2017

Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment

Jay P. Kesan

Carol M. Hayes

Article

Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment

Jay P. Kesan[†] **& Carol M. Hayes**[††]

[†] Professor and H. Ross & Helen Workman Research Scholar, University of Illinois; Project Leader, Critical Infrastructure Resilience Institute (CIRI), DHS S&T Center of Excellence, University of Illinois. We are grateful to our CIRI colleagues for helpful comments and suggestions, particularly Linfeng Zhang and Professor Sachin Shetty.

[††] Research Associate, Critical Infrastructure Resilience Institute (CIRI), University of Illinois. Copyright © 2017 by Jay P. Kesan and Carol M. Hayes.

INTRODUCTION

Cybersecurity is a popular topic these days. In October 2016, a distributed denial-of-service attack (DDoS attack) cut off millions of people from a considerable chunk of the Internet for a few hours.[1] In a separate incident, intelligence officials in the United States accused the Russian government of using cyberattacks to interfere with the American electoral process.[2] In late 2015, hackers used BlackEnergy malware to shut down sections of the power system in Ukraine for several hours.[3] A year later, Ukraine's capital city of Kiev experienced its own power disruption after an attack with a different type of malware, which researchers have named Crash Override.[4] These incidents are in addition to the ransomware, phishing campaigns, and data breaches that were already causing newsworthy incidents around the world.

The stakes are continually getting higher. According to the World Economic Forum, ineffective cybersecurity may cost the

[1] Bruce Schneier, *Lessons from the Dyn DDoS Attack*, SCHNEIER ON SECURITY (Nov. 8, 2016), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

[2] NAT'L CYBERSECURITY AND COMMC'NS INTEGRATION CTR., DEP'T OF HOMELAND SEC. & FBI, JOINT ANALYSIS REPORT, GRIZZLY STEPPE – RUSSIAN MALICIOUS CYBER ACTIVITY 1 (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[3] *Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, ICS-CERT (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[4] Andy Greenberg, *'Crash Override': The Malware That Took Down a Power Grid*, WIRED (June 12, 2017), https://www.wired.com/story/crash-override-malware. Unlike BlackEnergy, Crash Override appears to have been specifically built to disrupt physical systems like power grids.

world's economy as much as three trillion dollars by 2020.[5] Consumers are generally aware that data breaches put them at risk for identity theft and fraud, but hackers have also targeted hospital computers with ransomware. Once a computer is infected, the ransomware locks hospital employees out of computers that hold vital information about patients—information that could literally be the difference between life and death—and demands payment to restore employees' access to the systems.[6]

Generally speaking, it is a scary time to be a business owner who relies on computers for any important aspect of a business. Former FBI Director Robert Mueller has been quoted as saying that the only two types of companies are "those that have been hacked and those that will be."[7] Between 2012 and 2013, data breach incidents increased by sixty-two percent.[8] Studies have consistently shown an alarming rate of success for phishing attacks through e-mail.[9] Leaving abandoned flash drives around also remains a surprisingly effective way to infiltrate a computer network.[10] A company's network security is only as strong as its weakest link, and sometimes all it takes is one careless click.

So what can be done to improve the level of cybersecurity measures that are deployed throughout society? Kosseff criticizes many cybersecurity debates as being too focused on punitive, instead of collaborative, measures to unite the public and

[5] Danielle Gilmore & David Armillei, *The Future Is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork Is Laid for the Coming Storm*, *in* INSURANCE LAW 2016: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR 23, 24 (2016).

[6] *E.g.*, Danny Palmer, *Ransomware Blamed for Cyber Attack Which Forced Hospitals To Cancel Operations and Shut Down Systems*, ZDNET (Dec. 5, 2016), http://www.zdnet.com/article/ransomware-blamed-for-cyber-attack-which-forced-hospitals-to-cancel-operations-and-shut-down-systems.

[7] Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT TRIAL & INS. PRAC. L.J. 529, 531 (2014).

[8] Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 372 (2015) (noting as well that the average cost of a data breach in the United States over that time period was over seven million dollars).

[9] *E.g.*, Sharon D. Nelson & John W. Simek, *Law Firm Cyber Insurance: 'We Don't Insure Stupid'*, L. PRAC. MAG., Mar./Apr. 2016, at 24, 25 (citing a 2015 Verizon report finding that "23% of recipients open emails sent by scammers/hackers, and 11% download attachments from phishing emails").

[10] *See, e.g.*, Shaun Nichols, *Half of People Plug in USB Drives They Find in the Parking Lot*, REGISTER (Apr. 11, 2016), http://www.theregister.co.uk/2016/04/11/half_plug_in_found_drives.

private sectors.[11] The United States has been taking gradual steps towards the latter goal over the last several years. The National Institute of Standards and Technology (NIST) created the Cybersecurity Framework as a voluntary set of cybersecurity standards, pursuant to an executive order issued by President Obama.[12] In December 2015, Congress enacted the Cybersecurity Information Sharing Act (CISA) as part of the omnibus budget bill.[13] CISA allows for more cooperation between the private sector and the government on matters pertaining to cyber threat indicators.[14] To this end, a working group of business leaders has encouraged the creation of a cyber incident data and analysis repository (CIDAR) which is expected to contain information about cyberattacks and associated losses, as well as examining the viability of the market for cyberinsurance.[15]

This Article focuses on the goal of improving risk assessment and risk shifting through better information, to facilitate the expansion of the cyberinsurance market. Cyberinsurance coverage has become more widely available in recent years,[16] and has been described as a "new frontier" for the modern insurance market.[17] Done well, a cyberinsurance market could provide a fundamentally private market solution to some of the most pressing cybersecurity problems by urging the development and adoption of new security protections.[18] A poorly de-

[11] Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 418 (2016).

[12] Exec. Order No. 13,636, 3 C.F.R. 217 (2014); *Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH., http://www.nist.gov/cyberframework (last visited Oct. 6, 2017).

[13] Russell Brandom, *Congress Passes Controversial Cybersecurity Bill Attached to Omnibus Budget*, VERGE (Dec. 18, 2015), https://www.theverge.com/2015/12/18/10582446/congress-passes-cisa-surveillance-cybersecurity.

[14] 6 U.S.C. §§ 1502–1504 (2012).

[15] COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 19–20 (2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[16] *See* Collin J. Hite, *The Ever-Changing Scope of Insurance Law*, *in* INSURANCE LAW 2013: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR 5, 6 (2013).

[17] Anderson, *supra* note 7, at 591–92.

[18] Ranjan Pal et al., *Improving Network Security via Cyber-Insurance: A Market Analysis*, *in* ACM TRANSACTIONS ON PERFORMANCE EVALUATION OF COMPUTER SYSTEMS 1, 1:1–2 (2015), http://www-scf.usc.edu/~rpal/ACMTR.pdf ("Proponents of cyber-insurance believe that cyber-insurance would lead to the

signed cyberinsurance market, on the other hand, could aggravate existing failings, reward free riders, create moral hazards, and inadvertently limit the cyberinsurance market to market participants that are at greatest risk for cyberattacks. Government oversight could prove beneficial for establishing a proactive and efficient cyberinsurance market that offers extensive and affordable coverage.

Podolak describes data breaches as "[c]yber [r]isk's poster child."[19] As data breaches continue to make headlines, interest in shifting cyber risk through insurance will likely increase as well. In 2014, the cyberinsurance market brought in approximately one billion dollars in premiums.[20] Still, reports estimate that only about one-third of U.S. companies carry cyberinsurance policies.[21] In the event of a data breach, the other two-thirds often rely on third-party commercial general liability policies (CGL policies).[22] Many CGL policies, however, have language excluding losses of electronic data.[23] As more claims are denied, this will likely increase levels of interest in specific policies for cyber threats.[24]

Unfortunately, the financial fallout from data breaches is currently unpredictable, making the risk difficult to insure against.[25] Insurers also currently lack the kind of comprehensive actuarial data that informs decisions for other types of loss covered by insurance.[26] Some insurance companies may respond to this uncertainty by charging higher premiums, creating exclusions, and capping coverage, but these approaches may limit the reach of the cyberinsurance market. If cyberinsurance is too expensive, that leaves policyholders with less money to spend to

design of insurance contracts that would shift appropriate amounts of self-defense liability to the clients, thereby making the cyberspace more robust.").

[19] Podolak, *supra* note 8, at 371.

[20] Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 41 (2014).

[21] Anderson, *supra* note 7, at 533 (citing a 2013 Ponemon Institute study finding that thirty-one percent of companies carried cybersecurity insurance).

[22] *Id.* at 542.

[23] *See* Bailey, *supra* note 20, at 1.

[24] *Id.*

[25] *Id.* at 4.

[26] *Where Cyber Insurance Underwriting Stands Today*, INS. J. (June 12, 2015), http://insurancejournal.com/news/national/2015/06/12/371591.htm.

improve their information security.[27] The proposed CIDAR system could contribute significantly to making cyberinsurance more economically feasible by centralizing essential information.

In this Article, we have two overarching goals. First, we examine problems in the cyberinsurance market and suggest improvements. Second, in order to understand the legal risk attendant to interpretations of insurance policies, we conduct an empirical study of the current state of the insurance market by analyzing litigation over insurance coverage for computer-related harms. By focusing on technology, risk-transfer methods, and insurance-coverage litigation, we provide a comprehensive overview and a set of achievable goals that can strengthen the market for cyberinsurance.

In the first Part, we examine the threats, the potential responses, and the ultimate inadequacy of currently available methods of addressing cyber risk. In the second Part, we examine risk shifting and the foundations of insurance more generally, and also explore the use of potential analogies to workers' compensation insurance and the National Flood Insurance Program to inform the cyberinsurance debate. Additionally, we discuss the potential of alternative risk-transfer methods. In the third Part, we provide empirical analysis of litigation involving cyberinsurance coverage. Our empirical analysis is based on a lawsuit repository that we created—the Cyberinsurance Litigation Analytics Database (CLAD)—which focuses on legal disputes over insurance coverage for largely intangible, computer-enabled losses.

In the fourth Part, we offer recommendations for moving forward. First, we discuss how insurance policy coverage issues should be addressed in light of our empirical findings. Second, we urge cooperation between the government and private sector to create the CIDAR system, and take other actions as necessary to improve risk assessment. Third, we propose an alternative risk-transfer model for cyberinsurance that could supplement traditional insurance policies by using the mechanisms available in the financial markets for capitalization and risk shifting. Fourth, we discuss what the government can do to support the emerging cyberinsurance market.

[27] Bailey, *supra* note 20, at 5.

Cybersecurity is a modern crisis that requires flexibility and creative problem solving. Bad cybersecurity practices can disrupt economies and jeopardize national security. With the political divisions in the United States growing more contentious, it is more important than ever to work across party lines to address the risk of cybersecurity disasters that could lead to blackouts, recessions, and diplomatic crises. A stable cyberinsurance market could empower the private sector, and protect our national interests and economy.

I. CYBERSECURITY AND THE THREATS WE FACE

The Internet has transformed society. It has become a new playground, a ubiquitous center of learning, the bustling heart of commerce, and a social center. Its relative anonymity has also made it a haven for criminals,[28] in part because of how easy it is to disguise origins and preserve deniability. Its connection to sensitive targets has created a new battlefield for conflicts between nations.[29] The actors that evade security controls include benevolent researchers, mischievous troublemakers, malicious criminals, and government agencies.[30]

The National Research Council (NRC) has defined a cyberattack as "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[31] Cyberattacks can have physical effects as well,

[28] Svetlana Radosavac et al., *Using Insurance To Increase Internet Security*, *in* COMPILATION E-PROCEEDINGS OF THE SIGCOMM 2008 CONFERENCE & THE CO-LOCATED WORKSHOPS 43, 43 (2008).

[29] NAT'L RESEARCH COUNCIL OF THE NAT'L ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 50 (William A. Owens et al. eds., 2009) (noting the appeal of cyberattacks for covert action) [hereinafter NRC REPORT]; *accord* Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1834–35 (2016) (noting that cyber hostilities have affected Estonia, Georgia, Iran, and Ukraine over the last decade).

[30] *See* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 783 (2016) (defining "security researchers" as "non-malicious hackers" who look for flaws in software).

[31] NRC REPORT, *supra* note 29, at 80.

like the Stuxnet worm that was discovered in 2010 and is credited with destroying hundreds of nuclear centrifuges in Iran.[32] A German steel mill is also alleged to have suffered physical damage due to a cyberattack in 2014.[33] A power outage in Kiev, Ukraine, in December 2016 is thought to be the result of a malware package specifically designed to target industrial control systems.[34]

Cybersecurity is the counter to cyberattacks. Kosseff describes cybersecurity as actions to "safeguard the confidentiality, integrity, *and* accessibility of data."[35] Cybersecurity is necessary for the private and public sectors. Virtually everyone, from customers to private companies to the government, is aware of the existence of cybersecurity risks, though they may not be aware of their own exposure. The adoption of cybersecurity technology has been slow, but a study from 2013 indicated that corporate directors and general counsel ranked data security high as an issue of concern.[36] Small companies are especially vulnerable, as many of them may lack the resources to focus on security.[37] Hackers are also noticing that law firms are a good target for information and money, and, like small businesses, often lack strong security.[38]

Cybersecurity is practically defined by volatility, as the defenders must constantly adapt to counter the attackers, who are constantly adapting to get around new defenses.[39] Before the In-

[32] David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013), https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[33] Podolak, *supra* note 8, at 396.

[34] Kim Zetter, *The Malware Used Against the Ukrainian Power Grid Is More Dangerous Than Anyone Thought*, VICE (June 12, 2017), https://motherboard.vice.com/en_us/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industroyer.

[35] Kosseff, *supra* note 11, at 404.

[36] Hite, *supra* note 16, at 1.

[37] *See* Sarah E. Needleman, *Cybercriminals Sniff Out Vulnerable Firms*, WALL ST. J. (July 5, 2012), https://www.wsj.com/articles/SB10001424052702303933404577504790964060610.

[38] Dan Zureich & William Graebe, *Cybersecurity: The Continuing Evolution of Insurance and Ethics*, 82 DEF. COUNS. J. 192, 192–93 (Apr. 2015). Indeed, this is becoming an ethical issue for attorneys, with recent changes to the model ethics rules emphasizing the lawyer's obligation to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of" client information. Sean Harrington, *Cyber Insurance: What Minnesota Lawyers Need To Know*, 72 BENCH & B. MINN. 16, 18 (Nov. 2015).

[39] *See* Anderson, *supra* note 7, at 532.

ternet and the emergence of the personal computer market, computers were not really designed to interact with each other.[40] As computers became more networked and powerful, their capabilities grew exponentially, but the means to exploit them also grew.[41] Because of interdependent security risks, a single adverse cybersecurity event at one firm can have a cascade effect that harms other systems linked to the same network.[42] The highly publicized cyberattack on the Target retail chain in 2013, for example, happened because the attackers were able to hack Target's HVAC contractor and use that connection to get into Target's systems and steal payment data.[43]

Cybercrime has become a digital epidemic. Interpol considers there to be two types of cybercrime: advanced cybercrime and cyber-enabled crime. Advanced cybercrime is defined as attacks against hardware and software, while a cyber-enabled crime is a traditional crime perpetrated with the use of a computer.[44] A ransomware attack, for example, would be an advanced cybercrime, as it would not exist without the computers that it affects. On the other hand, when hackers exploit vulnerabilities in a bank's system to enable a massive theft, this is a cyber-enabled version of a bank robbery.[45]

The Ponemon Institute's 2016 Cost of Cyber Crime study examined 237 companies in six countries.[46] Organizations in the United States had the highest average cybercrime costs at over seventeen million dollars.[47] A study by the Center for Strategic and International Studies estimated annual global cybercrime

[40] *See* Carol M. Hayes, Note, *Content Discrimination on the Internet: Calls for Regulation of Net Neutrality*, 2009 U. ILL. J.L. TECH. & POL'Y 493, 498 (describing the function of protocols like the Internet Protocol).

[41] *See* Gilmore & Armillei, *supra* note 5, at 24 ("In 2010, McAfee, a leading cybersecurity firm, discovered a new piece of malware every fifteen minutes; by 2013, it uncovered a new instance of malware every second.").

[42] Bailey, *supra* note 20, at 9; Podolak, *supra* note 8, at 372.

[43] Podolak, *supra* note 8, at 372.

[44] Garrie & Reeves, *supra* note 29, at 1832.

[45] *E.g.*, J. Weston Phippen, *How Did Thieves in Japan Steal $13 Million from Convenience-Store ATMs?*, ATLANTIC (May 23, 2016), https://www.theatlantic.com/international/archive/2016/05/japan-atm-theft/483902 (noting that thieves in Japan were able to exploit ATM limits to withdraw nearly thirteen million dollars in two hours).

[46] PONEMON INST., 2016 COST OF CYBER CRIME STUDY & THE RISK OF BUSINESS INNOVATION 1 (2016), https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf [hereinafter PONEMON, CYBER CRIME].

[47] *Id.*

costs at over $400 billion in 2014.[48] Another Ponemon Institute study in 2016, which solely focused on data breaches, found that the average cost of a data breach in the United States was $221 per record lost.[49] The global mean cost per record was $158, with data breaches in the healthcare industry costing over twice that at $355 per record.[50] That study also found that having an incident response team and using encryption extensively were associated with lower per capita data-breach costs, while migrating a lot of the company's business to the cloud was associated with a higher per capita cost.[51]

A. THREATS

Vulnerabilities are at the heart of cyber threats. Consider, for instance, a DDoS attack. Flooding a system with data continues to be an effective attack method because a system's finite capacity for receiving and processing data makes it vulnerable. An attacker can therefore flood a target with data until the target crashes or is knocked off-line. Computer viruses likewise rely on vulnerabilities—specifically, flaws in code that allow an attacker to exercise control over the infected machine. Attacks enabled by viruses are much more versatile than attacks that rely solely on data capacity limitations because viruses can affect almost any part of the system, and their impacts are often much subtler than a simple denial of access.

The Ponemon Institute's 2016 cybercrime study enumerated eight categories of cyberattacks: (1) malware; (2) phishing and social engineering; (3) web-based attacks; (4) malicious code; (5) botnets; (6) stolen devices; (7) denial of service; and (8) malicious insiders.[52] The report noted that malware and malicious code attacks are linked, and the study considers malware attacks to be malicious-code attacks when they "successfully infiltrate[] the organizations' networks or enterprise systems."[53] Ninety-eight percent of the companies tracked in the 2016 Ponemon Institute cybercrime study experienced malware attacks, compared to

[48] Zureich & Graebe, *supra* note 38, at 192.

[49] PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 5 (2016), https://app.clickdimensions.com/blob/softchoicecom-anjf0/files/ponemon.pdf [hereinafter PONEMON, DATA BREACH].

[50] *Id.* at 10.

[51] *Id.* at 14.

[52] PONEMON, CYBER CRIME, *supra* note 46, at 8.

[53] *Id.*

sixty-one percent who experienced malicious-code attacks.[54] For our purposes, it is not necessary to distinguish between types of threats, though it is valuable to have a sense of their scope.

The goals of attackers vary widely. Cyberattack methods can be used for goals including causing a nuisance, espionage, and the disruption of critical infrastructure. It is very hard to tell at first glance what sort of attacker is involved. In 1998, the Pentagon was beset with a series of cyberattacks that were initially thought to be the actions of foreign terrorists.[55] In reality, the attackers were two teenagers from the United States and one teenager from Israel, likely acting more out of mischief than malice.[56] In 2000, a rejected job applicant in Maroochy Shire, Queensland, Australia, hacked into the local sewage control system and caused a raw sewage spill.[57] Whether driven by curiosity, revenge, or a general desire for destruction, the potential for harm by attackers is expansive.

Many attack methods, but not all, require an unwitting accomplice in the form of a computer operator who clicks on an infected file, uses bad password practices, or inserts an infected USB drive.[58] Human error can also be the whole cause of something like a data breach, even in the absence of a malicious attacker, as in the case of *Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC* which will be discussed in greater depth in a later section.[59] In the *Portal* case, the healthcare company's employees stored patient records in such a way that a simple search for a patient's name in Google allowed the searcher to access the patient's medical records.[60] The posting was likely inadvertent, and the company was sued in a class

[54] *Id.*

[55] Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 295 (2006).

[56] *Id.*

[57] Tony Smith, *Hacker Jailed for Revenge Sewage Attacks*, REGISTER (Oct. 31, 2001), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage.

[58] *See, e.g.*, Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 396 (2014) (describing an incident in which a cyber security official failed to use different passwords for his accounts, resulting in his company being hacked via an amateur SQL injection); Hahn & Layne-Farrar, *supra* note 55, at 290 (noting that Trojan horses and social engineering techniques are effective because people are generally inclined towards trusting others).

[59] 35 F. Supp. 3d 765 (E.D. Va. 2014).

[60] *Id.* at 768.

action for negligence or gross negligence, among other claims.[61] To borrow a term sometimes used by frustrated technical support professionals, a lot of threats to computer networks are at least partially PEBKAC issues—problem exists between keyboard and chair.[62]

B. RESPONDING TO THREATS

Threat responses can be categorized into what we call the three Ds: defend, deter, de-escalate. Defending can include passive methods like antivirus software and firewalls, as well as more active methods like tracing an attack back to its source. The goal of deterrence is to decrease the likelihood that an adversary will do something harmful. Currently, the criminal law is the primary approach used for deterrence,[63] though it remains difficult to identify attackers with sufficient certainty to support a conviction.[64] De-escalation is about the system's ability to bounce back after an attack, also referred to as its resilience.

