclude coverage for cyber losses under traditional property and liability policies could be viewed as profiteering. Insurers are providing less coverage under traditional policies by excluding coverage for cyber losses, which in the past were physical losses, so people need less traditional insurance today than they did in the past. Simultaneously, however, if consumers want coverage for the types of risks they actually face with greater probability today (i.e., cyber risks), then they are forced to purchase a standalone cyber policy at a high price in exchange for limited coverage.

One way to rectify this situation would be for traditional policies to simply cover cyber risks in the same way they cover the analogous risks of physical losses or injuries. Traditional insurance historically has covered many types of intangible and invisible injuries, so including cyber risks in the coverage would simply be another category of such injuries. For example, "[d]amages from pollution or gas, mold, odors, and asbestos are all losses covered by typical insurance policies."[174] Cyber risks would just be one more type of intangible losses that would be covered. As evidenced by the addition of the electronic data loss exclusion and other cyber risk exclusions to traditional insurance policies that are discussed in Section I.A, insurers obviously do not want to do that. Thus, if this approach were adopted, then legislatures or insurance regulators would need to force insurers to include coverage for cyber risks in traditional policies.

---

173. *See, e.g.*, Jeffrey W. Stempel, *Assessing the Coverage Carnage: Asbestos Liability and Insurance After Three Decades of Dispute*, 12 CONN. INS. L. J. 349, 355–58 (2006) (discussing the creation of CGL policies in the 1940s); ABRAHAM & SCHWARCZ, *supra* note 72, at 453 (reproducing ISO's CGL policy form under which the policy covers losses for bodily injuries, property damage, and personal injuries due to the policyholder's negligence).

174. Knutsen & Stempel, *supra* note 2, at 658 (citing Hazel Glenn Beh, *Physical Losses in Cyberspace*, 8 CONN. INS. L.J. 55, 66–67 (2001)).

Insurance is already a heavily regulated industry because of, among other reasons, insurers' significant information advantage over consumers, the large disparity in power between insurers and consumers, the monopolization by insurers of the drafting of insurance policy language, and insurers' sale of most types of policies on a take-it-or-leave-it basis.[175] Consequently, to protect policyholders, state insurance regulators are empowered to review and approve the policy forms used by insurers, including the language used in the policies and the coverages provided.[176] In doing so, regulators have the power to reject terms that are "unfair," "ambiguous," "unreasonable," and/or "contrary to public policy."[177] Insurance regulators could find that the exclusion of coverage for cyber risks under traditional policies, and the sale of cyber policies as currently drafted, is unfair, ambiguous, and/or unreasonable.

In addition, as discussed in Part II, cyber policies provide only limited coverage in exchange for high premiums, and policyholders need to employ expert insurance intermediaries and cyber security experts in order to attempt to understand what types of claims are actually covered by cyber policies. It is, however, within insurance regulators' power to force insurers to provide cyber coverage differently.

Under the techno-neutral approach, cyber risk coverage would revert to being included under CGL and all-risk property policies. As discussed in the Introduction, CGL policies and all-risk property policies cover all risks of loss unless a type of loss is specifically excluded.[178] Such policies are intended to be the broadest types of liability and property insurance sold.[179] One of the greatest attributes of all-risk insurance is that a purchaser does not need to be an insurance expert to understand the basic coverage being purchased—all risks are covered except for risks specifically excluded. Granted, the coverage provided by typical CGL policies and all-risk property policies has been whittled down some over the years, as reflected by the fact

175. *See, e.g.*, Christopher C. French, *Dual Regulation of Insurance*, 64 VILL. L. REV. 25, 33–35 (2019); NAT'L ASS'N INS. COMM'RS, STATE INSURANCE REGULATION 2 (2011), https://www.naic.org/documents/topics_white_paper_hist_ins_reg.pdf [https://perma.cc/6EKT-T88K] ("Insurance is more heavily regulated than other types of business because of the complexity of the insurance contracts, the lack of sufficient information for insurance consumers to adequately shop for prices and adequacy of coverage and because insurance contracts are generally contracts of adhesion.").