Each of these areas offers opportunities for public-private partnerships. For example, the government could subsidize defensive technologies. Additionally, more information sharing between the public and private sectors about threats can enhance everyone's defenses. Deterrence via criminal prosecution is generally beyond the control of the private sector, though citizens have the ability to make their voices heard through their legislators in the enactment of stronger laws. Government assistance during the aftermath of a cyberattack can improve resilience. Garrie and Reeves note that corporations tend to support government involvement in the context of cyber threats.[65] Indeed, if an attack on a private company is the work of a foreign power, as many suspect of the attack on Sony Pictures in late 2014,[66]

[61] *Id.*

[62] Darlene Storm, *90% of Security Incidents Trace Back to PEBKAC and ID10T Errors*, COMPUTER WORLD (Apr. 15, 2015), https://www.computerworld.com/article/2910316/90-of-security-incidents-trace-back-to-pebkac-and-id10t-errors.html.

[63] *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent*, 201 MIL. L. REV. 1, 71 (2009) ("Stringent criminal laws and vigorous law enforcement will deter cyberattacks.").

[64] NRC REPORT, *supra* note 29, at 40.

[65] Garrie & Reeves, *supra* note 29, at 1830.

[66] *See id.* at 1829 ("[T]he United States publicly attributed both the hacking and the threats to North Korea.").

relying on the government may be their only recourse.[67] Another way that the government can support private resilience efforts is through the promulgation of voluntary standards, like the National Institute of Standards and Technology's Cybersecurity Framework, by government agencies working with experts who are very knowledgeable about how to recover from adverse cyber events.[68]

1. Defend

Computer and network owners and operators have a lot of options for reducing their threat exposure, though Bailey notes that security investments have a diminishing rate of return.[69] Personal computer users typically have antivirus software, either as a standalone product or as part of their operating system.[70] Sensitive information can be encrypted, and traffic coming into the system can be automatically monitored with a firewall.[71] More technologically savvy users might set up virtual machines to keep potential threats isolated in what is essentially "a fake computer running inside [their] real computer."[72]

Good computer-security hygiene is another essential element of defense. Among other things, important files and systems should be backed up, users should be trained to avoid risks, and users should use good password practices.[73] As noted above, user error is a constant threat to computer security.

In a perfect world, everyone would use antivirus software and firewalls, encrypt sensitive information, and practice good computer-security hygiene. Moreover, in a perfect world, all of these things would be enough to avoid cyberattacks. Sklerov

[67] *Id.* at 1846.

[68] *See infra* notes 152–54 and accompanying text. *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[69] Bailey, *supra* note 20, at 8.

[70] AV COMPS., IT SECURITY SURVEY 2014 8 (2014), https://www.av-comparatives.org/wp-content/uploads/2014/03/security_survey2014_en.pdf.

[71] *See* Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 43 (2005) (discussing encryption and firewalls as ways for users to eliminate "harms from crime").

[72] Micah Lee, *With Virtual Machines, Getting Hacked Doesn't Have To Be That Bad*, INTERCEPT (Sept. 16, 2015), https://theintercept.com/2015/09/16/getting-hacked-doesnt-bad.

[73] *See* Sklerov, *supra* note 63, at 23–24 (discussing security administration as an element of cybersecurity).

points out that there are frequently design flaws in computer software that create security vulnerabilities.[74] These vulnerabilities in code are continually being discovered, and most defensive software cannot block code that exploits vulnerabilities unknown to the software's creators.[75] Such vulnerabilities are called zero-day vulnerabilities, and their scarcity makes them very valuable.[76] It is generally unlikely that an exploit that targets a large number of systems would rely on a zero-day vulnerability, but such exploits are the perfect example of why even the best defensive practices may ultimately be inadequate.[77] This is also a reason why recent cybersecurity innovations have focused more on recognizing behavioral outliers than on known virus signatures.[78]

2. Deter

During the Cold War, nuclear deterrence relied on the promise of mutually assured destruction.[79] Deterrence may be based on the threat of punishment or the denial of success.[80] Criminal prosecution is the clearest example of deterrence by punishment. Unfortunately, that requires accurate attribution of the attack, which is often very difficult with cyberattacks.[81] Additionally, it is often unclear the extent to which increased punishment actually enhances deterrence.[82] A report by the U.S. Sentencing Commission in 1996 cites research that criminalizing a behavior increases deterrence when there is a perception of "certain, swift

[74] *Id.* at 26.

[75] *See* LILLIAN ABLON & ANDY BOGART, RAND CORP., ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS at iii n.1 (2017).

[76] *Id.*

[77] Roger Park, *Guide to Zero-Day Exploits*, SYMANTEC CONNECT: BLOG (Nov. 9, 2015), http://www.symantec.com/connect/blogs/guide-zero-day-exploits.

[78] *See, e.g.*, *The Enterprise Immune System*, DARKTRACE, https://www.darktrace.com/technology (summarizing the company's approach to cyber threats as emphasizing machine learning and an "enterprise immune system") (last visited Oct. 6, 2017).

[79] Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 97 (2009).

[80] NRC REPORT, *supra* note 29, at 40.

[81] *Id.* at 41.

[82] U.S. SENTENCING COMM., REPORT TO CONGRESS: ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 9 (1996), https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/computer-crime/199606_RtC_Computer_Fraud_and_Vandalism_Offenses.pdf.

and severe" punishment.[83] If punishment is perceived to be lacking in any one of these areas, "the deterrent effect diminishes."[84] Some research even suggests that harsh penalties may actually exacerbate computer crime.[85]

The credible threat of in-kind counterstrikes may also have a punishment-derived deterrent effect,[86] but experts suggest that this approach may have limited applicability.[87] A core reason for this is that accurate attribution still remains elusive, and attackers will not feel deterred if they are confident in their anonymity.[88] Additionally, the legality of cybercounterstrikes is currently questionable at best. In 2008, a group of security researchers figured out how to dismantle a very large botnet, but they decided against acting on this knowledge out of concerns about legal liability.[89]

Under current conditions, therefore, deterrence by punishment seems inadequate. Similarly, deterrence by denial comes up short on credibility, especially for targets in the private sector.[90] With an ever-growing number of targets and vulnerabilities, defenders have to be prepared to defend everywhere against attackers who can strike anywhere.[91] If the attacker is denied success by one target, the attacker can just try a different attack method or a different target.

Future work should be done to explore how to credibly deter cyberattacks. For now, unfortunately, there does not seem to be an easy way forward to actually reduce the number of attempted attacks.

[83] *Id.*

[84] *Id.*

[85] Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 938 (2003).

[86] Sklerov, *supra* note 63, at 10.

[87] NRC REPORT, *supra* note 29, at 5.

[88] *Id.* at 41. Attribution efforts have improved over the last eight years since the NRC report was published, but accurate identification of aggressors remains a significant stumbling block.

[89] T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 527–28 (2010); Gregg Keizer, *Researchers Infiltrate Kraken Botnet, Could Clean It Out*, PCWORLD (Apr. 30, 2008), http://www.pcworld.com/article/145345/article.html; *cf.* Garrie & Reeves, *supra* note 29, at 1858–59 ("Active defense also opens the door for disproportionate retaliatory attacks that can cause collateral damage to innocent parties, especially when it is not clear who the target is.").

[90] NRC REPORT, *supra* note 29, at 305.

[91] Katyal, *supra* note 71, at 60.

3. De-escalate

After a cyberattack, victims switch to restoring their systems back to a pre-attack state. Costs of this stage include the costs of repairing systems and restoring data, among other things.[92] This stage also involves investigations, which can inform the victim's future security practices.[93] After a data breach, costs may include notifying affected parties and providing those parties with subscriptions to credit monitoring services.[94]

The Cybersecurity Framework created by NIST is divided into five functions: identify, protect, detect, respond, and recover.[95] De-escalation, or resilience, is centered in the fifth function, recovery.[96] The recover function in the Framework includes recommendations about recovery planning and how to implement and manage recovery plans.[97] Through the Cybersecurity Framework, the government has provided the private sector with centralized information about recovery practices as recommended by experts, mitigating some of the uncertainty facing business owners.[98]

Specific cyberinsurance policies are often drafted to cover the above described types of crisis management activities.[99] We consider insurance to be an element of de-escalation that is acquired prior to an event. Insurance coverage for cyberattacks often works alongside defensive measures, as insurers are likely

[92] *See* Henry Bodkin et al., *Government Under Pressure After NHS Crippled in Global Cyber Attack as Weekend of Chaos Looms*, TELEGRAPH (May 13, 2017), http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom.

[93] *See id.*

[94] *The True Cost of Data Breaches for Businesses, Consumers & the Payment Industry*, FIELD NATION (June 1, 2015), https://www.fieldnation.com/blog/the-true-cost-of-data-breaches-for-businesses-consumers-the-payment-industry.

[95] NAT'L INST. OF STANDARDS & TECH., *supra* note 68, at 7.

[96] *Id.* at 9.

[97] *Id.*

[98] The recover function is further divided into three categories: (1) recovery planning; (2) improvements; and (3) communications. In short, it emphasizes the importance of having plans for recovering from events, improving those plans as changes are needed, and communicating with others about recovery activities. *Id.* at 34–35.

[99] Anderson, *supra* note 7, at 604–05.

to demand that policyholders observe industry standards for security.[100] Some insurance companies also work with policyholders by providing fraud-prevention technologies or connecting the policyholders with security auditors.[101]

C. Existing Legal Framework

The United States does not currently have a comprehensive cybersecurity law.[102] Instead, there is a patchwork of fixes scattered throughout different levels of government.[103] Information technology regulation in the United States tends to err on the side of less regulation, but is this sustainable? Recently, leading cybersecurity expert Bruce Schneier testified before Congress that the newer threats to cybersecurity require government intervention due to market failure.[104]

The issue of whether and how to regulate cybersecurity evokes Kant's paradox of freedom. In an environment where there is no law, everyone is free—but in the absence of law, the strong control the weak, so the weak are not truly free.[105] The strong in cybersecurity are those in control of the production and distribution of insecure products, while the weak are those whose interests are harmed by the lack of emphasis on cybersecurity. This power imbalance could theoretically be corrected by the market, but this poses a separate challenge. If the market for computer products emphasized security as much as it emphasizes other features, there would be more demand for secure products. Instead, consumers are often ill-informed about security issues.[106] Unlike a set of features that can improve a user's

[100] Podolak, *supra* note 8, at 406–07 (noting, however, that industry standard security practices may still be inadequate or negligent).

[101] Anna Lee, *Why Traditional Insurance Policies Are Not Enough: The Nature of Potential E-Commerce Losses and Liabilities*, 3 VAND. J. ENT. L. & PRAC. 84, 89–90 (2001).

[102] Kosseff, *supra* note 11, at 401.

[103] *Id.*

[104] *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 4–6 (2016) (statement of Bruce Schneier, Security Technologist), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-SchneierB-20161116.pdf.

[105] Keith N. Hylton & Steven E. Laymon, *The Internalization Paradox and Workers' Compensation*, 21 HOFSTRA L. REV. 109, 117 (1992).

[106] *See* Michael Thornton, *You Can't Depend on Antivirus Software Anymore*, SLATE (Feb. 16, 2017), http://www.slate.com/articles/technology/future_tense/2017/02/why_you_can_t_depend_on_antivirus_software_anymore.html.

experience in an observable way, security is something that is only easily observable when it fails. More security testing before release would likely lead to higher prices for consumers, and it may prove challenging to convince consumers to pay more for an improvement that they cannot see.

One solution is to introduce regulations to induce the more powerful to act for the benefit of the less powerful, but again the paradox of freedom arises: the more laws there are governing how people act, the less free people become.[107] Cybersecurity is increasingly vital to society, so this balancing act across various economic actors will likely be ongoing.

1. Statutes

Statutory approaches to computer security issues are largely a patchwork process, with new provisions being added as needed to address specific problems. The current statutory approach to cybersecurity in the United States is largely backward-looking, and this, combined with its patchwork nature, makes it difficult to address future issues.[108]

One problem that statutes address to varying degrees is data breaches. Most states have laws about data breaches that address how companies should behave following a breach, but these are typically narrow and punitive rules.[109] Some states have additional data-privacy legislation. In California, for instance, the Song-Beverly Credit Card Act prohibits retailers from requiring customers to disclose personal identification information as a condition of accepting a credit card.[110]

There is no federal data-breach law yet, which creates considerable confusion for companies that may have to take different actions for customers in different states because of differing state data breach laws.[111] However, there are federal laws addressing specific data-privacy concerns, like the Children's Online Privacy Protection Act, the Video Privacy Protection Act, and the Health Insurance Portability and Accountability Act

[107] *Id.* at 117.

[108] Kosseff, *supra* note 11, at 406.

[109] *Id.* at 401–02.

[110] CAL. CIV. CODE § 1747.08(a)(2) (West 2011).

[111] *See* Kosseff, *supra* note 11, at 406 ("Accordingly, if a company experiences a data breach, it must devote significant time and staff to determining the states in which it must notify residents and regulators as well as the timing, form, and substance of the notification.").

(HIPAA), which all focus on the protection of data in narrow categories.[112]

There are also federal laws that focus on criminal liability or procedural issues. The Computer Fraud and Abuse Act is a federal law that prohibits a range of computer-based activities with varying subversive effects, but it does not address things like security standards or liability for anyone other than the attacker.[113] Congress made identity theft a federal crime with the Identity Theft and Assumption Deterrence Act of 1998, which criminalizes the act of producing, transferring, and possessing another's identification documents without authorization.[114]

In terms of investigatory schemes, Congress enacted the Stored Communications Act (SCA) in the 1980s. This statute includes provisions about how stored data can be disclosed to the government, either through voluntary or compelled processes.[115] Because its language has not been significantly updated, the SCA makes some very outdated distinctions between "electronic communication services" and "remote computing services."[116] Several commentators have urged amending the SCA and its parent statute, the Electronic Communications Privacy Act (ECPA).[117] Courts have also been tasked with evaluating the Fourth Amendment and how it applies to digital evidence; some of these analyses overlap with the SCA's provisions about compelled disclosure.[118]

[112] Patrick P. Gunn et al., *The Health Insurance Portability and Accountability Act Privacy Rule: A Practical Guide for Researchers*, 42 MED. CARE 321, 321 (2004); Kosseff, *supra* note 11, at 401–02.

[113] Computer Fraud and Abuse Act, 18 U.S.C § 1030 (2012).

[114] Identity Theft and Assumption Deterrence Act of 1998, *Id.* § 1028; Garrie & Reeves, *supra* note 29, at 1841.

[115] Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2710.

[116] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004).

[117] *E.g.*, Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails To Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 653 (2011); Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 313 (2010); Casey Perry, U.S. v. Warshak*: Will Fourth Amendment Protection Be Delivered to Your Inbox?*, 12 N.C. J.L. & TECH. 345, 364 (2011). The Wiretapping Act is another part of the ECPA that guides digital investigations, and it applies to data in transit. 18 U.S.C. §§ 2510–2522 (2012).

[118] *E.g.*, Riley v. California, 134 S. Ct. 2473, 2495 (2014) (holding that a cell phone's contents could not be searched without a warrant as part of a search incident to arrest); United States v. Graham, 824 F.3d 421, 427–28 (4th Cir.

There are many challenges with applying existing law to emerging cybersecurity problems, though that is outside the scope of this Article. Suffice it to say that the current statutory regime is woefully inadequate for addressing modern threats. At a minimum, Congress needs to enact federal data-breach legislation to address some of the economic uncertainty of cybersecurity risks.

2. Litigation

In the absence of clear ex ante guidelines, courts are increasingly being asked to evaluate liability issues following cybersecurity events. The 2013 breach of the retail giant Target was met with over 140 lawsuits.[119] Some of the claims against Target alleged harm caused by the company's violation of state data breach notification laws.[120] Not only are a lot of suits being filed, they are also being filed very quickly. For example, within two weeks of the discovery of Home Depot's data breach in September 2014,[121] consumers and financial institutions had already filed suits in federal courts.[122]

Though it remains difficult to identify with certainty the parties responsible for cyberattacks, civil lawsuits provide an avenue of redress against those who failed to safeguard data. One option under the common law is negligence, though the duty of care required for data protection is far from clear.[123] Many data-breach plaintiffs assert claims based on violations of common law and statutes. In *Galaria v. Nationwide Mutual Insurance Co.*, plaintiffs alleged invasion of privacy and negligence, common-law claims, and also argued that the company's behavior amounted to a violation of the Fair Credit Reporting Act

2016) (holding that historical cell site location data can be obtained from a mobile service provider using a special order under the SCA instead of a warrant).

[119] Podolak, *supra* note 8, at 376.

[120] Anderson, *supra* note 7, at 562.

[121] *Banks: Credit Card Breach at Home Depot*, KREBSONSECURITY (Sept. 2, 2014), https://www.krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot.

[122] Podolak, *supra* note 8, at 375.

[123] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261–63 (2007) (arguing that there may be a duty to safeguard sensitive data, but ultimately questioning the usefulness of negligence to address data protection issues).

(FCRA).[124] In a case involving data stolen from a government contractor, plaintiffs alleged violations of both the federal Privacy Act and FCRA, in addition to common-law claims for negligence and breach of contract, among others.[125] In some cases, the Uniform Commercial Code may come into play when evaluating whether the businesses' security practices were commercially reasonable.[126]

There have been several stumbling blocks for data-breach litigation. We will highlight two of these: the scope of data-breach statutes, and standing. As noted above, most states already have their own data-breach notification laws. The effectiveness of these laws for supporting data-breach litigation, however, varies. In Illinois, for example, the Personal Information Protection Act requires notification after a breach, and also states that a violation under the Act is also an unlawful practice covered by the Illinois Consumer Fraud and Deceptive Business Practices Act.[127] However, in *Cooney v. Chicago Public Schools*, a state appellate court found no violation of the data breach notification law because the law only created a duty to notify affected parties, not a duty to safeguard information.[128] Moreover, the *Cooney* court held that the state Consumer Fraud Act did not apply because the increased risk of identity theft did not constitute an economic injury.[129]

The actionability of increased risk of identity theft under state law is also related to the second major stumbling block: Article III standing. In 2013, the Supreme Court decided *Clapper v. Amnesty International* to clarify the doctrine of Article III standing for future harms.[130] In *Clapper*, the Court was asked to decide if Amnesty International had standing to challenge the constitutionality of warrantless surveillance under section 702 of the Foreign Intelligence Surveillance Act.[131] The Court concluded that the organization had no standing because the feared

[124] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 384 (6th Cir. 2016).

[125] *In Re*: Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 21 (D.D.C. 2014).

[126] Edward H. Klees, *The "Fandation" of Risk: Does a Banking Client Get Its Money Back After Cyber Theft?*, BUS. L. TODAY, May 2016, at 1, 2.

[127] 815 ILL. COMP. STAT. 530 / 20 (2017).

[128] Cooney v. Chi. Pub. Sch., 943 N.E.2d 23, 28 (Ill. App. Ct. 2010).

[129] *Id.* at 31.

[130] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013).

[131] *Id.* at 1138.

future warrantless interception was not "certainly impending."[132] The requirement that allegations of future harm must be certainly impending is problematic for digital privacy injuries. Following *Clapper*, several district courts declined to find standing in data-breach cases where the asserted injury was an increased risk of identity theft.[133]

Other courts have reached the opposite conclusion. In *Remijas v. Neiman Marcus Group*, the Seventh Circuit concluded that plaintiffs had standing due to the substantial risk of future injury following a data breach.[134] In *Remijas*, the Seventh Circuit noted that in *Clapper*, the standing issue was based on uncertainty over whether surveillance had taken place.[135] In other words, the data collection itself was speculative. The data breach at issue in *Remijas*, on the other hand, was not speculative. There had been a data breach and third parties had improperly gained access to sensitive customer information.[136] The Seventh Circuit thus concluded that it was plausible to infer a substantial risk of harm stemming from the data breach sufficient to find Article III standing.[137] In September 2016, the Sixth Circuit joined the Seventh Circuit in this reasoning, when it reversed a district court's conclusion that data breach plaintiffs lacked standing in the *Galaria* case.[138]

Remijas and *Galaria* both represent a willingness by federal appellate courts to conclude that data-breach victims have standing. If other jurisdictions follow suit, that may remove one

[132] *Id.* at 1152.

[133] Case v. Miami Beach Healthcare Grp., 166 F. Supp. 3d 1315, 1319–20 (S.D. Fla. 2016); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 961 (D. Nev. 2015); Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 582–83 (E.D.N.Y. 2015*); In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 25–28 (D.D.C. 2014).

[134] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 384–85 (6th Cir. 2016) (reversing district court's finding that data breach victims lacked standing).

[135] *Remijas*, 794 F.3d at 693.

[136] *Id.*

[137] *Id.* Another aspect of *Remijas* that is worth mentioning is the court's reference to Neiman Marcus's offer of free credit monitoring for affected customers. The court remarked that "it is unlikely that [Neiman Marcus] did so because the risk is so ephemeral that it can safely be disregarded." *Id.* at 694. This quote may prove to be a double-edged sword. Will companies reconsider the practice of offering free credit monitoring to customers affected by data breaches in order to more easily preserve an argument against Article III standing?

[138] *Galaria*, 663 F. App'x at 384–85.

of the early road blocks encountered by data-breach litigants, enabling more cases to be decided on the merits. More decisions on the merits in data-breach cases will, in turn, increase the need for risk shifting to minimize losses, and increase participation in the cyberinsurance marketplace.

3. Administrative Actions

Administrative agencies have also been involved to varying degrees. The Securities and Exchange Commission (SEC), for instance, has issued guidance documents about cybersecurity because of the impact that security events can have on stock prices.[139] The Department of Homeland Security (DHS) operates the National Cybersecurity and Communications Integration Center to coordinate responses with the private and government sectors.[140] DHS also operates the Office of Cybersecurity and Communications to focus on critical information infrastructure.[141] The Department of Health and Human Services (HHS) has released guidance on the interplay between the NIST's Cybersecurity Framework and the HIPAA Security Rule.[142]

So far, however, the Federal Trade Commission (FTC) has arguably been the most active agency in the data-security arena. The FTC has brought actions against companies with inadequate security practices under its authority to investigate unfair or deceptive acts or practices.[143] Section 5 of the FTC Act gives the FTC the authority to declare business practices to be unfair, and thus unlawful, if the practices cause "substantial injury" to consumers.[144] Many FTC actions end in settlements or consent decrees.[145] For example, in August 2014, the FTC settled charges against Fandango and Credit Karma regarding the companies'

[139] *See* Anderson, *supra* note 7, at 531.