176. *See, e.g.*, ALA. CODE § 27–14–9 (2016); GA. CODE ANN. § 33–24–10 (2016); NEB. REV. STAT. § 44–7513 (2016).

177. *See, e.g.*, ALA. CODE § 27–14–9 (2016); GA. CODE ANN. § 33–24–10 (2016); NEB. REV. STAT. § 44–7513 (2016).

178. *See supra* notes 17 and accompanying text.

179. *See, e.g.*, French, *supra* note 156, at 1107.

that such policies currently contain numerous exclusions.[180] But, the coverage such policies offer is still far more comprehensive and comprehensible than cyber policies, and CGL and all-risk property policies are sold using uniform, standardized policy forms. So, a purchaser does not need to attempt to compare and understand dozens of different policy forms before purchase, as it does for cyber insurance, in order to buy the right policy for its business.

Similarly, all-risk policies also have the advantage of providing coverage to businesses that do not have a sophisticated appreciation of the types of risks they are facing because the policies cover *all risks*. Thus, purchasers of all-risk insurance can let the experts at risk assessment—insurers—figure out what the policyholder's risks are and price the insurance accordingly. In short, all-risk policies shift the burden of risk assessment from policyholders to the parties most qualified to analyze the risks.

Because cyber risks essentially are just the twenty-first century manifestation of many of the traditional risks of loss or injury covered by CGL and property insurance, those lines of insurance could easily be updated to include coverage for cyber risks. It would be as simple as deleting a few exclusions from the policies and clarifying that the definition of "property damage" includes lost electronic data. Loss of use of property is already covered by such policies,[181] so a clarification that "property damage" includes lost electronic data and the inability to use a covered computer system would be the primary changes needed to accomplish this result.

Insurers, of course, likely would argue that cyber risks are different than traditional risks of physical loss or injury, which is why they exclude coverage for them under traditional lines of insurance.[182] They also would likely argue that they would not be able to charge actuarially sound premium rates due to the lack of cyber risk data, and that cyber risks are correlated risks such that they cannot be insured on an all-risk basis.[183]

There are, of course, rejoinders to such arguments. One rejoinder is that these obstacles apparently are surmountable when insurers sell cyber insurance as standalone policies with profit margins of sixty-five percent, so they also should be surmountable if cyber coverage were included in CGL and all-risk property policies. A second rejoinder is that insurers could and should make cyber risk losses less correlated by selling policies across diverse industries to diversify their insured pools and by using reinsurance

180. *Id.* at 1096–114 (discussing the erosion of coverage under all-risk policies over time).

181. *See, e.g.,* ABRAHAM & SCHWARCZ, *supra* note 72, at 453 (reproducing the definition of "property damage" in ISO's CGL policy form).

182. *See supra* Section I.A.

183. *See supra* Section II.A.

and catastrophe bonds to further spread the risks. A third rejoinder is that insurers, either cooperatively or through regulatory mandate, could share information regarding cyber risks and loss data to reduce the uncertainty regarding likely loss rates. By doing so, they could be more confident that the premium rates needed to cover such losses are actuarially sound.

C. Create Uniform Standalone All Cyber Risk Liability and Property Policies

Another option for addressing the current problems with cyber insurance would be for cyber insurance to be offered under uniform all cyber risk standalone policies that cover only cyber risks. Under this approach, there would be a uniform standalone all cyber risk liability policy, and a uniform standalone all cyber risk property policy. The policies would only cover cyber risks, but they would cover all cyber risks.

Offering separate liability and property policies would make cyber insurance more consistent with most other lines of insurance that do not combine third-party liability coverage with first-party property coverage in a single policy.[184] Although the techno-neutral approach of folding cyber risks back into the coverage provided by traditional lines of insurance makes some sense, cyber risks arguably are different than most traditional physical risks. This is because cyber risks are quickly evolving, and the reach of cyber criminals is worldwide. Risk modeling cyber risks in the absence of comprehensive claims and risk data creates a different risk/reward calculation for insurers, so it seems fair to allow insurers to treat cyber risks differently than traditional risks for which there are established claims databases. That does not mean, however, that insurers should be given carte blanche to do whatever they want when it comes to cyber insurance.

Offering separate all cyber risk liability and property policies would also allow policyholders to purchase coverage for just the risks with which they are concerned. For example, retail stores, such as Walmart, may be very concerned about losing personal customer information, such as credit card numbers, and the associated ensuing liabilities. Other companies, such as Pfizer, may be more concerned about having valuable intellectual property, such as the formulas for new vaccines, stolen by a hacker. Of course, if there were a market preference by policyholders for cyber policies to combine

184. *See, e.g.*, ABRAHAM & SCHWARCZ, *supra* note 72, at 183 ("First-party insurance protects the insured against a loss that she . . . suffers herself; it is 'victim's insurance.' Fire, property, life, health, and disability insurance fall into this category. In contrast, third-party insurance protects the insured against legal liability to a third-party resulting from the insured's actions."). Auto insurance and homeowners' insurance are the two most notable exceptions to the general rule that policies either provide first-party or third-party coverage.

first-party and third-party coverages in a single policy, as many cyber policies currently do, then it could continue to be done in the future as well.

The key under this approach, however, is to switch cyber insurance from named peril coverage to all-risk coverage and use uniform policy forms. Doing so would make the policies much easier to understand and would allow less sophisticated businesses to make informed purchases without the need to retain insurance expert intermediaries and cyber security experts. Offering cyber insurance as all-risk coverage also would make the coverage broader. As things stand now, the coverage provided under cyber policies is narrowly written and backstopped with a litany of exclusions that arguably take away much of the limited coverage provided in certain situations.[185] By selling cyber insurance as named peril insurance, where only specific types of cyber risks are listed and covered, the policyholder is left uninsured for any risk not specifically listed, including all unknown types of cyber risks.[186]

Ideally, the cyber risk policy forms sold by insurers also would be standardized and uniform such that all insurers selling cyber insurance would be using the same policy forms. This would allow policyholders to make apples-to-apples comparisons among insurers based upon premium prices and the quality of claims handling services.

Moving to all-risk coverage would provide the most meaningful improvement, however, if insurers did not then load up the policies with a prolix of exclusions. Yet, even if insurers were to attempt to remove a significant amount of the all-risk coverage provided through exclusions, the rules of insurance policy interpretation—insurers have the burden of proving the applicability of exclusions, any ambiguities in the policy language are construed against insurers, and exclusions should be interpreted in a way that prevents them from making the coverage grant illusory[187]—collectively

185. *See supra* Section II.E.

186. *See* WOLFF, *supra* note 15, at 188 ("[It is] difficult to take the named-peril approach to cyber underwriting that carriers have adopted without leaving significant holes in customers' coverage . . . .").

187. *See, e.g.*, SCSC Corp. v. Allied Mut. Ins. Co., 536 N.W.2d 305, 313 (Minn. 1995) (ruling that insurer has the burden to prove the applicability of an exclusion as an affirmative defense); Crawford v. Prudential Ins. Co., 783 P.2d 900, 904 (Kan. 1989) ("Since an insurer prepares its own contracts, it has a duty to make the meaning clear, and if it fails to do so, the insurer, and not the insured, must suffer.") (quoting Fowler v. United Equitable Ins. Co., 438 P.2d 46, 48 (Kan. 1968)); Powell v. Liberty Mut. Fire Ins. Co., 252 P.3d 668, 672 (Nev. 2011) ("While clauses providing coverage are interpreted broadly so as to afford the greatest possible coverage to the insured, clauses excluding coverage are interpreted narrowly against the insurer.") (quoting Nat'l Union Fire Ins. v. Reno's Exec. Air, Inc., 682 P.2d 1380, 1383 (Nev. 1984)); Bailer v. Erie Ins. Exch., 344 Md. 515, 525, 687 A.2d 1375, 1380 (1997) ("If the exclusion totally swallows the insuring provision, the provisions are completely contradictory. That is the grossest form of ambiguity . . . .").

would still make it much easier for policyholders to obtain coverage for cyber losses than under the current cyber policies.