[140] Garrie & Reeves, *supra* note 29, at 1847.

[141] *Office of Cybersecurity and Communications*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/office-cybersecurity-and-communications (last updated Sept. 12, 2017).

[142] Office for Civil Rights, *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html (last visited Oct. 6, 2017).

[143] Podolak, *supra* note 8, at 376 (citing Gregory D. Podolak, *Cyber Risk Coverage Litigation Heats Up as Exposure and the Insurance Market Evolve*, 24 ABA INS. COVERAGE LITIG. 2 (2014)).

[144] Gilmore & Armillei, *supra* note 5, at 39.

[145] *See id.*

failures to adequately secure sensitive information that customers submitted through their mobile applications.[146]

In 2015, the Third Circuit affirmed the FTC's authority in *FTC v. Wyndham*, concluding that the FTC may rightly consider a cybersecurity practice unfair when that practice has resulted in harm to consumers.[147] Past consent decrees indicate that unfair cybersecurity practices include not protecting against "commonly known or reasonably foreseeable attacks," not encrypting data, not using an intrusion-detection system, and not providing cybersecurity training to employees.[148]

This characterization of the FTC's authority, however, is inherently backward looking. The FTC and the Third Circuit both acknowledge that the FTC lacks the authority to require the adoption of "fair information practice policies."[149] Section 5 also addresses unfair practices that are "likely to cause" substantial injury,[150] but, so far, the FTC has not attempted to assert prescriptive authority to establish specific cybersecurity standards. Unfair cybersecurity practices have thus largely been in the realm of "I know it when I see it," with the FTC providing little, if any, concrete guidance for what makes data security practices adequate.[151]

A more forward-looking approach to security can be seen in the National Institute of Standards and Technology (NIST), which published the Cybersecurity Framework in response to President Obama's Executive Order 13,636.[152] The Cybersecurity Framework is a voluntary, performance-based standard that is directed at increasing the security of critical infrastructure, though it can be useful for other industries as well.[153] The Cy-

[146] *FTC Approves Final Orders Settling Charges Against Fandango and Credit Karma*, FTC (Aug. 19, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-orders-settling-charges-against-fandango.

[147] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015).

[148] *E.g.*, LabMD, Inc., No. 9357 (F.T.C. July 29, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf; Gilmore & Armillei, *supra* note 5, at 40.

[149] *Wyndham Worldwide*, 799 F.3d at 248.

[150] 15 U.S.C. § 45 (2012); Gilmore & Armillei, *supra* note 5, at 39.

[151] Kosseff, *supra* note 11, at 410.

[152] Exec. Order No. 13,636, 3 C.F.R. 217 (2014); *Cybersecurity Framework*, *supra* note 12.

[153] *Cybersecurity Framework*, *supra* note 12.

bersecurity Framework centralizes information about best practices and is a helpful guide for businesses that want to make sure that they are doing all that they can to reduce their risk.[154]

4. International Law

International cyber conflicts are beyond the scope of this Article, but we offer a brief introduction to the issues to support an awareness of the massive scope of cybersecurity problems.

Cybercrime complicates the application of laws. Because cybercrime passes through national borders frequently, jurisdictional issues can be contentious.[155] The European Convention on Cybercrime (ECC) is a treaty that aims to address this difficulty by standardizing cybercrime laws and encouraging cooperation between nations.[156] However, treaties are only enforceable against countries that sign them, and to date, only fifty-nine countries have signed the ECC.[157] Of some of the more cyber-active countries, the United States and Israel have ratified the ECC, but Russia and China have not.[158]

Cyberspace conflicts between nation states introduce a lot of new problems. While the ECC is potentially useful when a private citizen of one country hacks a private citizen of another country, things get much messier when the victim or attacker is a nation state.[159] At that point, the United Nations Charter and the laws of war start to apply. There are two aspects of the law of war: *jus ad bellum*, which is the law of conflict management and applies prior to a conflict, and *jus in bello*, which is the law of armed conflict and applies during a conflict.[160]

[154] *Id.*

[155] *E.g.*, Deb Shinder, *What Makes Cybercrime Laws So Difficult To Enforce*, TECHREPUBLIC (Jan. 26, 2011), http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce.

[156] Sklerov, *supra* note 63, at 63–64. The ECC is also known as the Budapest Convention. *Details of Treaty No. 185*, COUNCIL OF EUR., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (last visited Oct. 6, 2017).

[157] Council of Europe, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2003). Ghana will probably be added soon to the ECC. *Cabinet Approves Ghana's Accession to Budapest Convention*, GHANA BUS. NEWS (Nov. 23, 2016), https://www.ghanabusinessnews.com/2016/11/23/cabinet-approves-ghanas-accession-to-budapest-convention.

[158] Council of Europe, *supra* note 157.

[159] *See* Garrie & Reeves, *supra* note 29, at 1850–51.

[160] Sklerov, *supra* note 63, at 27.

The UN charter is primarily concerned with *jus ad bellum* and the rules governing state relations prior to war. The UN charter prohibits use of force by states, with an exception for self-defense in response to an armed attack.[161] The *Caroline* standard for self-defense under international law focuses on whether the response was necessary and proportionate.[162] But when dealing with cyberweapons instead of kinetic weapons, it is unclear what constitutes a use of force or an armed attack. This and other ambiguities led to the creation of the Tallinn Manual by a group of experts working with NATO.[163] The Tallinn Manual is non-binding, but it does provide some guidance for how traditional approaches to conflict might apply to cyber conflict.[164]

D. NEED FOR A NEW, COMPREHENSIVE MODEL

Cybersecurity is a crisis of our time. The threats are growing faster than the defenses, and the technology is evolving faster than the law.[165] It is difficult to catch the actual bad actors, so courts, legislatures, and administrative agencies are left weighing liability issues for the database operators who are often victims themselves. Courts are often being asked to consider data breaches and similar events through a negligence framework, but the threats may evolve too quickly for defendants to know what they should be doing to act within their duty of care.[166] Citron suggests that strict liability could be a more effective framework than negligence,[167] but this has not yet been tested effectively.

Too many of the efforts to address today's cybersecurity concerns are backward-looking. In principle, the reasoning resembles the res ipsa loquitur doctrine of negligence: the fact that the event happened at all indicates that the protections were inadequate.[168] The analysis then attempts to identify which weaknesses in cyberprotection may have enabled a successful attack.

[161] U.N. Charter art. 2, ¶4, art. 51; David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 88 (2010).

[162] Garrie & Reeves, *supra* note 29, at 1854–55.

[163] *Research*, NATO COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, https://ccdcoe.org/research.html (last visited Oct. 6, 2017).

[164] *Id.*

[165] *See, e.g.*, Citron, *supra* note 123, at 255.

[166] *Id.* at 268.

[167] *Id.* at 243.

[168] *Res Ipsa Loquitur*, BLACK'S LAW DICTIONARY (10th ed. 2014).

Policymakers should avoid relying on this kind of ex post analysis.

Cybersecurity, though, is a conceptually tricky area. It is easy to see when cybersecurity practices are bad, but if the practices are good, they are invisible. This is one of the reasons why NIST's Cybersecurity Framework is important. Establishing standards of conduct before a crisis can mitigate the worst of an event.

There are other regulatory alternatives as well. Kosseff suggests that Congress could enact a law directing the FTC to develop a safe harbor program for cybersecurity that would partially protect compliant companies from lawsuits or regulatory action.[169] Kosseff also suggests tax incentives for cybersecurity practices[170] and the creation of a national cybersecurity insurance system.[171]

The degree of government involvement needed in the cyberinsurance market is an open question. Insurance companies are increasingly offering insurance coverage for cyber events, but this coverage is not yet fully developed as an insurance product.[172] Government support in this arena can help insurance companies and policyholders adapt to the changing market. This is also not without precedent. Congress created the National Flood Insurance Program (NFIP) to improve the ability of property owners to obtain flood insurance.[173] NFIP uses an incentive model of legislation that is largely voluntary, but that provides benefits to states for participation.[174]

Cybersecurity policy requires cooperation between the government and the private sector. Insurance is a private-market solution to the problem of unavoidable risk. In the following Part, we will explore issues of insurance and risk shifting more fully, and the respective roles available to the government and various private-sector actors.

[169] Kosseff, *supra* note 11, at 412.

[170] *Id.* at 415–16.

[171] *Id.* at 416–18.

[172] *See Why 27% of U.S. Firms Have No Plans To Buy Cyber Insurance*, INS. J. (May 31, 2017), http://www.insurancejournal.com/news/national/2017/05/31/452647.htm.

[173] Christine M. McMillan, Comment, *Federal Flood Insurance Policy: Making Matters Worse*, 44 HOUS. L. REV. 471, 475–76 (2007).

[174] *Id.* at 479.

II. RISK SHIFTING

Risk can be defined as the probability of an adverse occurrence times the severity of the consequences if it occurs.[175] Many desirable activities are nonetheless plagued by risk. Insurance policies allow individuals to hedge against adverse events without abandoning risky pursuits and their possible rewards. There are four ways to manage risk: (1) risk mitigation; (2) risk avoidance; (3) risk acceptance; and (4) risk transfer.[176] Nobel Prize–winning economist Kenneth Arrow notes that if individuals are unable to buy protection against uncertainty, a loss of welfare can result.[177]

This Article is most concerned with the practice of transferring risks, especially in the context of cybersecurity. However, reduced risk is often accompanied by a moral hazard, because people may act carelessly when they do not bear the risk of failure.[178] People may also fail to prepare for risks because they underestimate the likelihood of an adverse event.[179] One version of this is the gambler's fallacy, where people begin to think that something is more likely simply because it has happened in the past.[180] If someone flips a coin nine times, and the coin comes up heads each time, the chance of the coin coming up heads on the tenth coin flip is still fifty percent. The gambler's fallacy would make someone erroneously conclude that the chance of a head or tail flip is something other than fifty percent.

This Part will primarily focus on insurance, which is the main device used for the transfer of risk. There are two key problems with the cyberinsurance industry as it exists today. First, informational asymmetry is rampant, because insurers do not have a guaranteed way to evaluate a potential client's cyber risk,

[175] Harrington, *supra* note 38, at 17. This can be described with an equation like $R = PI$ (risk equals probability times impact). *See id.*

[176] *Id.*

[177] Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609, 612 (1962).

[178] *Id.* at 613; Bailey, *supra* note 20, at 16. Bailey enumerates three types of moral hazard: (1) ex ante moral hazard, where the party fails to take optimal precautions; (2) ex post moral hazard, where the party fails to do enough to mitigate harm after an occurrence; and (3) fraud, or the possibility that someone will exaggerate the loss. *Id.* at 16–17.

[179] Adam F. Scales, *A Nation of Policyholders: Governmental and Market Failure in Flood Insurance*, 26 MISS. C.L. REV. 3, 9 (2006).

[180] *Id.*

so insurers charge higher premiums to cover their own uncertainty.[181] When premiums increase, an adverse selection problem emerges, where those with high cyber risk continue purchasing insurance while those with low risk instead focus on self-insurance.[182] This is the well-known lemons market problem, where only one party has full information about whether a product is a good or bad investment, leading to a distribution of quality in the market that is skewed towards lower-quality products.[183] For cybersecurity insurance, the informational asymmetry generally favors the policyholder who knows their systems to a greater degree than is possible for the insurer. If premiums are too high, only firms at greatest risk might seek insurance. On the other hand, if premiums are too low, the insurer may be subsidizing harmful behavior.[184] Currently, insurance companies use long and arduous surveys to evaluate potential clients' cyber-risk exposure, but this approach still relies on self-reporting.

The second key problem is data scarcity, in that there is not currently enough information about cyber risks in general.[185] This ties in to the informational asymmetry problem, because a lack of information about risks makes it more difficult for insurers to conduct accurate risk assessments.[186] There will be greater uncertainty and informational asymmetry if policyholders fail to disclose their own cyber risks related to their own IT infrastructure. This makes it difficult to systematically assess cybersecurity risk in various market sectors. Finally, there is global uncertainty about the scope of cyber risks.[187]

We note, however, that there is also an increasing interest in alternative risk transfer (ART) techniques.[188] Insurers often work with banks in this arena, such as when derivatives are

[181] *See* Chao-Hung Christophe Chen, *Information Disclosure, Risk Trading and the Nature of Derivative Instruments: From Common Law Perspective*, 4 NAT'L TAIWAN U. L. REV. 1, 18 (2009).

[182] Athenia Bongani Sibindi, *The Art of Alternative Risk Transfer Methods of Insurance*, RISK GOVERNANCE & CONTROL: FIN. MKTS. & INSTS., 2015, at 229; Scales, *supra* note 179, at 8–9.

[183] George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 492–93 (1970).

[184] Bailey, *supra* note 20, at 33–34.

[185] *Where Cyber Insurance Underwriting Stands Today*, *supra* note 26.

[186] *See id.*

[187] Bailey, *supra* note 20, at 38.

[188] Sibindi, *supra* note 182, at 223–24.

used as part of risk management.[189] ART markets have a lot of potential, especially in emerging risk classes.[190] Ultimately, ART techniques could potentially address cybersecurity risks in a way that traditional insurance policies cannot.

A. THE ECONOMICS OF RISK

Decision makers weigh a variety of costs when deciding a course of action. Economists refer to some costs as externalities when these costs affect external conditions more than they affect decision makers.[191] Because of the lack of immediate effect, externalities are often not given as much consideration as other costs.[192] For example, a factory owner has to determine how to dispose of waste from production activities, and they decide that the easiest disposal method is to dump the waste in a nearby river. The factory owner does not experience the downstream effects of this dumping, so the decision is economically appealing. Government regulations motivate decision makers to internalize these externalities.[193] If the cost of responsible disposal is less than the factory owner could expect to pay in noncompliance fines, the factory owner will probably comply until the disposal costs go up or the fines go down.

The problem of externalities is one reason why legal regimes may apply liability rules. In his seminal work, *The Costs of Accidents*, Calabresi argued that tort liability should generally attach to the lowest-cost avoider—that is, the party that can most cheaply avoid the accident.[194] In the data-breach context, this will generally be the database operator whose security controls are compromised.[195] By imposing liability on database operators for events like data breaches, the court system is edging network operators closer to the internalization of externalities.

[189] *Id.*; Christopher Kampa, *Part 1: A Broad Overview*, *in* ALTERNATIVE RISK TRANSFER: THE CONVERGENCE OF THE INSURANCE AND CAPITAL MARKETS 3 (2010), http://www.insurancestudies.org/wp-content/uploads/2010/07/ISI_Insurance-Convergence-Series-Part-I.pdf.

[190] Sibindi, *supra* note 182, at 230.

[191] *Externality*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[192] *Pigouvian Taxes*, ECONOMIST (Aug. 19, 2017), https://www.economist.com/news/economics-brief/21726709-what-do-when-interests-individuals-and-society-do-not-coincide-fourth.

[193] *See id.*

[194] GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 26–29 (1970); Citron, *supra* note 123, at 284.

[195] Citron, *supra* note 123, at 284–85.

Unlimited liability, however, could potentially stifle innovation.[196] This is where the risk-shifting function of insurance becomes more valuable. The goal of cybersecurity insurance should be to encourage policyholders to continue to internalize the larger societal costs of inadequate cybersecurity while reducing the risk of open-ended liability.[197]

Externalities are pervasive in cybersecurity, because the larger social costs of insecurity are often not borne by network operators.[198] Security is also costly, and many organizations would arguably prefer to focus on activities that generate profit.[199] With finite resources, therefore, a company that makes an Internet-connected device might prefer to invest in making the device cheaply over making the device with security in mind.

One possibility that has been raised by economists is to subsidize security investments.[200] Another proposal involves creating a new role for internet service providers (ISPs) as providers of insurance against cyber risk.[201] These kinds of interventions would mitigate some of the externality problems. In this Article, we are primarily concerned with the traditional model of insurance that uses a dedicated insurance company to help clients manage risks. Ultimately, insurance policies provide an economic tool for managing risks, and our concern is about how the lessons of the industry can be applied to improve cybersecurity.

B. INSURANCE

At its core, the insurance industry is about shifting risks from those with less ability to pay to those with more ability to

[196] *Cf.* Malika Kanodia, *The Fate of the Injured Patient in the Wake of* Riegel v. Medtronic*: Should Congress Interject?*, 32 HAMLINE L. REV. 791, 801 (2009) (noting that "lawsuits stifle research and product innovations" in the medical device context).

[197] *See* Hylton & Laymon, *supra* note 105, at 111–12 (discussing the goal of internalizing external costs).

[198] *See id.* at 113 ("According to the theory of externalities, economically inefficient decisions result from a divergence between private and social incentives."); Scales, *supra* note 179, at 19 (noting that rational actors are likely to act in a way that brings them an immediate benefit when the long-term consequences are something for which they will not be responsible).

[199] *See* Jun Zhuang, *Impacts of Subsidized Security on Stability and Total Social Costs of Equilibrium Solutions in an N-Player Game with Errors*, 55 ENGINEERING ECONOMIST 131, 132–33 (2010) (discussing reasons why people might still choose to not invest in security).

[200] *Id.* at 143.

[201] Radosavac et al., *supra* note 28, at 48.

pay, enabling those who might have been hobbled by risks to take actions to benefit both themselves and society. The insurance industry accepts premiums from policyholders, and in return, the policyholders get peace of mind.[202] In the absence of insurance, a small business owner could potentially be driven out of business by a slip-and-fall accident that occurred on their premises. Insurance companies effectively pool risk and distribute that risk among all of the members of the pool.[203]

People routinely purchase insurance policies to protect themselves against accidents or other adverse events. Insurance coverage is often socially desirable, and in some situations, insurance is mandatory. Mortgage lenders frequently require borrowers to have home insurance.[204] Almost every state requires drivers to carry insurance on their vehicles. In the case of auto insurance, making sure that drivers have insurance coverage helps to ensure that if a driver causes harm to persons or property, that harm can be redressed.

Insurers have several options for protecting their profitability. By diversifying their risk portfolios, for instance, they can reduce the likelihood of having more claims than they can pay.[205] Insurance companies also frequently require policyholders to use risk-reduction strategies.[206] For example, insurance companies can raise and lower premiums in response to the policyholder's actions, offsetting the moral hazard problem.[207] A driver who has a car accident may find that their insurance premiums increase significantly. Insurance companies can also offset their risks by participating in the reinsurance market.[208] Reinsurance is basically insurance for insurers.[209]

Another way that insurance companies protect their investments is by pooling and sharing loss data with other insurance companies.[210] In other industries, this kind of cooperation would

[202] Sibindi, *supra* note 182, at 223.

[203] Tamar Frankel & Joseph W. LaPlume, *Securitizing Insurance Risks*, 19 ANN. REV. BANKING L. 203, 204 (2000).

[204] Scales, *supra* note 179, at 17–18.

[205] McMillan, *supra* note 173, at 485.

[206] Scales, *supra* note 179, at 5.

[207] Bailey, *supra* note 20, at 18–19.

[208] McMillan, *supra* note 173, at 487–88.

[209] Sibindi, *supra* note 182, at 225.

[210] Bailey, *supra* note 20, at 28, 35; McMillan, *supra* note 173, at 485; Scales, *supra* note 179, at 5 ("Without reasonably accurate data to generate loss predictions, insurance cannot be correctly priced.").

raise red flags for possible antitrust violations, but the McCarran-Ferguson Act carves out exceptions for the insurance industry.[211]

There are a lot of decisions to be made when shaping an insurance policy. The Insurance Services Office (ISO) is a private entity that is largely responsible for developing the language of policy forms.[212] Insurers also need to decide how they will determine premiums, such as whether the premium is based on the industry or whether the premium is determined retrospectively, based on the client's claims from the previous year.[213] A policy may also be based on claims made, or it may be based on occurrences. A claims-made policy covers claims that are reported during the policy period, while an occurrence policy covers incidents that occur during the policy period without regard to when the claim is filed.[214]

One frequent concern for insurance companies is the problem of correlated risks. A lot of risks are uncorrelated, like the likelihood that two specific people will be in a traffic accident on the same day.[215] If a risk is correlated, that means that a large number of claims are likely to arise from the same harmful event.[216] Hurricanes are a classic example of a correlated risk. If a hurricane lands in a populated area, a lot of people are likely to file claims for property damage caused by high winds and floods.[217] Scales notes that correlation leads to more variability in losses, and thus higher premiums.[218] One of the challenges of the fledgling cyberinsurance market is that it is not always clear whether cyber-event losses are correlated or uncorrelated. If a virus is disseminated through spam e-mail, the harms caused by that virus may be considered correlated. However, more targeted

[211] 15 U.S.C. §§ 1011–1015 (2012).

[212] Scales, *supra* note 179, at 21; Podolak, *supra* note 8, at 377 (noting that ISO's process is almost legislative in nature).

[213] Hylton & Laymon, *supra* note 105, at 145 (discussing retrospective premiums in the context of workers' compensation insurance).

[214] Craig F. Stanovich, *The Claims-Made CGL Policy*, INT'L RISK MGMT. INST. (Nov. 2012), https://www.irmi.com/articles/expert-commentary/the-claims-made-cgl-policy; *see also* Willy E. Rice, *Insurance Decisions – A Survey and an Empirical Analysis*, 35 TEX. TECH. L. REV. 947, 1009–10 (2004) (discussing a case concerning claims-made policies).

[215] Scales, *supra* note 179, at 10.

[216] McMillan, *supra* note 173, at 485–86.

[217] *See* Scales, *supra* note 179, at 3 (discussing interdependencies in responding to catastrophes).

[218] *Id.* at 11.

attacks may be considered uncorrelated. The nature of cybercrime, unfortunately, can make it very difficult to distinguish between different types of attacks.

Exclusions are a frequently litigated aspect of insurance policies. Scales cynically notes that insurers often seek to exclude coverage for accidents that are of the type that the policy was clearly intended to cover.[219] Scales acknowledges that market segmentation may be part of the reason for this behavior.[220] If a homeowner's policy includes an exclusion for mold, the homeowner has an incentive to purchase additional coverage for mold. Through market segmentation, the experiences of customers and companies can be more tailored to their respective needs. Some commentators have noted that insurance companies seem to be fighting claims more than they might have in the past, which may be related to broad concerns about the economy.[221] We observed in our research that exclusions are often central to contested claims.[222]

In addition to excluding certain causes of loss, insurers may also use exclusion language to limit coverage when the policyholder does not do enough to avoid a risk. An exclusion for a cyberinsurance policy might, for example, exclude coverage for events if the policyholder failed to keep their security software updated.[223]

Anti-concurrent causation language may further complicate coverage. Such language basically says that excluded events are still excluded from coverage even when they are not the sole cause of a loss.[224] Some insurers have attempted to use anti-concurrent causation language to also exclude covered causes if an excluded cause contributed to a loss.[225] Consider a correlated risk like a hurricane, and a homeowner who has a policy that covers wind damage but excludes coverage for flood damage. A lot of the damage is likely to be attributable both to winds and

[219] *Id.* at 21.

[220] *Id.* at 22.

[221] Hite, *supra* note 16, at 10; Scales, *supra* note 179, at 4 ("As with healthcare, the system for allocating catastrophic loss is characterized primarily by the evasion of responsibility at all levels: private, commercial, and governmental.").

[222] *See infra* Table 5 (noting that ninety-three of the cases with outcomes at the time of this writing involved exclusions).

[223] Zureich & Graebe, *supra* note 38, at 198.

[224] Scales, *supra* note 179, at 30.

[225] *Id.*

flooding. Anti-concurrent causation language potentially provides the insurer with a contract-based argument for why none of the damage is covered by the policy.

This Article is primarily focused on insurance for cybersecurity events, so the most relevant potential policyholders are businesses. When businesses are considering insurance coverage, they typically consider first-party coverage and third-party coverage.[226] First-party coverage applies to the policyholder's losses from things like damaged property and lost earnings.[227] An all-risk policy is a broad type of first-party policy.[228] Third-party coverage is about the policyholder's potential liability to others who have been injured. CGL policies are generally the broadest type of third-party coverage. Companies may also have errors & omissions policies (E&O), crime policies, and directors & officers policies (D&O), and if the business wants more coverage, they may also purchase umbrella policies.[229] Lawyers and other professionals often have professional liability policies.[230]

The extent to which these traditional policies cover losses from cybersecurity events, however, is a frequent point of contention.[231] For claims that involve injuries to property, CGL policies have traditionally emphasized physical loss or damage, though some policies may include coverage for loss of use of tangible property.[232] As businesses have become more reliant on computers, coverage for intangible losses has seemed to grow, with a number of courts concluding that data-loss injuries are covered[233]—but as those losses themselves grow, coverage for

[226] Michael Sean Quinn, *The Cyber-World and Insurance: An Introduction to a New Insurance*, 12 J. TEX. INS. L. 20, 22 (2013); Bailey, *supra* note 20, at 11; Zureich & Graebe, *supra* note 38, at 197.

[227] *See* Anderson, *supra* note 7, at 584 (discussing business interruption coverage).

[228] Lee, *supra* note 101, at 85.

[229] Anderson, *supra* note 7, at 542; Bailey, *supra* note 20, at 12; *see also* Podolak, *supra* note 8, at 397 (describing an insurer's liability under a crime insurance policy).

[230] *See* Zureich & Graebe, *supra* note 38, at 196 (noting the extent to which professional liability policies may cover cyber claims).

[231] Anderson, *supra* note 7, at 542–43; Bailey, *supra* note 20, at 12; Zureich & Graebe, *supra* note 38, at 193.

[232] Lee, *supra* note 101, at 86.

[233] *See* Anderson, *supra* note 7, at 578–79 (discussing coverage for first party losses as a result of cyber events).

those losses has seemingly shrunk with the addition of new exclusions.[234]

1. Insurance Law

Insurance law is generally based on contract law, and likewise is governed by state law. Almost 150 years ago, the Supreme Court held in *Paul v. Virginia* that "[i]ssuing a policy of insurance is not a transaction of commerce[]" and thus the insurance industry is not included within Congress's purview under the Commerce Clause.[235] This view was largely overruled in 1944 in *United States v. South-Eastern Underwriters Ass'n*.[236] The *South-Eastern Underwriters* case concerned indictments over rate fixing by several entities. Chief Justice Stone dissented from the decision, stating that "the rule of stare decisis embodies a wise policy because it is often more important that a rule of law be settled than that it be settled right."[237] Congress may have agreed with Chief Justice Stone, as they passed the McCarran-Ferguson Act of 1945 the following year, officially deferring to states' authority to regulate the "business of insurance."[238]

Above, we noted that insurance companies often collaborate with each other to pool information about losses and rates. In most industries, cooperation among competitors violates federal antitrust law, but this is not the case in the insurance industry.[239] In passing the McCarran-Ferguson Act, Congress declared that it was in the public interest to leave regulation and taxation of the insurance industry to the states.[240] The Act applies to the "business of insurance."[241] States may have different interpretations of what constitutes the business of insurance, though most of them use some version of the three-prong test crafted by the Supreme Court.[242] In *Union Labor Life Insurance Co. v. Pireno*, the Supreme Court held that the business of insurance includes practices that: (1) have "the effect of transferring

[234] *See* Podolak, *supra* note 8, at 398 (noting ISO's creation of an exclusion for harm to electronic data).

[235] Paul v. Virginia, 75 U.S. (1 Wall.) 168, 183 (1868).

[236] United States v. S.-E. Underwriters Ass'n, 322 U.S. 533, 553 (1944).

[237] *Id.* at 579 (Stone, C.J. dissenting).

[238] 15 U.S.C. §§ 1011–1015 (2012).

[239] Hylton & Laymon, *supra* note 105, at 143.

[240] Bailey, *supra* note 20, at 25.

[241] 15 U.S.C. § 1011.

[242] *See* Bailey, *supra* note 20, at 26; Frankel & LaPlume, *supra* note 203, at 210.

or spreading a policyholder's risk"; (2) are "an integral part of the policy relationship between the insurer and the insured"; and (3) are "limited to entities within the insurance industry."[243]

The McCarran-Ferguson Act explicitly excludes the insurance industry from the reach of federal antitrust statutes, except on issues related to agreements or acts of boycott, coercion, or intimidation.[244] Parties have litigated questions about the extent to which the McCarran-Ferguson Act preempts the application of other federal laws, like the Federal Arbitration Act.[245] As the business of insurance has evolved to include unconventional approaches like alternative risk-transfer techniques, the degree to which state law will continue to preempt federal law may become a contentious issue, especially regarding the securitization of risks.[246]

One of the benefits of federal regulation is that the laws and enforcement are consistent between states.[247] Instead of a unifying federal regime, the insurance industry has the National Association of Insurance Commissioners (NAIC).[248] Among other things, NAIC provides model acts for how states should regulate insurers.[249] NAIC suggestions may include insurance rate regulations. Many states have regulations that allow for rates to be approved by the state provided that the rates are "adequate, not excessive, and not unfairly discriminatory."[250] Some regulators have been moving away from more involved rate regulations.[251] Randall warns that the largely private nature of NAIC and its lack of accountability to the general public indicate regulatory

[243] Union Labor Life Ins. Co. v. Pireno, 458 U.S. 119, 129 (1982); Rice, *supra* note 214, at 954–55.

[244] 15 U.S.C. § 1013 (2012).

[245] Rice, *supra* note 214, at 954 (discussing a Fifth Circuit case where the court concluded that the FAA was not preempted).

[246] Frankel & LaPlume, *supra* note 203, at 209.

[247] United States v. S.-E. Underwriters Ass'n, 322 U.S. 533, 551 (1944) ("The power confined to Congress by the Commerce Clause is declared in The Federalist to be for the purpose of securing the 'maintenance of harmony and proper intercourse among the States.'").

[248] Susan Randall, *Insurance Regulation in the United States: Regulatory Federalism and the National Association of Insurance Commissioners*, 26 FLA. ST. U. L. REV. 625, 629–30 (1999).

[249] Bailey, *supra* note 20, at 27.

[250] *E.g.*, TEX. INS. CODE ANN. § 2251.155 (West 2009); *see also* Angelo Borselli, *Insurance Rates Regulation in Comparison with Open Competition*, 18 CONN. INS. L.J. 109, 112–13 (2011).

[251] Borselli, *supra* note 250, at 141–42.

capture.[252] It is unclear how much of the insurance industry's profitability could reasonably be attributed to industry-friendly regulations proposed by NAIC.

In the health insurance industry, a lot of states have regulations pertaining to medical loss ratios. The federal Affordable Care Act also has a medical loss ratio provision. Such regulations require insurers to spend at least a specific percentage of their premiums on health care, leaving the remaining percentage to cover administration and marketing with the rest being the insurer's profit.[253] A minority of states also have broader excess-profit statutes that require insurers to refund to the policyholder a portion of their premiums if the insurer's profits exceed a particular threshold.[254] It may be worthwhile to consider the possibility of an analogous security loss ratio for cyberinsurance.

A lot of the insurance industry has a fairly low barrier to entry, allowing newer companies to enter the insurance market more easily.[255] Most states have minimum capital requirements for insurance companies, which serves as a barrier to entry, but also ensures that the market is not flooded by undercapitalized insurers.[256]

Insurance companies frequently deny or challenge claims. Some recent issues in insurance law have focused on whether insurance companies can recoup defense costs from policyholders and how to determine when a claim denial was made in bad faith.[257] Among other things, insurers may challenge whether a claim was based on an occurrence under the policy.[258] When

[252] Randall, *supra* note 248, at 639.

[253] Efthimios Parasidis, *Health Outcomes Metrics and the Role of Financial Derivative Instruments in the Health Care Industry*, 10 IND. HEALTH L. REV. 447, 461 (2013); *Explaining Health Care Reform: Medical Loss Ratio (MLR)*, KAISER FAMILY FOUND. (Feb. 29, 2012), http://kff.org/health-reform/fact-sheet/explaining-health-care-reform-medical-loss-ratio-mlr.

[254] *E.g.*, FLA. STAT. § 627.215 (2017); *see also* Hylton & Laymon, *supra* note 105, at 144, 152 (describing the extent to which specific states control the financial operations of insurers).

[255] Borselli, *supra* note 250, at 139.

[256] *See* NAT'L ASS'N OF INS. COMM'RS, UNIFORM CERTIFICATE OF AUTHORITY APPLICATION: STATUTORY MINIMUM CAPITAL AND SURPLUS REQUIREMENTS (2017), http://www.naic.org/documents/industry_ucaa_chart_min_capital_surplus.pdf; Hylton & Laymon, *supra* note 105, at 150–51.

[257] Hite, *supra* note 16, at 3–4.

[258] *Id.* at 8 (discussing a Virginia case where the court held that a commercial general liability did not apply to assertions that the insured's practices contributed to climate change issues in Alaska).

courts are asked to evaluate insurance policies, rules of construction vary depending on the affected party. Courts tend to view an insurer's duty to defend as being a broader obligation than its duty to indemnify.[259] Courts also typically construe coverage terms broadly and exclusions narrowly.[260] In spite of this, commentators sometimes perceive courts as being friendlier towards insurance companies than towards policyholders.[261]

2. Commercial Coverage and CGLs

In this Section, we will focus on CGL policies to provide insight into commercial insurance coverage. The strengths and weaknesses of CGL policies contribute to the health of the insurance industry in general, and are also very important to consider in light of our empirical analysis of coverage litigation.

Businesses often acquire CGL policies to protect against potential losses from third-party injuries.[262] The standard CGL policy drafted by ISO includes three main types of coverage: Coverage A applies to bodily injury and property-damage liability, Coverage B applies to personal and advertising liability, and Coverage C applies to medical payments.[263] CGL policies often impose on the insurer a duty to defend and indemnify the insured.[264]

In our analysis of cases, we found a large number of cases involving data-based harms where policyholders filed claims under their CGL policy, often under Coverage B.[265] The personal and advertising injury coverage typically includes privacy injuries caused by the "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[266] One of

[259] *E.g.*, America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 93 (4th Cir. 2003) ("And the obligation to defend is broader than the obligation to indemnify.").

[260] Scales, *supra* note 179, at 26.

[261] *See* Rice, *supra* note 214, at 1035–36 (noting the appearance of judicial bias in insurance cases).

[262] *See* Podolak, *supra* note 8, at 382 ("CGL insurance is the most common type of coverage found in corporate insurance programs . . . .").

[263] *Id.* at 380.

[264] Quinn, *supra* note 226.

[265] *Infra* Part III; *see also* Podolak, *supra* note 8, at 380 (noting that the extent of Coverage B "is routinely at issue in data/privacy breach coverage disputes").

[266] Anderson, *supra* note 7, at 544; Podolak, *supra* note 8, at 380; *see, e.g.*, Travelers Indem. Co. v. Portal Healthcare Solutions, LLC, 644 F. App'x 245,

the essential questions for CGL policy coverage in data-breach cases thus becomes whether the breach constitutes a publication.[267] Litigation has also emphasized Coverage A claims about bodily injury and property damage, in which case the focus tends to be on whether the claim arises from an injury to tangible property or the loss of use of tangible property.[268] Insurers have been increasingly challenging claims under both categories of coverage, making cyberinsurance more necessary to cover these modern injuries.[269]

Exclusions impose limits on coverage, and over the years, new exclusions have been added to standard CGL policies. Some of these exclusions are what we categorize as definitional exclusions, where the exclusionary language is added to a definition within the policy. In 2001, ISO altered the definition of property damage to exclude harm to electronic data.[270] Other exclusions are listed in sections about coverage, instead of in the definitions section of the policy. Policies often exclude claims about the policyholder's completed work, or claims that arise from intentional acts.[271] ISO recently amended the standard policy language to exclude coverage for injuries "arising out of any access to or disclosure of any person's or organization's confidential or personal information."[272]

As a creature of contract law, the interpretation of insurance contracts often turns on a court's interpretation of the language. For example, some coverage language refers to claims "arising out of" a type of injury, but other policies may refer to claims that "result from" a type of injury.[273] Podolak notes that "arising out of" tends to be interpreted more broadly than the phrase "result from."[274] The interpretation may also vary depending on

246–47 (4th Cir. 2016) (discussing whether an allegation that private information was posted online was sufficient to trigger an insurer's duty to defend).

[267] Podolak, *supra* note 8, at 383.

[268] Anderson, *supra* note 7, at 569–70 ("A leading insurance law authority notes that the issue as to whether 'computerized information is tangible property' has 'not been satisfactorily resolved.'").

[269] Bailey, *supra* note 20, at 12.

[270] Anderson, *supra* note 7, at 571; Podolak, *supra* note 8, at 398. *But see* Lee, *supra* note 101, at 87–88 (explaining how there may still be coverage if the policy covers loss of use of tangible property, depending on the injury).

[271] Anderson, *supra* note 7, at 574–75.

[272] Podolak, *supra* note 8, at 387; Zureich & Graebe, *supra* note 38, at 195–96 (emphasis omitted).

[273] Podolak, *supra* note 8, at 404.

[274] *Id.*

where it is in the policy. Scales observes that the phrase "arising out of" tends to be construed more broadly when it applies to coverage, and more narrowly when it applies to exclusions.[275]

3. Cyber Insurance

Arguments for electronic-harm coverage under a CGL policy are facing an increasingly uphill battle with recent amendments to standard CGL policy language. This is one reason for the increase in popularity of cyber-specific insurance policies. Cyberinsurance can be defined as "the transfer of financial risk associated with network and computer incidents to a third party."[276]

As insurers increasingly narrow their CGL policies to exclude claims for data breaches,[277] cyberinsurance becomes more necessary for businesses of all sizes. It is also possible that cyberinsurance will become essentially mandatory as vendors and clients increasingly draft contracts to require such policies.[278] Yet a 2013 study by the Ponemon Institute found that fewer than a third of respondents reported that their organization had cyberinsurance.[279]

Nelson and Simek report that the cyberinsurance market is "the fastest growing segment of the insurance industry."[280] The 2016 Betterley Report on the Cyber/Privacy Insurance Market notes that there has been a lot of growth in the number of policies being issued to small and midsized companies.[281] Policy

[275] Scales, *supra* note 179, at 26.

[276] Inger Anne Tøndel et al., *Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective*, *in* AVAILABILITY, RELIABILITY, AND SECURITY IN INFORMATION SYSTEMS 175, 175 (2016) (quoting Rainer Böhme & Galina Schwartz, Modeling Cyber-Insurance: Towards a Unifying Framework 1 (May 21, 2010) (working paper) (on file with the University of Minnesota Law Review)).

[277] Zureich & Graebe, *supra* note 38, at 195.

[278] Harrington, *supra* note 38, at 17.

[279] PONEMON INSTITUTE, MANAGING CYBER SECURITY AS A BUSINESS RISK: CYBER INSURANCE IN THE DIGITAL AGE 4 (2013), https://www.experian.com/innovation/thought-leadership/ponemon-study-managing-cyber-security-as-business-risk.jsp.

[280] Nelson & Simek, *supra* note 9, at 24; *see also* Harrington, *supra* note 38, at 17 (reporting a thirty-eight percent annual growth rate for the cyberinsurance market as of 2015).

[281] RICHARD S. BETTERLEY, BETTERLEY RISK CONSULTANTS, THE BETTERLEY REPORT: CYBER/PRIVACY INSURANCE MARKET SURVEY – 2016, at 5 (June 2016) (2016), https://www.irmi.com/docs/default-source/authoritative-reports/betterley-executive-summaries/cyber-privacy-media-liability-summary-2016.pdf.

makers at the highest levels have indicated interest in the cyberinsurance market.[282] The rapid growth of the cyberinsurance market presents a challenge for regulators, insurers, and policyholders.

Insurance companies are faced with many challenges when designing cyberinsurance policies. Above, we noted that premiums that are too low or too high can cause far-reaching problems.[283] There is also an inherent informational asymmetry, because the policyholder knows significantly more about their day-to-day risks than would the insurer. With cybersecurity policies, the uncertainty is magnified by a lack of actuarial data.[284] To the extent that cybersecurity risks are correlated risks, this greatly increases the insurer's risk exposure.[285]

Insurers work very hard to realistically identify and address these problems in policy language. Figure 1 illustrates how informational asymmetry between the insurers and the insured can create a vicious circle, resulting in an insurance market characterized by high premiums, broad exclusions, and insurance caps. All of these policy mechanisms are designed to address the downstream risks posed by adverse selection and moral hazard, which are present at the outset due to the informational asymmetry between the insurers and the insured. Ultimately, the only way to reliably address the problems in the cyberinsurance market is to improve risk assessment (which includes technological risk, legal risk, and portfolio risk), reduce informational asymmetry, and counteract data scarcity.

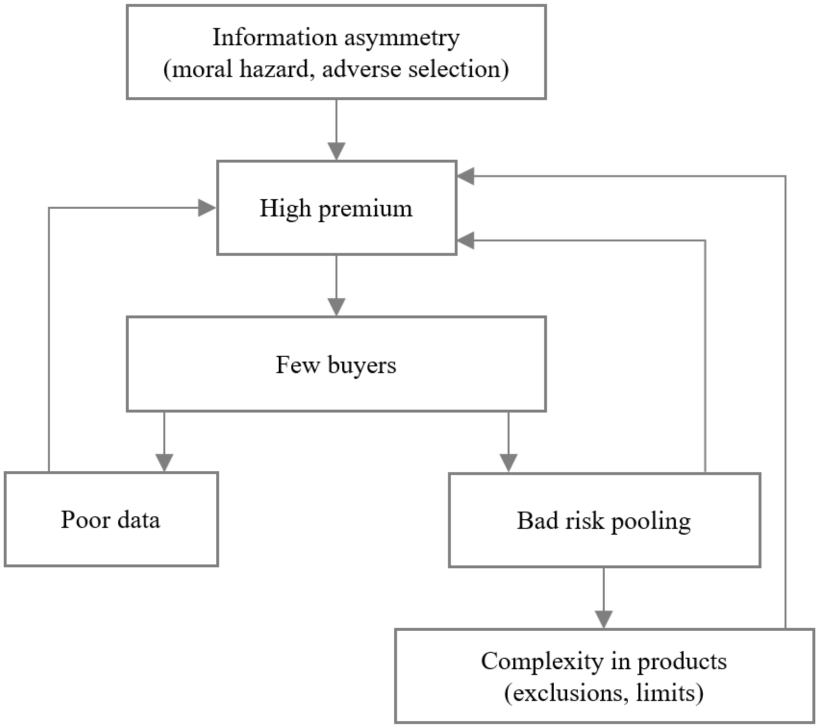
[282] Anderson, *supra* note 7, at 534 (discussing the White House's consideration of cyber insurance as a category of possible incentive for adapting the NIST's Cybersecurity Framework).

[283] *See supra* Part II.

[284] *Where Cyber Insurance Underwriting Stands Today*, *supra* note 26.

[285] RAINER BÖHME, VULNERABILITY MARKETS: WHAT IS THE ECONOMIC VALUE OF A ZERO-DAY EXPLOIT? 4 (2005), https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf; Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (2006).