D. Use the Federal Government as an Excess Insurer or Reinsurer of Cyber Risks

Another option for addressing many of the current problems in the cyber insurance market would be for the federal government to act as an excess insurer or reinsurer for private insurers where losses exceed a certain stated amount for any individual insurer. One advantage of this approach is that it does not simply shift cyber insurance from a market-based approach to a government monopoly approach because it keeps private insurers as participants in the cyber insurance market and encourages competition.

Another key advantage of using the federal government as an excess insurer or reinsurer for cyber insurance is that it would eliminate the correlated risk problem from private cyber insurers' perspectives. The primary explanation insurers provide regarding why cyber risk coverage is sold on a named peril basis with relatively low limits of coverage is their concern that a catastrophic cyber event could result in disastrous losses for insurers.[188] Using the federal government as a reinsurer or an excess insurer above a certain stop-loss point would cap private insurers' losses and thus effectively eliminate the catastrophic downside risk to insurers created by correlated losses.

The federal Terrorism Risk Insurance Program ("TRIA") could serve as a template for the cyber insurance market.[189] The terrorist attacks on September 11, 2001, caused more than $45 billion in insured losses.[190] As a result, insurers began excluding coverage for terrorism risks, and in 2002, the TRIA was enacted to address the new gap in coverage.[191]

---

188. *See supra* notes 15, 39, 105 and accompanying text.

189. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002) (codified as amended in various sections of 15 U.S.C.). Some scholars, such as Michelle Boardman, contend that certain risks, including terrorism, are uninsurable because the risks cannot be accurately quantified, and therefore the TRIA is a misguided attempt to make terrorism appear to be an insurable risk. *See* Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L.J. 783, 786 (2005) ("This Article argues that terrorism insurance is not possible. The terrorism risk is a known unknown; we are aware of the risk but are still too ignorant to calculate and redistribute the risk in an insurance pool."). Pursuant to this theory, cyber risks also could be considered uninsurable risks because not enough loss data or information regarding the risks exists to actuarially price premiums for the insurance. *See supra* notes 21–22 and accompanying text.

190. *See* FED. INS. OFF., U.S. DEP'T TREASURY, REPORT ON THE EFFECTIVENESS OF THE TERRORISM RISK INSURANCE PROGRAM 3 (2020), https://home.treasury.gov/system/files/311/2020-TRIP-Effectiveness-Report.pdf.

191. *Id.*

Under the TRIA, insurers are required to offer terrorism coverage, but the federal government serves as a stop-loss for insurers when the insurance industry's aggregated losses exceed $200 million, and any individual insurer's losses exceed 20% of the insurer's earned premiums on lines of insurance eligible for terrorism coverage.[192] Once the TRIA is triggered, individual insurers are only responsible for 20% of the terrorism losses.[193] The TRIA also has a program cap of $100 billion.[194] Once the aggregated losses exceed $100 billion, neither the federal government nor private insurers have any obligation to pay for such losses.[195]

The cyber insurance market could be handled similarly to the terrorism insurance market. Private insurers could continue to sell cyber insurance with the federal government serving as an excess insurer or reinsurer above a certain stop-loss point to ensure that there is adequate capital to cover catastrophic cyber loss events.

Under this approach, the federal government would also have an incentive to reduce the risk of cyber attacks and losses because it potentially would be financially responsible if cyber losses occurred at a catastrophic level. Consequently, the government likely would be incentivized to mandate that insurers share cyber risk and loss data and that businesses employ the best system security practices, so all parties would have a better understanding of the risks and how to minimize them. The sharing of risk and loss data also would enable insurers to price cyber policies in a more actuarially sound way.

One problem with seeking federal involvement in the cyber insurance market at this point, however, is that there has not been a complete market failure for cyber insurance, which is what historically has prompted the federal government to become involved with insurance programs. For example, as noted, the TRIA was created in 2002 only after private insurers added terrorism exclusions to their policies following September 11th.[196] Similarly, the National Flood Insurance Program was created in 1968 after private insurers added flood exclusions to their policies.[197] The Affordable Care Act was adopted in 2010 because there were more than forty million people without health insurance, as insurers refused to sell health insurance to people with pre-existing conditions or to high-risk people at affordable

192. *Id.* at 5–6.