Figure 1: Issues with the Cyberinsurance Market



ISO provides their subscribers with a standard form, the information security protection policy,[286] though this form may not be enough to address the constantly evolving risks. The market is affected by a lot of unknowns concerning the technology and the scope of the risks, further complicated by a lack of actuarial data.[287] Scales remarked that a major problem facing the National Flood Insurance Program was "[h]ow to price a product no

[286] Toni Scott Reed, *Cybercrime: Losses, Claims, and Potential Insurance Coverage for the Technology Hazards of the Twenty-First Century*, 20 FIDELITY L.J. 55, 79 (2014); *see also* Anderson, *supra* note 7, at 592 (referring to the policy's former name, Internet Liability and Network Protection Policy).

[287] Matthew Sturdevant, *When Terrorists Attack Online, Is Cyber-Insurance Enough?*, HARTFORD COURANT (Jan. 26, 2015), http://www.courant.com/business/hc-cyber-terrorism-insurance-20150126-story.html; Tøndel et al., *supra* note 276, at 177.

one had sold for thirty years, such that consumers would actually purchase it and the pool would remain solvent."[288] This observation is also an effective summary of one of the biggest problems faced by insurers who want to offer cyberinsurance. This uncertainty has a cost, as one study notes that the ratio of premiums to the coverage limit for cyberinsurance is triple the ratio of other liability policies and six times higher than the ratio for property insurance.[289]

We previously explained some of the frequent problems encountered when addressing cyber harms through technology and the law. In the previous Section, we discussed the narrowing of CGL policies to make it harder to successfully file claims over cyber harms like data breaches. Cyberinsurance has the potential to help mitigate both of these problems, if used correctly. Cyberinsurance is already a billion dollar market, but these policies continue to represent a mere sliver of the premiums collected for commercial-line insurance policies in the United States.[290]

In an earlier Part, we noted that one method that legislatures have used to address commercial cyber risks is to enact data breach statutes that require notification to affected individuals.[291] Cyberinsurance policies often cover these kinds of expenses.[292] However, data-breach statutes can cause a snag in claim disputes if the policy includes language prohibiting policyholders from making voluntary payments without obtaining prior approval from the insurer.[293] The question then becomes whether the expenses from breach notifications required by statute are voluntary.

Cyberinsurance policies have been evolving to address things like business interruption coverage, direct and indirect causation of privacy injuries and injuries caused by intellectual property infringement, and cyber extortion.[294] A cyber policy is likely to exclude property damage covered by real-world property

[288] Scales, *supra* note 179, at 15.

[289] HER MAJESTY'S GOV'T & MARSH, UK CYBER SECURITY: THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK 22 (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

[290] Bailey, *supra* note 20, at 41.

[291] *See supra* Part I.C.2.

[292] Podolak, *supra* note 8, at 400.

[293] *Id.* at 402.

[294] Quinn, *supra* note 226, at 21–23.

insurance, and real-world property insurance is likely to exclude cyber harms.[295] Major cyber policy providers include ACE, AIG, the Beazley Group, Marsh, Liberty International Underwriters, Chubb Corp., and Zurich Insurance.[296]

The moral hazard noted above with insurance generally is also prevalent with cyberinsurance. If a policyholder decides to invest in cyberinsurance instead of cybersecurity, this can increase the risk of loss.[297] To mitigate the moral hazard problem, any cyberinsurance solution must be accompanied by requirements for security audits.[298] Some cyberinsurance products offer risk management services, including privacy training and credit monitoring.[299] Coverage may include losses from extortion and various data-breach expenses, though the policy language may impose time limitations or require the use of designated crisis-management vendors.[300] These elements are intended to reduce some of the risk in this volatile environment.

Even so, cyberinsurance remains a risky field. A study of the Nordic cyberinsurance market notes that the lack of experience and data affects insurers' ability to assess risks in this emerging market.[301] The normal informational asymmetry exists between policyholder and insurer, but the overall risk to all policyholders is also a big unknown.[302] One possible solution is to create an independent body to allow insurers to share information about claim costs from data breaches and similar events.[303] Another

[295] *Id.* at 23.

[296] *Cyber Insurance*, AIG, http://www.aig.com/business/insurance/cyber-insurance (last visited Oct. 6, 2017); *Cyber Liability*, LIBERTY INT'L UNDERWRITERS, https://www.liu-usa.com/Pages/CyberLiability.aspx (last visited Oct. 6, 2017); *Cyber Risk Insurance*, MARSH, https://www.marsh.com/us/services/cyber-risk.html (last visited Oct. 6, 2017); Harrington, *supra* note 38, at 17; *see also* Podolak, *supra* note 8, at 400 (discussing the limitations of some companies' cyber policies).

[297] Bailey, *supra* note 20, at 21. Some critics question whether cyber insurance would help improve security at all. Harrington, *supra* note 38, at 17.

[298] Bailey, *supra* note 20, at 23; Podolak, *supra* note 8, at 406.

[299] Anderson, *supra* note 7, at 593; Harrington, *supra* note 38, at 18.

[300] Anderson, *supra* note 7, at 603, 605, 607–08.

[301] Tøndel et al., *supra* note 276.

[302] *Id.* at 177; Bailey, *supra* note 20, at 38 ("Unlike fire insurance or other traditional lines of property and casualty insurance, one of the most prominent issues in underwriting cyber-risk coverage is the lack of information regarding frequency, magnitude, and claim costs of both actual and potential data breach incidents.").

[303] Bailey, *supra* note 20, at 38–39.

proposal concerns putting ISPs in charge of cyberinsurance because of their control over the infrastructure,[304] though this may not work in all markets.

Some insurers attempt to address the unknown risks by requiring policyholders to comply with security standards in order for their security practices to be construed as reasonable.[305] In order for the cyberinsurance market to be profitable for insurers though, they need a lot of customers. To get a lot of customers, the insurer cannot set the bar too high in terms of how strong a potential client's security has to be to get insurance.[306] Historically, cyberinsurance providers have used questionnaires to assess potential clients, though it is becoming more common to have specific conversations with the potential clients to get a sense of their vulnerabilities and risk-management controls.[307] Insurers also sometimes use third-party cybersecurity specialists to evaluate a potential policyholder's risks.[308]

One of the differences between CGL policies and cyberinsurance policies concerns timing. CGL policies are often occurrence-based, while cyberpolicies are often claims-based.[309] This difference is likely out of necessity. CGL policies are typically designed to address injuries that are immediately apparent, like a slip-and-fall accident in a store. The date of the incident is often easy to discern, so it is trivial to determine whether the occurrence happened within the policy period. Compare this to a data breach, where the network operator may go a year or more without realizing that anything was lost. A claims-made policy is arguably better suited for a situation where there is a gap between when an incident occurs and when it is discovered.[310] For either type of policy, however, the policy will still likely have provisions concerning notice, and it may be wise for a policyholder to obtain a policy that has a provision for an extended reporting period.[311]

[304] Radosavac et al., *supra* note 28, at 43.

[305] Gilmore & Armillei, *supra* note 5, at 30.

[306] Tøndel et al., *supra* note 276, at 182.

[307] *Id.* at 178.

[308] *Id.* at 182.

[309] Anderson, *supra* note 7, at 609; Stanovich, *supra* note 214.

[310] *See* Templo Fuente De Vida Corp. v. Nat'l Union Fire Ins. Co., 129 A.3d 1069, 1077–78 (N.J. 2016) (comparing claims-made and occurrence-based policies in terms of notice requirements).

[311] Anderson, *supra* note 7, at 609.

C. Existing Schemes

Analogies are helpful when addressing a new problem in the legal field. Cybersecurity is no exception. This area may yet prove to be sui generis, but that hasn't stopped policy makers from trying to drum up concern by warning about a "Cyber Pearl Harbor,"[312] and some commentators have compared cybersecurity issues to things like floods caused by accidents at reservoirs[313] and the looting of antiquities from archaeological sites.[314] This Section follows this trend by juxtaposing cyberinsurance issues with workers' compensation on the one hand and NFIP on the other.[315] Zureich and Graebe have made similar observations about cyberinsurance issues and the growth of employment practice liability insurance during the 1990s.[316] In the latter situation, employment practice liability insurance emerged as a specialized coverage as insurers narrowed general liability policies to exclude these types of claims.[317] Another option, though one that we do not consider in detail, is the possibility of the government serving a reinsurance role, similar to its role under the Terrorism Risk Insurance Act.[318]

1. Workers' Compensation

We chose to look at the origin of workers' compensation insurance because, like cyber risks, the risk of worker injury is ubiquitous and hard to predict. The workers' compensation model focuses on the lowest-cost avoider, the employer.

One thing that we believe makes workers' compensation insurance a reasonable analog to cyberinsurance is the severity and frequency of possible injuries. Risk is often described as the product of the probability that an event will occur times the severity of the harm if it occurs.[319] Fire insurance is designed to

[312] *E.g.*, Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor,"* 18 VA. J.L. & TECH. 289, 293 (2014).

[313] Citron, *supra* note 123, at 243–44.

[314] Kesan & Hayes, *supra* note 30.

[315] The latter analysis builds on Jeff Kosseff's work. *See generally* Kosseff, *supra* note 11 (discussing ways to fix the current problems that exist with cybersecurity).

[316] Zureich & Graebe, *supra* note 38, at 197.

[317] *Id.*

[318] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002); Scales, *supra* note 179, at 45.

[319] Harrington, *supra* note 38, at 17.

address a devastating but fairly low-probability event.[320] Workers' compensation insurance is designed to address the higher probability of generally smaller injuries.[321] While there is a potential for catastrophic cyberattacks, most cyberattacks will not rise to that level,[322] yet the risk is still significant because the probability for a less-severe event is very high.

Scholars trace the origin of workers' compensation to Imperial Germany and then later to Great Britain, though the British law was less comprehensive than the German law.[323] Fowler points out that Caribbean pirates also had a form of workers' compensation, as crew members who lost body parts received a larger share of treasure based on their injuries.[324]

Workers' compensation is handled by states individually, so it is similar to how insurance in general is handled.[325] In 1972, there was an attempt to federalize workers' compensation because of deficiencies in state programs at the time, but the push for federalization fizzled out when a lot of states started reforming their workers' compensation systems voluntarily.[326]

The basic premise of workers' compensation is to provide financial protection for workers who are injured on the job.[327] The system provides injured workers with more certain remedies and allows workers and employers to avoid costlier tort litigation.[328] Workers' compensation was needed in part because employers

[320] Christian Schade et al., *Protecting Against Low Probability Disasters: The Role of Worry* 2 (Univ. Pa., Working Paper No. 2009-12-23, 2009).

[321] *See* Ginny Kipling, *Employer Tips for Managing Workers' Comp*, BENEFITS PRO (May 23, 2011), http://www.benefitspro.com/2011/05/23/employer-tips-for-managing-workers-comp?t=employee-participation&slreturn=1504563241 (asserting that while injuries are guaranteed, the vast majority are inconsequential).

[322] *See* Taylor Armerding, *Catastrophic Cyber Attack on U.S. Grid Possible, but Not Likely*, CSO (Apr. 15, 2016), http://www.csoonline.com/article/3055718/critical-infrastructure/catastrophic-cyber-attack-on-u-s-grid-possible-but-not-likely.html.

[323] David B. Torrey, *100 Years of Pennsylvania Workers' Compensation: History, the Current Scene, and Challenges Ahead*, 87 PA. B. ASS'N Q. 6, 8 (2016); Hylton & Laymon, *supra* note 105, at 136–37.

[324] Russell Fowler, *The Deep Roots of Workers' Comp: Pirates, Prussians and Progressives Are All in the Family Tree*, TENN. B.J. 10, 12 (2013).

[325] *See* Joan T.A. Gabel & Nancy R. Mansfield, *Practicing in the Evolving Landscape of Workers' Compensation Law*, 14 LAB. LAW. 73, 74–75 (1998).

[326] Torrey, *supra* note 323, at 12–13.

[327] Hylton & Laymon, *supra* note 105, at 136 (explaining the origins of workers' compensation).

[328] Gabel & Mansfield, *supra* note 325, at 75.

could use defenses like contributory negligence and assumption of risk to avoid civil liability for worker accidents.[329]

With the workers' compensation system, employees can recover medical expenses and a percentage of their lost income.[330] In return, employers and insurers are safe from more expensive litigation and the possibility of higher compensatory or punitive damages.[331] Another protection for employers is the exclusive remedy doctrine, which limits a worker to redressing their injuries through the workers' compensation system, instead of through civil litigation.[332] There are, however, many exceptions to the exclusive remedy doctrine.[333] For example, under California law, if there is fraudulent concealment of a worker's injury, the exclusive remedy doctrine does not apply.[334]

Workers' compensation insurance is mostly provided by private insurance companies,[335] but a handful of states operate state-managed insurance funds.[336] Many employees with workers' compensation claims will settle their dispute in exchange for a lump-sum payment, which benefits employers because they are able to close the case and shift the work injury cost to other nonoccupational payers such as Medicare.[337] In response to an increasing number of settlements that favored employers, many jurisdictions started to require the existence of a bona fide dispute about benefit entitlement before the injured worker can agree to a settlement.[338]

Workers' compensation cases involving standard injuries are less complicated than cases involving occupational illnesses that develop over a long period of exposure.[339] In the latter types of cases, employers are often successful in challenging coverage.[340] This may be due, in part, to most workers' compensation

[329] Torrey, *supra* note 323, at 7.

[330] Gabel & Mansfield, *supra* note 328, at 73.

[331] *Id.*

[332] *Id.*

[333] *Id.* at 73–74.

[334] Kimberly Wong, *The 5 Exceptions to the Workers' Compensation Exclusive Remedy Rule that Every Personal Injury Attorney Should Know*, VEEN FIRM (2014), http://www.veenfirm.com/News-Events/Publications/The-5-Exceptions-to-the-Workers-Compensation.shtml.

[335] Rice, *supra* note 214, at 1022.

[336] Hylton & Laymon, *supra* note 105, at 142.

[337] Torrey, *supra* note 323, at 16–17.

[338] *Id.* at 18.

[339] Hylton & Laymon, *supra* note 105, at 158–59.

[340] *Id.* at 158.

policies being occurrence-based instead of claims-made.[341] This is further support for why it is more appropriate to take a claims-made approach to cyber insurance policies, because, like asbestos exposure, the full effects of a cyberattack may be unknown until long after the initial security breach.

Premiums for workers' compensation insurance are often set using class rating or experience rating.[342] With class rating, the premium is based on the industry of the business.[343] With experience rating, the premium is calculated based, in part, on that business's losses from previous years.[344] Either of these approaches could work for establishing cyberinsurance premiums, though we recommend an alternative.

A less-common method for setting premiums is retrospective ratings. When ratings are set retrospectively, the policyholder will pay a minimum fee to the insurer, and then the insurer will take care of the costs during a policy period and bill the policyholder at the end of the policy period for the amount up to the policyholder's maximum out-of-pocket costs.[345] If there are no incidents one year, the firm's premiums may exceed their losses, but the next year may see a large number of incidents, such that the policyholder's losses reach the policy cap.[346] A retrospective rating approach may be an appealing option for cyberinsurance coverage for data breaches, because it provides a degree of flexibility as the insurers and policyholders adapt to new threats and new insurance products.

Workers' compensation statutes often include caps, at least for temporary and partial disabilities.[347] Some states also cap the compensation available for permanent total disabilities and

[341] *Unique Issues of Claims-Made Policies*, SCOTT SIMMONDS, https://www.scottsimmonds.com/bank-insurance-coverage/unique-issues-claims-made-policies (last visited Oct. 6, 2017).

[342] Hylton & Laymon, *supra* note 105, at 146.

[343] *Id.*

[344] *Id.* at 147–48.

[345] *Id.* at 145–46; Rice, *supra* note 214, at 1023.

[346] Hylton & Laymon, *supra* note 105, at 145–46.

[347] *See, e.g.*, *Permanent Partial Disability Award Schedules*, WASH. ST. DEP'T OF LAB. & INDUS., http://www.lni.wa.gov/CLAIMSINS/CLAIMS/BENEFITS/DISABILITY/PPDAWARDSCHEDS.ASP (last visited Oct. 6, 2017) (providing tables with maximum payouts for various types of partial disabilities).

fatalities.[348] In Arkansas, for example, the lifetime cap for permanent total disability is currently just over $200,000.[349] These caps are arguably not good public policy, but something similar might work in a modified approach to cyberinsurance, where the matter is less likely to be a life-or-death decision. For example, if data breach or identity theft insurance were widely available to individuals, a lifetime cap might make such a program more financially manageable. With current models, however, such a system is unlikely because consumers are rarely held liable for fraudulent charges.[350] In the alternative, regulations could potentially introduce minimum and maximum award amounts for individuals whose data is compromised in a data breach.

According to Fowler, workers' compensation statutes in the United States address eight common elements: (1) what triggers an entitlement; (2) a no-fault approach concerning the employee's injury; (3) only employees can receive benefits; (4) wage benefits are a percentage of the employee's weekly wage, and there is no compensation for pain and suffering; (5) the workers' compensation system provides the "exclusive remedy" available for a worker while receiving benefits;[351] (6) if a third party caused the worker's injury, the worker can sue the third party, but the financial award must be shared with the employer to reimburse the employer's costs; (7) the compensation system is state-run and not based on traditional judicial proceedings, the system tends to favor awarding benefits; and (8) employers must obtain insurance or meet self-insurance mandates to cover workers' compensation costs.[352] This informal legal framework for workers' compensation is helpful for shaping questions that can aid regulatory support of the emerging cyber insurance market.

[348] *E.g.*, *Workers Compensation Claim State Environmental Guide - Arkansas*, TRAVELERS, https://www.travelers.com/iw-documents/claims/workers-compensation/ce-10174wcbenefitoverview-ar.pdf (last visited Oct. 6, 2017) [hereinafter *Workers Compensation Claim*]; Hylton and Laymon, *supra* note 105, at 175.

[349] *Workers Compensation Claim*, *supra* note 348.

[350] *See* FTC, LOST OR STOLEN CREDIT, ATM, AND DEBIT CARDS 1 (2012), https://www.consumer.ftc.gov/articles/pdf-0075-lost-or-stolen-credit-atm-and-debit-cards.pdf.

[351] There are, however, some claims that an injured worker could still bring, such as those based on the Americans with Disabilities Act or the Family Medical Leave Act. Gregory B. Cairns & Amy L. Brewer, *Workers' Compensation, the ADA and the FMLA: The Ten Questions Most Commonly Asked by Colorado Employers*, 24 COLO. LAW. 2293, 2293 (Oct. 1995); Gabel & Mansfield, *supra* note 328, at 74.

[352] Fowler, *supra* note 324, at 11.

For example:

> (1) What triggers the payout for a cyber insurance policy?
> (2) Do any factors reduce the payout, like the policyholder's liability?
> (3) Who is eligible for coverage?
> (4) In the case of business interruption expenses, what kinds of expenses are covered? Cost of restoring services? Lost profits?
> (5) Does cyber insurance coverage affect legal rights? Would a data breach settlement affect legal rights?
> (6) How does coverage apply, and how should data breach litigation be affected, when a third party causes the injury?
> (7) Should cybersecurity event coverage issues be addressed through legislation? Could an insurance-based approach be adapted to reduce the costs of litigating data breaches?
> (8) Should the government mandate cyber insurance for companies of a certain size or in certain industry sectors involving critical infrastructure?

Looking at the third question, most discussion about cyberinsurance assumes that businesses will obtain cyberinsurance coverage. However, the workers' compensation system potentially provides a model for a consumer-facing approach where consumers, who are subjected to the risks of data insecurity by virtue of their participation in the modern economy, could be covered through a policy issued to data-service providers. This is one potential approach to cyberinsurance, though it may not be desirable because there are simply too many different entities with access to an individual consumer's information. An employer-focused system is much simpler for workers' compensation because most individuals only have one employer, but a similar dynamic does not exist with respect to information-related services.

2. National Flood Insurance Program

As a second part of our analysis, we chose to consider NFIP as a potential model for an approach to cyberinsurance. For homeowners and business owners, floods pose a huge risk that could destroy years of investment in a moment. Some regions are inherently at greater risk of flood, but many of these regions also have a lot of economic and agricultural value. It is economically sensible to allow people to purchase flood insurance to encourage investment in these regions.

Unfortunately, the demand for flood insurance is highest in flood-prone areas, but not so high in areas where floods are unlikely, leading to a market with poorly spread risk.[353] Congress enacted the National Flood Insurance Act of 1968 (NFIA) to create "a reasonable method of sharing the risk of flood losses."[354] Prior to the NFIA, flood insurance was a risky bet for insurance companies.[355] With the NFIP, the government provided some tools for offsetting some of that risk by, among other things, subsidizing flood insurance premiums.[356] The NFIP conditions participation in the program on commitments to regulate development in high-risk areas.[357] Because of its purpose as a risk-mitigating regulatory program, the NFIP could serve as a guide for future regulatory efforts to support cybersecurity and the cyberinsurance market.

Under the NFIP, the Federal Emergency Management Administration (FEMA) creates minimum standards for development in flood-prone areas, and once a community has adopted FEMA's guidelines, residents are able to purchase flood insurance.[358] FEMA drafts flood insurance policies and establishes community-specific insurance rates, and insurance companies act as agents of FEMA under the Write Your Own program.[359] With the Write Your Own program, the NFIP underwrites the policies, and the private insurers who sell the policies get approximately thirty percent of the premiums as commission.[360] Scales notes that this arrangement is similar to ERISA, in the sense that, under the latter, "private health insurers administer insurance contracts governed by federal common law, while being underwritten entirely by employers."[361]

[353] Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L.J. 783, 828 (2005).

[354] 42 U.S.C. § 4001(a) (2012); *cf.* Kosseff, *supra* note 11, at 417 (asserting that Congress enacted the NFIP to address the issue of "building homes on rivers and other floodplains").

[355] McMillan, *supra* note 173, at 486–87.

[356] *Id.* at 487.

[357] *Id.* at 476.

[358] *Id.* at 481.

[359] *Id.*; Scales, *supra* note 179, at 14.

[360] Scales, *supra* note 179, at 14.

[361] *Id.* at 32.

Sometimes with the NFIP, policyholders may be placed at a disadvantage compared to other types of insurance. The NFIP imposes some procedural requirements on policyholders, including a sixty-day deadline to submit proof of loss after a flood. Missing that deadline is often the basis for claim denials.[362] The fact that the private insurers are not underwriting flood claims can also create an incentive for insurers to categorize claims as flood damage so that the loss falls to the government instead of the insurer.[363]

A study by the American Institutes for Research cites several successes of the NFIP, including the successful prevention of billions of dollars of flood damage, reduction in federal expenditures, and the fact that millions of people are able to purchase flood insurance on their properties.[364] One study from 2006 estimated that "approximately one-half of homes most at risk are insured against flood."[365] It is somewhat surprising that the insurance rate is not higher, considering that banks and mortgage providers have ample financial incentives to require borrowers to purchase flood insurance in flood-prone areas.[366]

Subsidies are another core element of the NFIP. In part because of the lack of actuarial data, the NFIP initially subsidized flood insurance policies so that the program could start providing affordable services while the data was still being collected.[367] The NFIP was designed to gradually reduce the amount of subsidization over time, and as of a decade ago, somewhere between twenty-eight percent and thirty-five percent of NFIP policies were still subsidized.[368]

Some scholars, however, question whether the NFIP has actually been a boon or a bane for communities with high flood risks, like Houston, Texas. In 2001, Tropical Storm Allison destroyed entire neighborhoods in Houston with flooding, but by

[362] *Id.* at 33.

[363] *Id.* at 36–37 (noting that this is one of the problems that emerged in litigation over Hurricane Katrina).

[364] AM. INSTS. FOR RESEARCH, THE EVALUATION OF THE NATIONAL FLOOD INSURANCE PROGRAM FINAL REPORT 42 (2006), https://www.fema.gov/media-library-data/20130726-1602-20490-1463/nfip_eval_final_report.pdf.

[365] Scales, *supra* note 179, at 15.

[366] *Id.* at 18, 20.

[367] *Id.* at 15–16.

[368] Boardman, *supra* note 353, at 829 (citing a thirty-five percent subsidization rate); Scales, *supra* note 179, at 16 (citing a twenty-eight percent subsidization rate).

2007, many of those neighborhoods had been rebuilt with brand new townhouses.[369] Scales expresses criticism of flood control projects in general, asserting that such projects merely buy time.[370]

Some question whether this kind of flood program creates a moral hazard. When a community has flood controls in place and flood insurance available, more people may move to the community because they believe that it is now physically and financially safe to do so.[371] A community may have been safer with new controls at an earlier size, but growth encroaches further onto the floodplain, increasing the risk again.[372] By encouraging management instead of abandonment of floodplains, the NFIP may have actually increased economic risks.[373]

Local governments and developers are generally aware of flood risks,[374] but the availability of flood insurance allows parties to partially externalize the consequences. McMillan argues that through the mechanism of easily available flood insurance, the NFIP "encourages irresponsible behavior and contributes to loss of life."[375] Manns also notes that the federal government has historically undercharged for flood insurance.[376] If these criticisms are accurate, NFIP clearly has a moral hazard problem.[377] Scales suggests addressing the NFIP's weaknesses by gradually eliminating subsidies for everyone except low-income homeown-

[369] McMillan, *supra* note 173, at 473.

[370] Scales, *supra* note 179, at 6.

[371] *Id.*

[372] Beth Davidson, Note, *How Quickly We Forget: The National Flood Insurance Program and Floodplain Development in Missouri*, 19 WASH. U. J.L. & POL'Y 365, 388 n.147 (2005).

[373] Scales, *supra* note 179, at 13.

[374] *Local Official Survey Findings on Flood Risk*, FEMA, https://www.fema.gov/local-official-survey-findings-flood-risk (last updated Feb. 21, 2017); McMillan, *supra* note 173, at 475.

[375] McMillan, *supra* note 173, at 475.

[376] Jeffrey Manns, Note, *Insuring Against Terror?*, 112 YALE L.J. 2509, 2544 (2003).

[377] *Id.* at 2510–11 ("The federal government has a long history of offering subsidized insurance programs, such as flood insurance, that are rife with moral hazards and have often served no one's interests save the insured beneficiaries."); Robert J. Rhee, *Terrorism Risk in a Post-9/11 Economy: The Convergence of Capital Markets, Insurance, and Government Action*, 37 ARIZ. ST. L.J. 435, 492–93 (2005) (noting that "federal crop and flood insurance programs have had problems of adverse selection, moral hazards, poor underwriting and mismanagement").

ers, and by requiring all homeowner policies to include flood insurance.[378]

The NFIP provides a partial blueprint for a regulatory approach to cyberinsurance, but it also provides lots of warnings. Like flood insurance, cyberinsurance is an area where the risks are significant and often unpredictable. Government subsidies for cyberinsurance could support this growing market while more data is collected. More importantly, the broad availability of cyberinsurance will support further innovation in the information technology sector. The NFIP's Write Your Own model, however, appears to give insurers a windfall as they collect premiums without actually bearing the risk, and should not be adopted for cyberinsurance without significant changes. Ultimately, a cyberinsurance regulatory system must strike a balance between encouraging innovation and discouraging irresponsible investments.

D. Financial Markets

The cyberinsurance market is growing, but insurers are in a bind because of the lack of actuarial data. Alternative risk-transfer methods, especially those that employ financial markets, may be an effective alternative.[379] Sibindi argues that insurance has experienced a paradigm shift from indemnity to value enhancement.[380] Financial markets themselves have potential as a tool to improve cybersecurity,[381] and an approach to cyberinsurance that focuses on derivatives-based alternative risk transfer could hit two birds with one stone. Dozens of insurance companies already use derivatives in financial markets to hedge against risks.[382] Global banking giant Credit Suisse raised eyebrows (and capital) in 2016 when it created a catastrophe bond to cover itself against internal catastrophes like cyberattacks and rogue traders.[383] This Section therefore examines financial markets and their intersection with the insurance industry.

[378] Scales, *supra* note 179, at 44–45.

[379] Sibindi, *supra* note 182, at 223.

[380] *Id.*

[381] *See, e.g.*, Kesan & Hayes, *supra* note 30, at 782–83.

[382] *Capital Markets Special Report*, NAT'L ASS'N OF INS. COMM'RS, (July 15, 2011), http://www.naic.org/capital_markets_archive/110715.htm.

[383] Leslie Scism & Anupreeta Das, *'Cat Bonds' Rattle Insurance Industry*, WALL ST. J., Aug. 8, 2016, at A1.

The securitization of insurance risks is a topic that has received some attention.[384] Securitization can be defined as "a method of converting illiquid financial assets into liquid marketable assets."[385] Organizations can use securitization to transfer risks to investors in a way that is functionally similar to how insurance providers pool and distribute risk.[386] The potential legal issues of securitization of insurance are considerable. Should such practices be covered by state law as being part of the business of insurance? Should the securities be regulated by the SEC? To the extent that the securitized risks are cast as derivatives, that may also require the involvement of the Commodity Futures Trading Commission (CFTC).[387]

Alternative risk-transfer products generally function like financial instruments instead of traditional insurance policies.[388] Catastrophe bonds, or cat bonds, have a similar function. Catastrophe bonds have existed since the 1990s and were originally designed to insure against natural disasters.[389] Catastrophe bonds are a private-market solution, but they also typically fall within the SEC's regulatory power, providing some assurance of oversight.[390] In the past, catastrophe bonds have been traded as options at the Chicago Board of Trade.[391] Scales notes, however, that catastrophe bonds can have high transaction costs.[392] These costs are often related to their nature as securities, and can include things like underwriting fees, fees imposed by ratings agencies, and legal fees for things like preparing disclosures for investors.[393]

Insurance companies often seek their own insurance in the reinsurance market, and financial markets provide a distributed

[384] Frankel & LaPlume, *supra* note 203, at 203.

[385] *Id.*

[386] *Id.* at 203–04.

[387] *Id.* at 208, 219.

[388] Sibindi, *supra* note 182, at 224.

[389] Scism & Das, *supra* note 383.

[390] Scales, *supra* note 179, at 46; *Catastrophe Bonds and Other Event-Linked Securities*, FIN. INDUS. REG. AUTH., http://www.finra.org/investors/alerts/catastrophe-bonds-and-other-event-linked-securities (last updated Oct. 29, 2013).

[391] Sibindi, *supra* note 182, at 228.

[392] Scales, *supra* note 179, at 46.

[393] Véronique Bruggeman, *Capital Market Instruments for Natural Catastrophe and Terrorism Risks: A Bright Future?*, 40 ENVTL. L. REP. 10,136, 10,142 (2010).

alternative to reinsurance.[394] As such, a shift to securities like catastrophe bonds could potentially have negative effects on the reinsurance market.[395] In May 2016, Credit Suisse Group sold a variation of a catastrophe bond to insure itself "against the risk of rogue traders, cyber hacking and accounting fraud."[396] The long-term benefits and pitfalls of such bonds are currently unknown.

There are many possible forms that securitization could take in the cyberinsurance context. Parasidis presents a proposal for utilizing financial markets to address uncertainty in the health care industry, through the trade of derivatives based on health outcomes indices.[397] A similar model may be possible for cybersecurity using a security outcomes index, with a value that is tied to measures of security throughout different industries.

III. CYBERINSURANCE LITIGATION

In the preceding Part, we presented perspectives about the inadequacy of cybersecurity preparations, laws, and current approaches to cyber risk shifting. Addressing these problems requires, at the outset, an understanding of current benchmarks. For this reason, we have compiled and analyzed lawsuits concerning coverage issues and electronic harms.

In addition to providing a benchmark for more general recommendations, a study of relevant insurance litigation is also potentially very valuable for the overall goal of shaping cyberinsurance policies. To these ends, we thoroughly studied over 140 cases that implicate issues relevant to cyberinsurance, most of which were litigated through to a decision on the merits. For the cases that concerned third-party liability, almost all of the underlying litigation was between private companies or citizens. There were, however, three cases that examined insurance coverage for FTC actions.[398]

[394] Scales, *supra* note 179, at 46.

[395] Frankel & LaPlume, *supra* note 203, at 206–07; Scism & Das, *supra* note 383.

[396] Scism & Das, *supra* note 383.

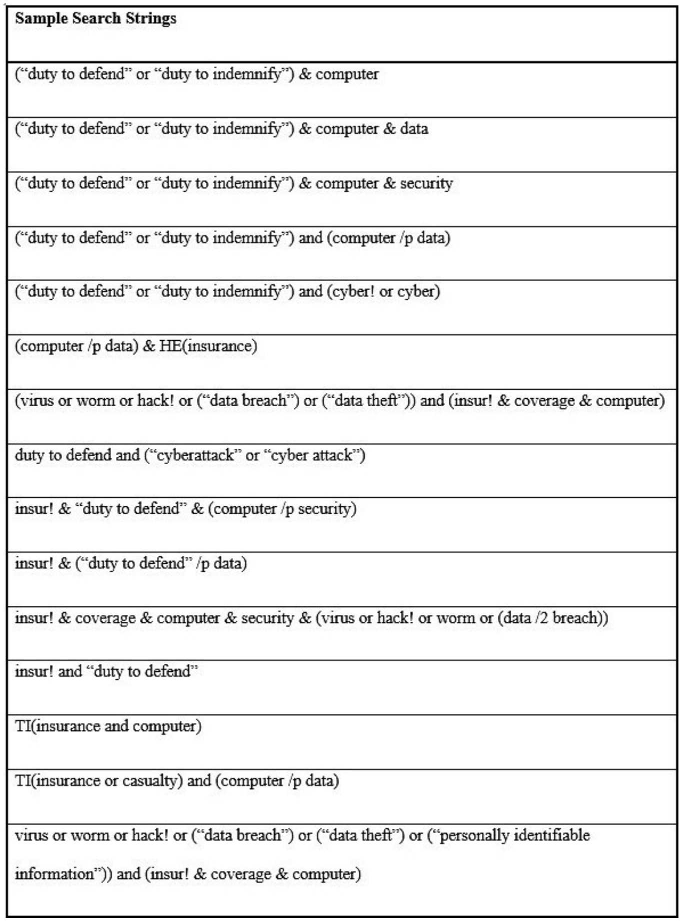
[397] Parasidis, *supra* note 253, at 448.

[398] *See* Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012); State Farm Fire & Cas. Co. v. Nat'l Research Ctr. for Coll. & Univ. Admissions, 445 F.3d 1100 (8th Cir. 2006); Complaint for Declaratory Judgment, Allied World Nat'l Assurance Co. v. DeVry Educ. Grp. Inc., No. 1:15-cv-01408 (N.D. Ill. Feb. 14, 2015).

A. Methodology

To obtain as many cases as possible, we searched Bloomberg Law and Westlaw using a variety of search terms, including those outlined in Table 1. In addition to cases identified with specific search terms, some cases were identified because they were cited in other cases.

Table 1: Sample Search Strings



Sample Search Strings
(“duty to defend” or “duty to indemnify”) & computer
(“duty to defend” or “duty to indemnify”) & computer & data
(“duty to defend” or “duty to indemnify”) & computer & security
(“duty to defend” or “duty to indemnify”) and (computer /p data)
(“duty to defend” or “duty to indemnify”) and (cyber! or cyber)
(computer /p data) & HE(insurance)
(virus or worm or hack! or (“data breach”) or (“data theft”)) and (insur! & coverage & computer)
duty to defend and (“cyberattack” or “cyber attack”)
insur! & “duty to defend” & (computer /p security)
insur! & (“duty to defend” /p data)
insur! & coverage & computer & security & (virus or hack! or worm or (data /2 breach))
insur! and “duty to defend”
TI(insurance and computer)
TI(insurance or casualty) and (computer /p data)
virus or worm or hack! or (“data breach”) or (“data theft”) or (“personally identifiable information”)) and (insur! & coverage & computer)

We also searched federal dockets in Bloomberg Law by filtering for the insurance contract nature-of-suit code (110) and looking for keywords including (data /2 breach) and the prefix cyber. A shortcoming of Bloomberg Law searches that should be noted is that these searches were limited to information in the dockets. If these terms were found within the names of the parties or their contact information, or if the terms were in the description field of the docket, these cases would be identified by the search. The searches would also find litigation documents that had already been uploaded to the docket pursuant to a request from another party, provided that the documents were in a format that allowed for their text to be searched with an automated tool.

The suit-code-limited Bloomberg Law search yielded 80 results when looking for (data /2 breach) and 254 results when looking for the prefix cyber. There was some overlap between the two, and we also uncovered the aforementioned issue with Bloomberg searches. While examining the over 300 cases, we had to manually request the complaint in approximately 100 cases. One of the reasons that there may have been more search results for cyber is that it is a fairly common prefix that we found to also be used as part of the contact e-mail addresses for several attorneys. We also found a small number of cases that did not seem to be properly categorized as insurance litigation. In addition, we found a small number of cases that were relevant to our study but that were categorized with suit code 109 (Contract: Other).[399]

We then reviewed all of the results of each search string and identified the cases with the most potential relevance to cyberinsurance disputes. Once the universe of cases was identified, we consolidated those cases into a single spreadsheet and populated the spreadsheet with standard case information: case name, citation, docket number, date of filing, and date of disposition, among numerous other fields. Currently, we have 146 fully analyzed cases in our CLAD repository.

Selection bias is an important concern in virtually any empirical study, and this study is no different. By focusing on litigation, our study is inherently concerned with insurance claims that are disputed, rather than the potentially hundreds or thousands of claims that an insurance company pays without challenge or reservation. Because of this selection bias, our study should not be viewed as a comprehensive guide about insurance

[399] *E.g.*, Complaint, Marion State Bank v. Everest Nat'l Ins. Co., No. 3:16-cv-01436 (W.D. La. Oct. 13, 2016) (using the cause of action code "12:635 Breach of Insurance Contract").

activity. It is, however, a good representation of the more contentious issues that arise in cyber-related insurance litigation, since these claims could not be resolved without initiating litigation, and, in most of the cases in our database, continuing litigation through to a decision on the merits.

Furthermore, our database is not comprehensive with regard to insurance coverage for privacy injuries, because that is outside the scope of our current analysis. In creating our database, we focused on intangible harms that were reasonably connected to technology issues. Because of our interest in intangible harms, some of the cases that we analyzed focused on intellectual property infringement. We chose to exclude many cases involving privacy rights created by statute, like the Telecommunications Consumer Privacy Act (TCPA) and the Fair Credit Reporting Act (FCRA). Our database includes some TCPA and FCRA cases, but those are limited to cases where the issues were more centered on computers and information technology. Future work might examine litigation and insurance disputes involving these specific statutes.

Because insurance law is generally left to the states, it is possible that there were many more state cases than we were able to access. Each state has its own method of record keeping, and, while it is fairly easy to find information about trial-level federal litigation, most states do not make detailed trial information available in an easily searchable form on the web or through the subscription services that our researchers could access.

B. RESULTS AND ANALYSIS

We tracked a large number of variables across cases, including the duration of litigation and where the cases were litigated. Where possible, we analyzed both the district court and appellate court opinions, so our database includes some cases at multiple court levels. In total, we identified 121 unique cases. Of the 121 unique cases, 68 cases were brought by the insured after a claim denial, and 53 cases were brought by an insurer seeking a declaratory judgment that there was no coverage. Because some of these cases were affirmed and some were overturned, we will generally discuss our data in terms of the overall number, 146 cases.[400]

[400] There is an exception for situations where the total number of cases was lower for other reasons, such as the analysis focusing on cases that were decided

Table 2: Case Duration, Federal and State

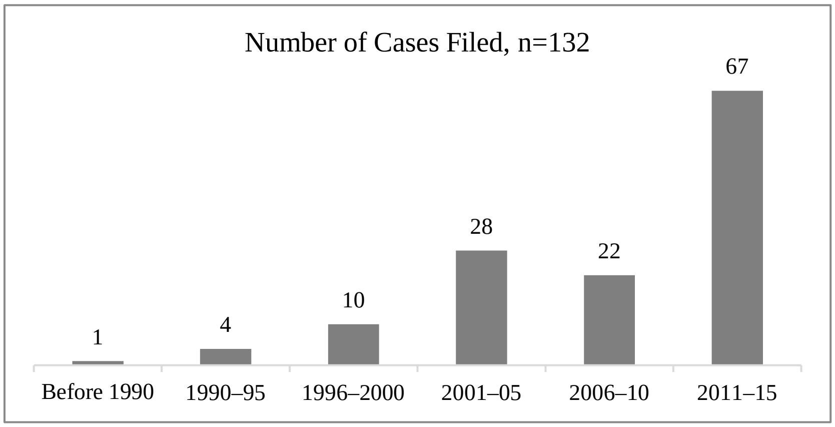
Duration	Federal	State
< 1 year	37	4
1–2 years	40	9
2–3 years	12	4
3–4 years	9	2
4+ years	4	2
N/A	2	5
Ongoing	14	2
Total	118	28

Of the 146 cases in our database, 118 were in federal court and 28 were in state court. We categorized cases by duration. If litigation lasted for 11 months or less, it was categorized as < 1 year. If litigation lasted between 12 to 23 months, we categorized this as "1–2 years." The "2–3 years" category was for cases that lasted between 24 and 35 months, the "3–4 years" category was for cases that lasted between 36 and 47 months, and litigation that continued for 48 months or more was placed into the "4+ years" category. At the time of this writing, there were 14 ongoing federal cases and 2 ongoing state cases. The cases in the "N/A" row of Table 2 currently have unknown status for one reason or another. Approximately 33.9% of cases in federal court were resolved within 1–2 years, compared to approximately 32.1% of cases in state court. Seventy-five percent of federal cases were resolved within 3 years.

We were unable to identify a filing date in 7 cases, and we have identified 7 cases so far that were filed in 2016. The latter number is likely to increase as more cases progress to stages where their documents become more searchable. Figure 2 depicts 5-year increments to illustrate how the number of cases filed on these topics has increased over the last 30 years.

by a judge or jury, in which instance we omitted cases that were settled or ongoing.

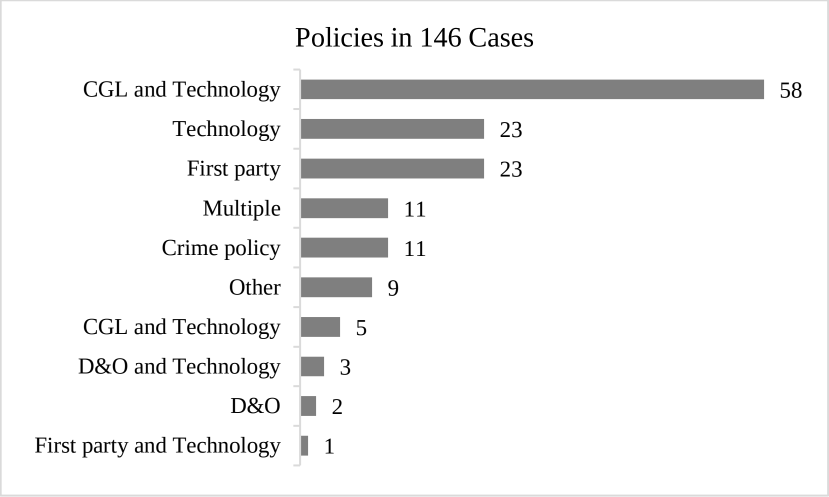
Figure 2: Cases by Filing Year



We also tracked cases according to the type of policy at issue. There were cases involving attorney malpractice policies, business income insurance policies, technology errors and omissions policies, umbrella policies, crime policies, and CGL policies, among others. The descriptive names of the policies in the cases varied, and we categorized the cases into several groups according to the type of policy at issue: CGL policies, crime policies, D&O policies, first party policies, technology policies, multiple policies, and a catch-all category for other policies.[401] We further identified which cases involving multiple policies involved a technology-related insurance policy. As the following figure shows, we identified 58 cases that involved just a CGL policy, and 5 cases that involved a CGL policy and a technology-related policy. The 11 cases in the "Multiple Policies" category did not involve a technology-related policy. In Figure 3, the policy categories are listed in the order they appear in the pie chart, starting with 58 cases involving CGL policies and proceeding clockwise.