193. *Id.* at 7.

194. *Id.*

195. *Id.*

196. *See supra* note 191 and accompanying text.

197. *See* National Flood Insurance Act of 1968, Pub. L. No. 90-448, 82 Stat. 572 (codified as amended at 42 U.S.C. §§ 4001–4127 (2012)).

prices.[198] Thus, Congress usually only acts with respect to insurance matters when there is a complete market failure.

As discussed in Part II, the cyber insurance market has some significant flaws, but there is a market for cyber insurance. Indeed, the cyber insurance market is rapidly growing and highly profitable for insurers,[199] so insurers likely would not support federal intervention if they thought such intervention would reduce the profitability of cyber insurance. On the other hand, from the policyholders' perspective, it would be very attractive to gain access to increased cyber insurance limits at affordable prices, with the federal government serving as an excess insurer or reinsurer for amounts above those that private insurers are willing to sell.

One of the strongest arguments against this approach would be the potential moral hazard problems it could create. Moral hazard theory posits that a person will take less care to avoid losses if the losses are insured because the financial impact of the losses will be borne by another entity.[200] If the federal government were to provide stop-loss coverage to insurers, then insurers would be protected to some extent against their own poor underwriting practices and decisions, so insurers would have less incentive to exercise prudent underwriting practices. Similarly, policyholders would have little incentive to avoid or minimize cyber risks or become knowledgeable regarding their own cyber risks or system security

198. *See* ABRAHAM & SCHWARCZ, *supra* note 72, at 349; KAREN POLLITZ, RICHARD SORIAN & KATHY THOMAS, HOW ACCESSIBLE IS INDIVIDUAL HEALTH INSURANCE FOR CONSUMERS IN LESS-THAN-PERFECT HEALTH? 1–2 (2001), https://www.kff.org/health-costs/report/how-accessible-is-individual-health-insurance-for/ [https://perma.cc/NHH9-8GSU].

199. *See supra* notes 28–31 and accompanying text.

200. *See, e.g.*, W. Cas. & Sur. Co. v. W. World Ins. Co., 769 F.2d 381, 385 (7th Cir. 1985) ("Once a person has insurance, he will take more risks than before because he bears less of the cost of his conduct."); ROBERT H. JERRY, II & DOUGLAS R. RICHMOND, UNDERSTANDING INSURANCE LAW 12 (5th ed., 2012) ("[T]he existence of insurance can have the perverse effect of increasing the probability of loss. . . . This phenomenon is called *moral hazard*."); Scott E. Harrington, *Prices and Profits in the Liability Insurance Market*, *in* FOUNDATIONS OF INSURANCE ECONOMICS: READINGS IN ECONOMICS AND FINANCE 626, 631 (George Dionne & Scott Harrington eds., 1992) ("Moral hazard is the tendency for the presence and characteristics of insurance coverage to produce inefficient changes in buyers' loss prevention activities, including carelessness and fraud . . . ."); George L. Priest, *The Current Insurance Crisis and Modern Tort Law*, 96 YALE L.J. 1521, 1547 (1987) ("Moral hazard refers to the effect of the existence of insurance itself on the level of insurance claims made by the insured. . . . *Ex ante* moral hazard is the reduction in precautions taken by the insured to prevent the loss, because of the existence of insurance."); Adam F. Scales, *The Chicken and the Egg: Kenneth S. Abraham's "The Liability Century,"* 94 VA. L. REV. 1259, 1263 (2008) (describing the term moral hazard as the phenomenon where people have a "tendency to take fewer precautions in the presence of insurance"); Gary T. Schwartz, *The Ethics and the Economics of Tort Liability Insurance*, 75 CORNELL L. REV. 13, 338 n.117 (1990) ("'Moral hazard' is sometimes distinguished from 'morale hazard,' the former referring to deliberate acts like arson, the latter to the mere relaxation of the defendant's discipline of carefulness.").

weaknesses if cyber insurance was widely available with unlimited policy limits.

To some extent, the moral hazard problem that would be created by more fully insuring cyber risk is a theoretical problem rather than a real problem because there are proven ways to address moral hazard concerns. With respect to insurers, they still would suffer losses up to their stop-loss points, so they would still be incentivized to exercise good underwriting practices even if the federal government provided stop-loss excess insurance or reinsurance. Insurance is not profitable for insurers if they are regularly paying more in claims than they are collecting in premiums.[201] Thus, if insurers were regularly paying the limits of their policies and triggering the federal stop-loss protections, then it is unlikely they would be profitable companies.

With respect to policyholders, insurers can address moral hazard concerns by using deductibles and pricing the insurance appropriately.[202] Policyholders could be incentivized to lower their risks based on the premium prices charged and by insurers covering the costs of loss minimization efforts taken by the policyholders in the event of cyber attacks, just as insurers currently do under other lines of commercial insurance.[203]

Similarly, cyber policies could include sizeable deductibles to ensure policyholders take steps to avoid losses.[204] Deductibles align policyholders'

---

201. Insurers, however, also generate revenues from the "float"—the investment income they make from premiums while waiting to pay claims. Indeed, Warren Buffet has famously acknowledged that Berkshire-Hathaway earns most of its profits from the float, as opposed to underwriting profits (i.e., the amount of premiums collected that exceed the amount paid for claims). *See* Stempel, *supra* note 173, at 357, n.18; FEINMAN, *supra* note 21, at 16.

202. *See, e.g.*, Ben-Shahar & Logue, *supra* note 16, at 209 ("[I]nsurers do, in fact, commonly share losses with insureds in various ways, including through deductibles and copayments."); Haitao Yin, Howard Kunreuther & Matthew W. White, *Risk-Based Pricing and Risk-Reducing Effort: Does the Private Insurance Market Reduce Environmental Accidents?*, 54 J.L. & ECON. 325, 326 (2011) (discussing the use of lower premium prices for risk avoidance activities in the context of environmental liability policies); Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 UCLA L. REV. 1412, 1429 (2013) ("The deductible for the driver's first-party property damage coverage in the auto policy should control the moral hazard of insurance in these instances.").

203. *See, e.g.*, John S. Clark Co. v. United Nat'l Ins. Co., 304 F. Supp. 2d 758, 767–68 (M.D.N.C. 2004) ("To be covered as reimbursable sue and labor expenses [under a commercial property policy], those expenditures must be made for the benefit of the insurer in mitigating or preventing a covered loss.") (quoting Swire Pac. Holdings, Inc. v. Zurich Ins. Co., 139 F. Supp. 2d 1374, 1385 (S.D. Fla. 2001)); Haitao Yin, Howard Kunreuther & Matthew W. White, *Risk-Based Pricing and Risk-Reducing Effort: Does the Private Insurance Market Reduce Environmental Accidents?*, 54 J.L. & ECON. 325, 326 (2011) (discussing the reduction of premium prices for risk avoidance activities in the context of environmental liability policies).

204. *See, e.g.*, Ben-Shahar & Logue, *supra* note 16, at 209; Tom Baker & Rick Swedloff, *supra* note 202, at 1429–30.

interests with insurers' interests in minimizing or eliminating losses because policyholders' losses are not completely covered in the event of a loss.[205] Thus, the potential moral hazard concerns could be addressed because policyholders who do not use the best cyber risk practices and systems would pay higher premiums, and policyholders would absorb a portion of the losses through deductibles if they were to have cyber loss claims.

E. Create Uniform Standalone All Cyber Risk Liability and Property Policies and Use the Federal Government as an Excess Insurer or Reinsurer of Cyber Risks (the "All-Risk Private-Public" Approach)

A fifth option would be to create uniform, but separate, standalone all cyber risk liability and property policies while also using the federal government as an excess insurer or reinsurer of cyber losses once an insurer's losses exceed a stop-loss amount. This hybrid approach, the "All-Risk Private-Public" approach, would solve the biggest problems facing the cyber insurance market. It also would capture the best aspects of the various approaches.