[401] The "other" category is the category to which the attorney malpractice policy case was assigned. The other cases in this category involved home insurance, a garage liability policy, four professional liability policies, a contract with a payment processor and an acquiring bank, and a bond. The last two cases were very relevant to our inquiry into cyber-risk-shifting, though they were not traditional insurance policies.

Figure 3: Policy Type



Of the 146 cases, 39.2% of the cases solely concerned CGL policies. A number of other cases focused on CGL policies and other kinds of policies at the same time, and for our purposes, we considered cases that involved a CGL policy and an umbrella policy to pertain to multiple types of policies. Of the 146 cases, 15.8% of the cases were solely concerned with a technology-related policy. Several other cases focused on a technology-related policy and another kind of policy. We considered a policy to be technology-related if the coverage focused on events relating to computers and data. Including cases involving multiple policies, there were 32 cases where a technology policy was raised. Most of these cases were technology errors and omissions policies, though there were also some that were explicitly meant to cover cybersecurity events.

There were many different CGL policy provisions at issue in the analyzed cases. For example, many cases focused on the idea of tangible property and asked several questions, such as (1) is loss of data a harm to physical property?; (2) is loss of data considered direct physical damage?; and (3) is economic loss a harm to tangible property? Several cases also concerned provisions about the loss of use of tangible property, and others examined whether intellectual-property theft was a form of property damage. Cases also often focused on identifying the injury for policy purposes, and the injury categories under the policies included personal injury, advertising injury, and privacy injury.

One case that involved claims of property damage stemming from a data breach is *RSVT Holdings, LLC v. Main Street America Assurance Co.*[402] The burger chain Five Guys experienced a data breach in 2011, and was sued by Trustco Bank for over $100,000 for the fraudulent charges and the cost of replacing 1701 debit cards.[403] RSVT Holdings, the parent company of Five Guys, filed suit against its insurer in New York state court, seeking a declaration that the insurer had a duty to defend RSVT in the underlying action.[404] RSVT based its argument on the provision in its CGL policy covering "property damage."[405] Property damage under the policy was defined as including injury to, or loss of use of, tangible property.[406] The trial court ruled for RSVT, but the appellate court reversed the decision and found for the insurer.[407] The policy's definition of tangible property specifically excluded electronic data, and the appellate court concluded that negligent handling of the electronic data of customers did not result in property damage under the policy.[408]

Some cases turned on the personal and advertising injury provisions of CGL policies. For example, in *Travelers Indemnity Co. v. Portal Healthcare Solutions, LLC*, the relevant policy language concerned publications as a personal or advertising injury.[409] More specifically, the case concerned the publication of material that "give[s] unreasonable publicity to . . . [a person's] private li[fe]."[410] While the *RSVT* case focused on data breaches as a form of property damage, the *Portal* case considered data breaches as a form of personal or advertising injury. The Fourth Circuit affirmed the district court's judgment that the exposure

[402] RSVT Holdings, LLC v. Main St. Am. Assurance Co., 136 A.D.3d 1196 (N.Y. App. Div. 2016). At the time of this writing, LexisNexis cites the name of the plaintiff as RVST Holdings instead of RSVT Holdings. It is also listed as RVST in the PDF of the order. It is listed as RSVT in Bloomberg Law and Westlaw. RSVT Holdings, LLC is registered in Albany, NY. We have reported this discrepancy to LexisNexis.

[403] *See* Eric Anderson, *Insurer Won't Have To Cover Five Guys' Data Breach*, TIMES UNION (Feb. 18, 2016), http://blog.timesunion.com/business/insurer-wont-have-to-cover-five-guys-data-breach.

[404] *RSVT Holdings*, 136 A.D.3d at 1197.

[405] *Id.* at 1198.

[406] *Id.*

[407] *Id.* at 1197.

[408] *Id.* at 1198.

[409] Travelers Indem. Co. v. Portal Healthcare Sols., LLC, 35 F. Supp. 3d 765, 767 (E.D. Va. 2014), *aff'd per curiam*, 644 F. App'x 245, 246 (4th Cir. 2016).

[410] *Portal Healthcare Sols.*, 644 F. App'x at 247 (quoting *Travelers Indem. Co.*, 35 F. Supp. 3d at 771).

of patient files was a publication, even in the absence of indications that a third party had accessed the patient files.[411]

We also assigned each case to a single category based on subject matter. Some of the cases implicated more than one category, and in those cases, we assigned the case to whichever category was more prominent. Twenty-one cases concerned a data breach, and 13 cases concerned data losses. For our purposes, we define a data breach as an incident where an unauthorized third party can or does obtain access to sensitive information.[412] A data loss, on the other hand, can include technicians accidentally wiping a customer's hard disk drive without backing it up.[413]

We also examined 3 cases concerning insurance coverage for the cost of mitigating the infamous Y2K bug that caused millions of people to worry about whether the shift from 1999 to 2000 in computer clocks would cause mass chaos at midnight on January 1, 2000.[414] This was because early programmers typically omitted the first 2 digits of the year in their projects in order to save space, and it was thought that this bug could cause countless errors if the computer started acting as if the year were 1900 instead of 2000.[415]

In Figure 4, there are separate categories for "fraud" (17 cases), "hacking fraud" (5 cases), and "data breach" (21 cases). All 3 involve computers. Cases we considered fraud cases typically involved an unknown third party spoofing an e-mail's origin to convince a company to transfer a large amount of money. In these cases, the recipient believed the e-mail to have come from either an executive at that company or someone that the company works with.[416] Hacking fraud cases involved a third party breaking into a computer network for their own profit in a manner that does not seem to implicate data theft. Data breach

[411] *Portal Healthcare Sols.*, 644 F. App'x at 248.

[412] *See Data Breaches*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/data-breaches.html (last visited Oct. 6, 2017) ("The ITRC defines a data breach as an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure.").

[413] *See id.* ("The ITRC currently tracks seven categories of data loss methods: . . . Employee Error / Negligence / Improper Disposal / Lost . . . .").

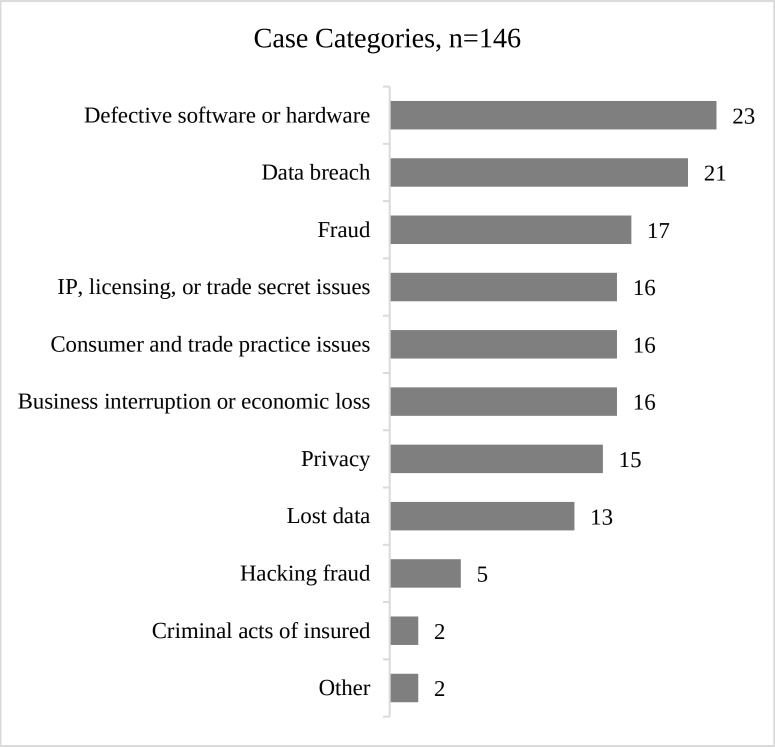
[414] *See Y2K Bug*, NAT'L GEOGRAPHIC: ENCYCLOPEDIC ENTRY, https://www.nationalgeographic.org/encyclopedia/Y2K-bug (last visited Oct. 6, 2017).

[415] *Id.*

[416] *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x at 252, 253 (5th Cir. 2016).

cases, on the other hand, typically involved a third-party intrusion and data theft—though there were also cases where the breach was purely the result of the data caretaker's negligence. For example, in April 2016, the Fourth Circuit held in a per curium opinion that, under a CGL policy, an insurer has a duty to defend a health care service provider in a class action stemming from the provider's negligent recordkeeping system.[417] For a period of at least 4 months, Portal Healthcare Solutions, the policyholder of the present case, stored patient records for Glen Falls Hospital in a manner that made these records discoverable without a password by anyone who searched for a patient's name on Google.[418]

Figure 4: Case Categories



[417] Travelers Indem. Co. v. Portal Healthcare Sols., LLC, 644 F. App'x 245, 248 (4th Cir. 2016).

[418] *Id.* at 246.

Some of the cases that we looked at examined the boundaries of computer fraud insurance coverage. In *Apache Corp. v. Great American Insurance Co.*, an oil company challenged a claim denial based on the computer fraud provision of a crime policy.[419] The underlying facts are as follows. An unknown person contacted Apache by phone and claimed to represent Petrofac, one of Apache's vendors.[420] The caller wished to change the bank account that Petrofac used for receiving payments from Apache.[421] The caller was informed that such requests must be in writing on official letterhead.[422] A week later, the company's accounts-payable department received an e-mail following up on this request.[423] The thieves e-mailed Apache from the domain "petrofacltd.com" instead of "petrofac.com," the vendor's actual domain name, but the discrepancy went unnoticed.[424] The account information was changed after an Apache employee called the phone number provided in the e-mail to verify the request.[425] Apache transferred approximately seven million dollars to this bank account before they discovered that the real vendor was not receiving the payments.[426]

In an earlier section, we noted that insurance policies often include causation conditions like that the claim result directly from a particular type of occurrence. The trial court granted summary judgment for Apache, ruling that there was coverage under the computer fraud provision of the crime policy.[427] The primary issue was whether the injury "result[ed] directly from the use of any computer to fraudulently cause a transfer."[428] The trial court reasoned that the e-mail was a substantial factor in the loss, so the theft did result directly from the e-mail.[429] The Fifth Circuit disagreed, vacating the earlier judgment and rendering judgment for GAI, holding that the direct cause of the loss

[419] *Apache Corp.*, 662 F. App'x. at 254.

[420] *Id.* at 253.

[421] *Id.*

[422] *Id.*

[423] *Id.*

[424] *Id.*

[425] *Id.*

[426] *Id.* at 253–54 (suffering an actual loss of approximately $2.4 million).

[427] Apache Corp. v. Great Am. Ins. Co., 2015 WL 7709584 (S.D. Tex., Aug. 7, 2015), *vacated*, 662 F. App'x 252 (5th Cir. 2015).

[428] *Id.* at *1.

[429] *Id.* at *3.

was Apache's failure to adequately investigate the new information provided by the thieves.[430]

Of the 146 cases in our database, 103 are trial level, 39 are appellate level, and 4 cases were decided by a state's highest court. As Table 3 shows, insurers prevailed more often than policyholders at the trial court level, but on appeal, the difference between insurer success and policyholder success decreased noticeably. Omitting mixed outcomes and settlements, insurers prevailed 67% of the time in trial court and just less than 61% of the time in appellate court.

Table 3: Court Level and Prevailing Party

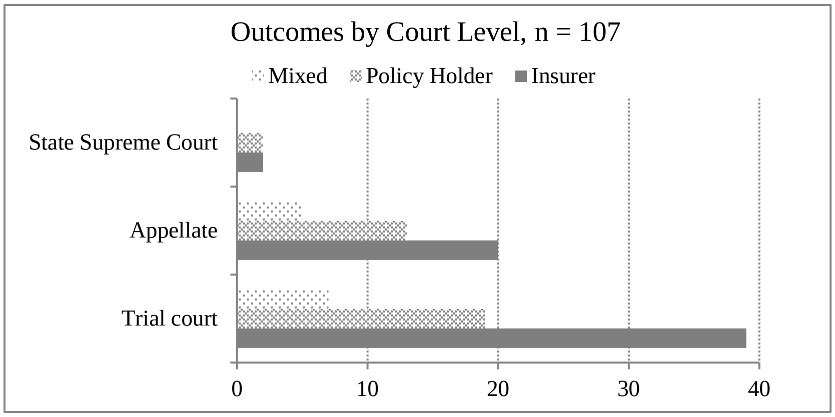
Prevailing Party	Trial Court	Appellate Court	State Supreme Court
Insurer	39	20	2
Mixed	7	5	0
Policy holder	19	13	2
Settled	18	0	0

Of the 146 cases in our database, 13 of these cases were at least partially reversed on appeal. Eight times, the full or partial reversal affected a case where the insurer had originally prevailed, and 3 times, the full or partial reversal affected a case where the policyholder had originally prevailed. Two times, there was a full or partial reversal and the decision of the lower court was what we considered mixed, in that the lower court held for the insurer on some issues and the policyholder on other issues.

[430] *Apache Corp.*, 662 F. App'x at 259. *Contra* Medidata Sols., Inc. v. Fed. Ins. Co., 2017 WL 3268529, at *5–7 (S.D.N.Y. July 21, 2017) (addressing the issue under very similar circumstances—except it started with an actual spoofed e-mail instead of a phone call—the court did not follow the Apache court; the case is currently on appeal).

Figure 5 depicts prevailing parties for 107 cases. The outcomes of 39 cases were unknown at the time of this writing.

Figure 5. Prevailing Party by Court



Not all cases concerned a traditional insurance policy. One case, for example, concerned a dispute over a retailer's contract with a transaction processing service. In that case, the Schnuck supermarket chain was litigating with First Data over the amount Schnuck should pay for the cost of banks reissuing payment cards affected by a data breach of Schnuck's systems.[431] The merchant payment processing agreement set a liability cap for the retailer at $500,000, unless certain conditions were met.[432] Schnuck alleged that First Data was withholding more funds from Schnuck's account activity than permitted under the contract, in order to pay the charges to the banks.[433] If the charges were third-party fees, which is one exception to the liability cap, Schnuck's liability would not be capped at $500,000, the additional withholdings would be permitted, and First Data could withhold the full amount from Schnuck.[434] The court concluded that the reissue fees charged by banks after the data

[431] Schnuck Mkts., Inc. v. First Data Merch. Data Servs. Corp., 86 F. Supp. 3d 1055, 1056 (E.D. Mo. 2015).

[432] *Id.* at 1057.

[433] *Id.* at 1056.

[434] *Id.* at 1057.

breach were not third-party fees, and thus First Data was limited to recovering $500,000 from Schnuck for the fees assessed for card reissuance.[435]

We also tracked more specific information for each case and coded each case for different features. For example, we tracked how many cases raised issues about tangible property provisions, the insurer's duty to defend, the presence of an underlying suit, and policy exclusions. Table 4 lists several of these factors and how many times they appeared in cases in federal and state courts.

As shown by these excerpts, insurance cases that implicate digital data involve a wide range of issues. Of the 146 cases analyzed, 89 of the cases involved a duty to defend, and 101 of the cases included discussions of policy exclusions.

We also examined some frequently litigated issues and how many times a particular party prevailed when those issues were raised. Of particular interest was the distribution with respect to tangible property (generally Coverage A of a CGL policy) and advertising or personal injury (Coverage B).

Table 4: Court Type and Issues Raised

	Federal	State	Total
Exclusions Raised	81	20	101
Tangible Property and Damage	43	13	56
Occurrence	24	2	26
Causation	30	4	34
Duty to Defend	69	20	89
Publication	20	6	26
Presence of Underlying Suit	75	19	95

The total count differs in Table 5 because we omitted cases where the outcome was unknown or that were still ongoing. One unexpected observation was the distribution of settlements.

[435] *Id.* at 1066.

While settlements did not account for a large number of our cases, over 26% of the cases we analyzed that examined personal or advertising injury provisions (Coverage B) ended in settlement. Furthermore, excluding mixed outcome and settled cases, over 70% of cases that raised tangible property provisions were decided in the insurer's favor, compared to 58% of advertising injury cases decided for the insurer.

Table 5: Prevailing Party and Issues Raised

	Prevailing Party				Total
	Insurer	Mixed	Policyholder	Settled	
Duty to Defend	43	9	15	14	81
Tangible Property	29	4	12	6	51
Loss of Use of Tangible Property	15	2	7	2	26
Advertising Injury	14	1	10	9	34
Publication	12	2	7	1	22
Lost Business Income or Business Interruption	6	2	9	2	19
Policy Exclusions	48	9	24	12	93

Regarding the specific characteristics or issues particular to each case, we employed the Pearson's chi-squared test (χ^2) to explore whether there are any statistically significant differences in the 29 issues/characteristics[436] with respect to the prevailing

[436] The twenty-nine variables that we tracked through the cases are: the presence of causation issues, discussion of whether an incident was an "occurrence" under the policy, whether a claim implicated covered property, whether the loss occurred on premises, the presence of computer fraud coverage, claims for lost business income or business interruption, language in policies about actions in the course of business, advertising or personal injury, tangible property or physical damage, loss of use of tangible property, policy coverage for intentional or accidental events, data loss as personal injury, insurance provisions

party, either an insurer or a policyholder. The results suggest that the only statistically significant issues between cases where the insurer prevailed versus cases where the policyholder prevailed are the duty to defend and the lost business income or business interruption.

Excluding mixed outcome and settled cases, over 74% of cases which raised duty to defend provisions were upheld in the insurer's favor. This is statistically significantly higher than the portion of cases upheld in the policyholder's favor, as shown by the Pearson chi-squared test (p-value = 0.09). This result suggests that insurers are more likely to win a case where the issue of duty to defend was raised. Further, 72% of cases not involving an issue regarding lost business income or business interruption were upheld in the insurer's favor (p-value = 0.01), suggesting that insurers are more likely to win the case if the policyholder does not address an issue about their lost business income or business interruption.

We also employed the Pearson chi-squared test to explore statistically significant differences in the 29 issues with respect to whether the cases were settled or litigated to an outcome. Eighty-seven percent of cases which raised an issue about policy exclusions did not result in a settlement (p-value = 0.03), suggesting that parties are less likely to settle if any policy exclusion provisions were raised in the case.[437]

Appearing in over 69% of cases analyzed, policy exclusions are clearly an important consideration in litigation involving data and risk shifting. We identified 44 individual exclusions.

concerning work completed by the policyholder, insurance concerns about damages, coverage or incident timing issues, publication, policy exclusions, coverage for malicious third-party acts, the presence of an underlying suit, valuation of harm issues, duty to defend or indemnify, standing for plaintiffs in underlying litigation, security preconditions of policy, policy caps, cases that implicate the Fair Credit Reporting Act (FCRA), cases that implicate the Telephone Consumer Protection Act (TCPA), reference to privacy injuries, cases that emphasize first party policy coverage, and cases with no court order.

[437] Among the other twenty-nine issues, we found statistically significant differences in issues about coverage or incident timing (p-value = 0.01), standing for plaintiffs in underlying litigation (p-value = 0.03), and insurance concerns about damages (p-value = 0.06) with respect to settled versus the non-settled (*i.e.*, litigated to an outcome) cases. Our results suggest that a case is less likely to be settled if these three issues were not raised, even though most of the cases in our sample were litigated to an outcome, regardless of these three issues. However, we caution that the number of settled cases in our dataset is rather small.

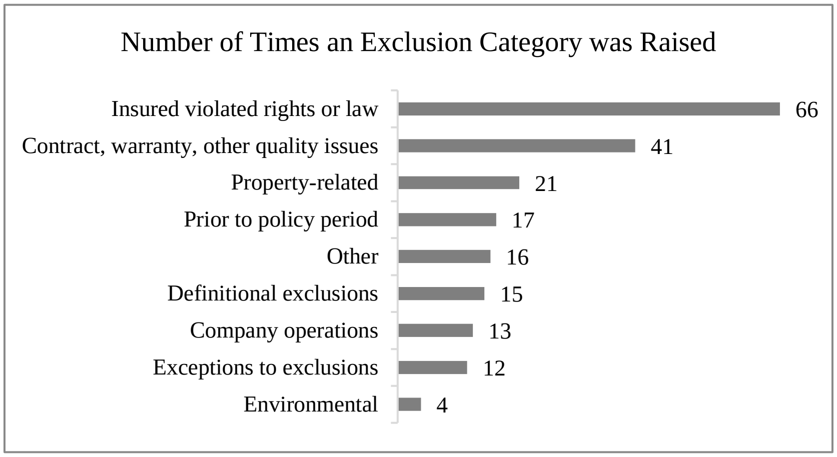
Many cases involved multiple exclusions. The most common singular exclusion concerned breach of contract or a failure of the insured to deliver a product or service as promised. This exclusion or a close variation of it appeared in 23 of the 101 cases where exclusions were an issue. There were 15 cases where an argument emphasized an exclusion written into the definition of a word in the policy, and 13 cases with arguments concerning exclusions for claims involving infringement of intellectual property rights by the insured. There were also 12 cases that discussed exceptions to exclusions.

We categorized these exclusions into nine categories: (1) exclusions pertaining to company operations; (2) computer-related exclusions; (3) exclusions regarding contracts, warranties, or quality; (4) definitional exclusions; (5) environmental exclusions;[438] (6) exclusions pertaining to a violation of rights or law by the insured; (7) exclusions based on occurrences taking place prior to the policy period; (8) property-related exclusions; and (9) a category for other types of exclusions that did not fit in the preceding categories.

The category for other types of exclusions included: (1) statutory exclusions; (2) the exclusion of claims because they should be covered by one of the policyholder's other insurance policies; (3) the exclusion of claims because they pertain to excluded damages, such as regulatory fines or punitive damage awards; (4) exclusions for unexplained loss; and (5) exclusions for claims where the loss was considered too indirect or remote for coverage to apply.