By using single, uniform policy forms, the federal government would have some certainty as to what risks it would be assuming with respect to each and every insurer instead of the current situation where dozens of insurers are selling cyber policies with different coverages being provided using different policy language.[206] Policyholders also would have more certainty regarding the scope of coverage being provided by the various insurers offering cyber insurance because the insurers would all be offering the same coverages.[207] The differences between cyber insurers would then be revealed by the premium prices charged and the quality of claims handling services.

Policyholders also would not need to be experts regarding insurance and insurance policy language, or cyber risks, in order to buy cyber insurance because, as all-risk coverage, they would only need to be concerned with the price of the policy and the quality of the insurer selling it.[208] Under this approach, insurers would be tasked with assessing the risk presented by policyholders when pricing the insurance. This would place the burden of calculating the appropriate premium prices for the coverage on the parties most qualified to assess and price the risk—the insurers. It also would

205. *See, e.g.*, ABRAHAM & SCHWARCZ, *supra* note 72, at 7 ("Insurers attempt to combat . . . moral hazard with . . . deductible, coinsurance, and dollar limits of coverage in policies so that all losses are not fully insured . . . .").

206. *See supra* Section III.C.

207. *See supra* Section III.C.

208. *See supra* Section II.D.

maintain and encourage competition between insurers in procuring policyholder accounts.

The potential moral hazard problems for both policyholders and insurers would, of course, still exist under this hybrid approach, as it does under the fourth approach.[209] Insurers would be protected to some extent by the federal government from poor underwriting practices and decisions if the federal government were to provide stop-loss excess insurance or reinsurance for cyber risks. Policyholders also would have less incentive to ensure that their computer systems are as secure as possible because they would be protected by insurance. But those problems could be addressed by the ways discussed in Section III.D.

In addition, by selling cyber insurance for first-party risks under one policy form and third-party risks under a separate policy form, the traditional distinction between first-party and third-party risks would be preserved. This approach also recognizes that the risks policyholders face are not uniform—some policyholders face substantial third-party risks, but not first-party risks, and vice versa.[210]

Selling cyber insurance as standalone insurance—as opposed to being a part of CGL or all-risk property insurance—also recognizes that cyber risks are different in some respects than physical risks of loss, as discussed in Section III.C. Thus, insurers that do not want to be involved in the cyber insurance market, or insurers that do not acquire the necessary expertise to become involved, would not be forced to provide cyber coverage by including it in CGL policies and all-risk commercial property policies.[211]

CONCLUSION

Cyber risks present some of the biggest risks of the twenty-first century. They also are some of the most challenging risks to insure. The cyber insurance market currently is fragmented with hundreds of insurers selling different cyber risk insurance policies that cover different types of cyber risks.[212] This means purchasers of cyber insurance must be experts or hire experts regarding both insurance and cyber security to make a knowledgeable purchase.[213] Yet, even knowledgeable purchasers of cyber insurance can only obtain limited coverage for cyber losses because the insurance is sold

209. *See supra* Section III.D.
210. *See supra* Section III.C.
211. *See supra* Section III.C.
212. *See supra* note 77 and accompanying text.
213. *See supra* note 124 and accompanying text.

on a named peril—as opposed to all-risk—basis under policies laden with exclusions and with relatively low policy limits.[214]

Although there are numerous approaches to insuring cyber risks that could address some of the current problems in the cyber insurance market, the All-Risk Private-Public approach—where cyber risk insurance would be provided under uniform all cyber risk liability and property policies, with the federal government serving as a reinsurer or excess insurer above a stop-loss amount—may be the best approach to insuring cyber risks moving forward.[215] Such an approach would address the correlated risk problem insurers face, bring uniformity to the policy forms sold in the cyber insurance market, and allow policyholders to obtain greater coverage for cyber risks.[216]

214. *See supra* Section III.B.
215. *See supra* Section III.E.
216. *See supra* Section III.E.