[438] This category refers to aspects of the physical environment, like storms.

Figure 6: Exclusion Categories



C. IMPLICATIONS

In this Part, we have presented our analysis of litigation over insurance coverage. The analysis highlights a number of recurring themes that insurers, policyholders, and lawyers will need to take into consideration.

Trying to use CGL policies to cover the full range of risks to Internet-connected businesses is enormously problematic. Currently, CGL policies are not very effective because of the uncertainty about how CGL policies apply to computer-related losses. One current observation about data-breach litigation is that plaintiffs are experimenting with various theories for liability.[439] This is also the case with insurance coverage litigation that arises because of those cases.[440]

We noted above that standard CGL policies include multiple types of coverage, two of which are referred to as Coverage A and Coverage B. When litigating over coverage for data incidents, some policyholders argue that the injury is covered under the

[439] *See* Chad Hemenway, *Most Cyber D&O Cases So Far Unsuccessful, but Plaintiffs' Attorneys Will 'Continue To Experiment*,' ADVISEN FRONT PAGE NEWS (Jan. 27, 2017), http://www.advisen.com/tools/fpnproc/fpns/articles_new_1/P/274388974.html ("[P]laintiffs' attorneys 'continue to experiment' despite the dismissals of the past . . . .").

[440] *See id.* ("Plaintiffs' lawyers are looking for the right kind of case, or the right kind of fact pattern.").

bodily injury and property damage provisions of Coverage A,[441] while others argue that the injury is covered under the personal and advertising injury provisions of Coverage B.[442] Our empirical examination of cases revealed that insurers tended to prevail more, relative to the policyholder, in litigation involving property damage provisions. Furthermore, a higher percentage of the advertising injury cases that we analyzed ended in settlements compared to cases involving claims for property damage. This suggests that litigation based on Coverage B of a CGL policy encounters more outcome uncertainty than litigation based on Coverage A.

The *Portal* case suggests that in some jurisdictions, courts may find that standard CGL policies cover harms from data-related incidents.[443] At the same time, the *Apache* court warns litigants that causation analysis may render inapplicable specific policy provisions targeting computer fraud.[444] Should a CGL policy cover intangible harms like the deletion or exposure of data? Should a computer fraud policy cover injuries from employees not looking closely enough at information in an e-mail?

Insurers and policyholders should take care with policy elements like anti-concurrent causation language as digital injuries begin to be insured separately from tangible injuries. As the *Apache* case shows, the line between computer fraud and regular fraud may be blurry because thieves operate across multiple spaces.[445]

Our analysis also raises questions about the specific language of provisions in the Coverage A and Coverage B sections of a CGL policy. The *Portal* case involved policy language covering advertising injuries and personal injuries, with both types of injuries being defined as including a publication that "gives unreasonable publicity to [a person's] private li[fe]."[446] In the *Portal* case, the Fourth Circuit held for the policyholder by reasoning

[441] RSVT Holdings, LLC v. Main St. Am. Assur. Co., 136 A.D.3d 1196, 1198 (N.Y. App. Div. 2016).

[442] Travelers Indem. Co. v. Portal Healthcare Sols., L.L.C., 35 F. Supp. 3d 765, 767 (E.D. Va. 2014), *aff'd per curiam*, 644 F. App'x 245, 246 (4th Cir. 2016).

[443] *See id.* at 248.

[444] *See* Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 253 (5th Cir. 2016).

[445] *Id.* at 259 ("Apache failed to investigate accurately the new, but fraudulent, information provided to it.").

[446] *Portal Healthcare Sols.*, 644 F. App'x at 247 (quoting *Travelers Indem. Co.*, 35 F. Supp. at 771).

that the exposure of confidential patient information was a publication, even when there was no indication that anyone other than the patients themselves accessed the records online.[447]

On the other hand, the *RSVT Holdings* case focused on property damage provisions of a CGL policy to provide coverage for a data breach involving financial information.[448] There, the policyholder argued that the theft of customer credit card information was property damage under the policy.[449] The insurer prevailed in *RSVT Holdings* because electronic data was excluded from the definition of tangible property under the policy.[450] These two cases suggest that data breaches can be covered by CGL policies based on the exposure being a publication and thus covered as an advertising or personal injury, but arguments for coverage based on the data breach amounting to property damage are likely to fail, especially in the presence of exclusions for electronic data.

As described in the earlier Section, we found a statistically significant relationship between the prevailing party variable and two of our other variables: duty to defend, and business interruption coverage. Cases that examined the duty to defend were more likely to favor the insurer, while cases that involved business interruption coverage were more likely to favor the policyholder. The duty to defend generally arises in the context of third-party liability policies. Business interruption coverage, on the other hand, is more often an issue in first-party business and property insurance policies. This may indicate greater sympathy for policyholders whose businesses are harmed. It could also indicate that policyholders can offer better arguments for coverage in the well-established area of business interruption policy provisions. However, applying general liability principles to data losses affecting third parties (where the duty to defend is most relevant), is more challenging. Analogies between data and property may face an uphill climb in a court system that functions best with easily quantifiable harms.

[447] *Id.* at 247–48.

[448] RSVT Holdings, LLC v. Main St. Am. Assur. Co., 136 A.D.3d 1196, 1198 (N.Y. App. Div. 2016).

[449] *Id.*

[450] *Id.* ("Crucially, the policy further states that . . . 'electric data is not tangible property.'").

Our database also indicates that litigation over issues of coverage for data breaches and other intangible harms has increased significantly since 2011. Even as we start getting clearer answers to questions about data breaches as publications and data breaches as property damage, the increasing volume of cases spells trouble. As cyberattacks become even more prevalent, businesses will need ways of managing their risk in and out of the courtroom. A strong cyberinsurance market with new cyber-specific insurance products could mitigate the uncertainty of litigation and provide incentives for investing in cybersecure infrastructure and achieving good computer hygiene.

IV. RECOMMENDATIONS

As technology becomes more intertwined with life and business, risk shifting becomes more important. Many CGL policies use language that is ambiguous about electronic data issues, and courts are faced with a significant task when evaluating how this policy language should apply to risks faced by modern businesses. The Fourth Circuit's decision in the *Portal* case indicates a willingness to interpret CGL policies as covering cyber events.[451] Many insurance providers are troubled by this because of the lack of actuarial data for cyber events. CGL policies are typically issued with a fairly good idea of what the existing risks are, but the occurrence and financial consequences of cyber events are currently unpredictable. The empirical analysis of the insurance lawsuits that we presented above underscores the need for new insurance products directed at specifically covering cyber risks and harms.

Insurers are in a unique position to push companies to adopt more consistently secure data-security practices, including encryption, firewalls, intrusion detection systems, and stronger internal controls for data handling. As private-sector participants with a more direct relationship to the policyholders, the insurers could impose the kind of Best Available Control Technology standards that the EPA imposes on polluters under the Clean Air Act. Compared to federal or state regulators though, insurers are in a better position to communicate directly with policyholders and conduct audits to ensure policyholder s' security standards keep up with technological developments. It could also benefit insurance companies and the public interest for insurers to

[451] *Portal Healthcare Sols.*, 644 F. App'x at 246.

invest in cybersecurity research aimed at protecting commercial enterprises.

A. ADDRESSING COVERAGE ISSUES

Our analysis in Part IV illustrates the scope of litigation over coverage for many of the intangible harms that are difficult to insure. We noted in Part III that insurers are increasingly narrowing policies, and our analysis supports this observation. Exclusions for electronic data may prevent data breaches from being covered as property damage. After *Portal*, it is possible that more insurers will exclude data breaches from coverage as publications of sensitive personal information. The record of litigation supports a trend towards market segmentation with the introduction of more accessible cyberinsurance policies.

Cyber events are currently being addressed through civil litigation, though our research indicates a fair amount of controversy over the application of different types of insurance coverage and how courts will interpret them. Perhaps what is needed is a centralized location where insurance coverage and data-breach litigation are viewed as parts of the same whole, providing more insight into the interactions between risk management and the experiences of consumers. The Internet has already eroded national borders. Maybe now there should be some kind of organization that erodes the borders between managing risks and responding to risks. The insurance industry has great potential to stimulate investment in cybersecure infrastructure and improved computer hygiene across the private sector, but it cannot do it alone.

Perhaps a third-party organization, such as the RAND Corporation or the Information Technology and Innovation Foundation for Policy, could bring together thought leaders from the fields of economics, law, insurance, and computer security to evaluate risks and propose solutions. Intersectoral cooperation could help address uncertainties associated with emerging risks. A dedicated cybersecurity think tank could collaborate with ISO, NAIC, CERT, other private organizations, and various government agencies to get everyone speaking the same language as we work towards addressing the cybersecurity threats that create uncertainty in courtrooms, board rooms, and living rooms.

The key is to reduce informational asymmetries so that insurers can more easily track their own risks and policyholders can anticipate coverage issues. Ideally, this kind of collaboration would reduce litigation in addition to reducing uncertainty. Our second recommendation is more explicitly focused on reducing informational asymmetries.

B. Improving Risk Assessment

Insurance policies are becoming more available for cyber risks, and the policy language is becoming more focused on specific problems faced by insurers and policyholders. Yet there is a serious need for more information. Insurers still lack enough information to make measured decisions about how to design the policies, what the conditions of the policies should be, what the policy caps should be, and a variety of other issues. For this reason, we strongly support the DHS in its efforts to develop the CIDAR, in order to improve technological risk assessment, including the size of the potential losses, brought about by the presence of vulnerabilities in computer software and hardware.

The Cyber Incident Data and Analysis Working Group (CIDAWG) of DHS published a white paper detailing the proposed structure of CIDAR.[452] The sixteen proposed categories include broad information like the type and severity of the incident, and more specific information about the victim organization, such as its information security practices and procedures at the time of the incident and whether the incident was caused by a failure of a security control, how the incident was detected, how the organization responded to the incident, and costs incurred as a result.[453]

CIDAR is envisioned as a voluntary and anonymous way to "share, store, aggregate, and analyze sensitive cyber incident

[452] U.S. Dep't of Homeland Sec., Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository 1 (2015), https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf (outlining the basis of a future repository development effort).

[453] *Id.* at 1–2 (helping the private and public sector organizations assess cyber risks, identify effective controls, and improve risk management practice).

data."[454] If implemented, CIDAR would greatly aid in risk assessment activities and reduce informational asymmetries.[455] We have compiled our database of insurance cases about computer-related claims as a complement to a program like CIDAR. Insurers and policyholders will greatly benefit from a centralized database of cyber-incident information. These parties will also benefit from our CLAD, which traces the application of law to these disputes.

Ultimately, what policyholders and insurers need more of is information. CIDAR and CLAD can work together to help these parties evaluate risks and legal implications. Data breaches and cyberattacks can have serious financial implications for businesses, and as such, the interest in cyberinsurance policies is growing.[456] In addition to tracking incidents and litigation, there should also be a centralized collection of information about emerging security threats and patterns. By providing access to a range of data, the government or third-party organization in charge of CIDAR can support insurers and policyholders in their ongoing efforts to manage modern information security risks.

C. ALTERNATIVE RISK TRANSFER

By maintaining a comprehensive repository of information about cybersecurity research and events, policy makers, insurers, and policyholders will be able to observe and respond to trends. However, it is not enough just to know that things happen.

The growth of the cyberinsurance market offers an amazing opportunity to test the viability of alternative risk-transfer methods on a large scale. In analyzing cases, we found that a lot of policyholders and insurers are still relying on traditional CGL

[454] U.S. DEP'T OF HOMELAND SEC., THE VALUE PROPOSITION FOR A CYBER INCIDENT DATA REPOSITORY 1 (2015), https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf. For some criticism of voluntary models of cybersecurity regulation, see Jay P. Kesan and Carol M. Hayes, *Creating a "Circle of Trust" To Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475, 1537–40, 1543 ("[A] purely voluntary approach to either cyber threat information sharing or technology adoption could hinder the effectiveness of the programs . . . .").

[455] *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 452.

[456] *See* Ed Silverstein, *Does Your Company Have Cyber-Insurance?*, INSIDE COUNSEL (May 12, 2016), http://www.insidecounsel.com/2016/05/12/does-your-company-have-cyber-insurance (stating the average total cost of a single cyberattack is $6.5 million).

policies when a cyber event occurs. While the uncertainties surrounding cyber coverage currently make premiums and returns unpredictable at best, there are two alternative risk-transfer approaches that may be particularly applicable to the cyber risk market: securitization and captive insurance.

Securitization of cyber risks could resemble catastrophe bonds, like Credit Suisse's recent issuance of bonds aimed at mitigating internal risks like cyberattacks, accounting errors, and rogue traders.[457] Bonds are a debt security and are a way to loan money to the bond issuer, which will generally be repaid with interest at the maturity date.[458] Catastrophe bonds tend to have a higher interest rate relative to, say, government bonds, because there is a greater risk that the full value of the bond will be lost.[459] This may make bonds an unappealing option for solely shifting cyber risk because of the lack of risk diversity, but this can be addressed by following a model similar to Credit Suisse and using the bond to cover multiple possible causes of loss in addition to cyber risk.[460]

We have also previously analyzed the potential for using financial instruments as a tool to quantify and transfer risks associated with software security vulnerabilities.[461] In this kind of market, insurance companies might elect to participate in the market by taking short or long positions on contracts for security vulnerabilities of different severity tiers.[462] These kinds of investments could allow companies to hedge their risks against adverse cyber events.[463] This approach could potentially be structured to supplement catastrophe bonds for cybersecurity events.

[457] *See* Jan-Henrik Forster & Oliver Suess, *Credit Suisse Said To Study Novel Bond Sale To Offload Risk*, BLOOMBERG TECH. (Apr. 21, 2016), https://www.bloomberg.com/news/articles/2016-04-22/credit-suisse-said-to-study-novel-bond-sale-to-offload-bank-risk.

[458] Lisa Smith, *Why Companies Issue Bonds*, INVESTOPEDIA http://www.investopedia.com/articles/investing/062813/why-companies-issue-bonds.asp (last visited Oct. 6, 2017).

[459] *See* Forster & Suess, *supra* note 457, at 1 ("The insurance industry uses so-called cat bonds to limit exposure to disasters such as hurricanes and earthquakes. Investors get above-market yields for taking a chance on their money being wiped out.").

[460] *Id.*

[461] Kesan & Hayes, *supra* note 30.

[462] *See id.* at 821.

[463] *See id.*

Another possibility is to shift the focus away from traditional insurance companies and consider addressing cyberinsurance problems through a captive insurance approach. When a business is deciding how to address various risks, two options include self-insurance and third-party insurance. Captive insurance is a third option that occupies a middle ground between self-insurance and traditional insurance, where the company that needs insurance creates a dedicated subsidiary for this purpose.[464] Operating a captive insurance company can often retain the tax benefits of paying insurance premiums to a third party, because the IRS generally considers premiums paid to a captive insurance company to be tax-deductible business expenses.[465] Unlike with traditional insurance, however, the premiums remain in the company family, and can be invested.[466] Operating a licensed captive insurance company can also enable participation in the reinsurance market.[467]

D. GOVERNMENT INVOLVEMENT IN THE CYBERINSURANCE MARKET

We have noted that there is a lot of interest in CIDAR as a tool for improving risk assessment for cyber insurance. As we discussed in earlier sections, precedent for government involvement in the cyberinsurance market can be observed with workers' compensation and NFIP.[468] NFIP provides a partial model for a partnership between the government and private sector on cyberinsurance. As noted above, however, the NFIP model is far from perfect. NFIP premiums are often regarded as too low, and the protection of a federally subsidized flood insurance program arguably creates incentives for more people to move to places at high risk for flooding, thus aggravating the moral hazard problem that is already prevalent with insurance.[469] Nonetheless, a government program supporting the cyberinsurance market could support market growth. We are especially focused on two aspects of a potential cyberinsurance regime: voluntariness, and the presence of subsidies.

[464] Constance A. Anastopoulo, *Taking No Prisoners: Captive Insurance as an Alternative to Traditional or Commercial Insurance*, 8 OHIO ST. ENTREPRENEURIAL BUS. L.J. 209, 213 (2013).

[465] *Id.* at 213–14.

[466] *See id.* at 216–17.

[467] *See id.* at 224.

[468] *See supra* Part II.C.

[469] *See supra* notes 369–78 and accompanying text.

One option is to require companies, or at least companies in some sectors, to carry cyberinsurance. In their research, Pal et al. note that a voluntary cyberinsurance system may be inadequate for the goal of maximizing social welfare, because security is a public good.[470] A mandatory cyberinsurance program avoids the problem of high-risk parties purchasing a disproportionate share of insurance policies and creating a lemons market.[471] This is one reason why most states require drivers to carry automobile insurance, why employers are required to carry workers' compensation insurance, and why the Affordable Care Act requires all citizens to have health insurance. On the other hand, some experts claim that voluntary programs have lower costs than mandatory programs,[472] and Kant's paradox of freedom implicitly warns that there is a delicate balance between regulations that benefit the less powerful and regulations that reduce freedom.

As a policy matter, should cyberinsurance be treated in a manner similar to workers' compensation? Employers have to carry insurance in case workers get injured on the job, so perhaps companies that collect and store personal information should be required to carry insurance to guard against computer-based risks. Such a program could potentially be cost prohibitive for smaller businesses. A middle ground may be desirable, where cyberinsurance is mandatory for some industries or some sectors of the economy involving critical infrastructure, but not for others. For example, critical infrastructure industries like transportation and power companies should be required to carry cyberinsurance, but not smaller businesses like retailers that are more focused on brick-and-mortar locations. There could be positive spillover effects from the mandatory industries in terms of technology improvements, and the assured premiums from these industries might enable the cyberinsurance providers to offer more competitive rates for smaller businesses that want coverage for cyber events.

Another aspect to consider is the extent of government subsidies for both insurance and security technology. There are many ways that such a system could be designed. For example,

[470] Pal et al., *supra* note 18.

[471] *Id.* at 6.

[472] Sidney A. Shapiro & Randy Rabinowitz, *Voluntary Regulatory Compliance in Theory and Practice: The Case of OSHA*, 52 ADMIN. L. REV. 97, 100 (2000) (citing E. Donald Elliot, *Environmental TQM: Anatomy of a Pollution Control Program That Works!*, 92 MICH. L. REV. 1840, 1848 (1994)).

the tax code might be revised to introduce tax credits for cybersecurity investments or cyberinsurance premiums. The subsidies could also take on the form used in NFIP, with the government subsidizing part of the cyberinsurance premiums to offset the uncertainty experienced by both insurers and policyholders.[473] As the market develops, the need for a subsidy should be lessened by the introduction of more thorough information about threats and responses. But, as with NFIP, careful attention must be paid to ensure that the program does not incentivize reckless behavior.[474]

Another option for government involvement is to emphasize the role of courts to adjust common-law ideas of privacy injuries to be more in line with modern risks. William Prosser's 1960 article *Privacy* revolutionized how courts approached privacy litigation by identifying four privacy torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light publicity; and (4) appropriation of name or likeness.[475] But Prosser's framework has proven to be very rigid and, consequently, very limiting in the modern world.[476]

Unfortunately for modern plaintiffs, Prosser viewed privacy violations as proprietary injuries, not mental or personal injuries,[477] and this focus on privacy as a proprietary injury can be seen in a slightly different form in standing challenges to data-breach litigation. The first element of Article III standing under the law is that there must be an injury-in-fact, defined in part as an invasion of a legally protected interest.[478] If courts viewed data insecurity (that is, personal data not being secure anymore) as an injury, and thus considered plaintiffs injured the moment their personal information is compromised, uncertainty in data-breach litigation would significantly decrease. If courts expanded their understanding of privacy injuries to include recovering from compromised personal data or privacy invasions (for example, the time and effort spent in replacing compromised credit cards or paying for future credit monitoring) and include

[473] *See supra* Part II.C.

[474] *See supra* Part II.C.2.

[475] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889–90 (2010) (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388–89 (1960)).

[476] *Id.* at 1890 (stating that Prosser's skepticism of privacy law made it difficult for the law to adapt to future circumstances).

[477] *Id.* at 1916 (citing Prosser, *supra* note 475, at 406).

[478] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

injuries that do not, at the moment the lawsuit is filed, have a dollar value attached, uncertainty for insurers would also decrease and allow civil litigation risks to be more reliably estimated.

CONCLUSION

Cybersecurity events can be hugely disruptive for businesses, governments, and the economy. In this Article, we focus on efforts to address these new risks. In order to understand the legal risk in policy coverage, we performed an empirical study of 146 insurance cases that are relevant to electronic data issues and insurance policy coverage to evaluate how these issues are currently playing out in courts across the country. Our findings reflect a litigation environment more favorable towards insurers at the trial level, with most cases brought in federal court being resolved within three years. We demonstrate how the use of CGL policies to cover cyber losses is unpredictable and problematic, thereby underscoring the need for more cyber-specific insurance products.

This analysis provides a starting point for further discussion and development of the cyberinsurance market. By providing a theoretical analysis of problems in the insurance industry and a practical view of insurance litigation involving harm that is often hard to predict, see, and value, we hope to provide support for the development of much needed, better insurance products. Intersectoral collaboration to improve risk assessment, including technological risk, legal risk and portfolio risk, would be a huge boon for insurers, their clients, the cybersecurity industry, and society in general.

As interest grows in specialized cyberinsurance, insurers and policyholders will need to collect and analyze a lot of information. DHS's CIDAR proposal provides one potential tool that can ease this transition. Insurers and potential policyholders may also consider alternative risk-transfer mechanisms, like catastrophe bonds and risk securitization. Effective cyber risk management could support cybersecurity improvements and strengthen critical infrastructure against developing threats. Cooperation at all levels of society, from the government to insurance companies, small businesses, and individual consumers, can facilitate the development of a stronger and more resilient world.