Vol. No. 2 CONNECTICUT INSURANCE LAW

2020-2021

CONNECTICUT INSURANCE LAW JOURNAL

ARTICLES

NOTES

Volume 27 2020-2021 Number 2

CONNECTICUT INSURANCE LAW JOURNAL

Volume 27, Number 2
Spring 2021

University of Connecticut School of Law
Hartford, Connecticut

Connecticut Insurance Law Journal (ISSN 1081-9436) is published at least twice a year by the Connecticut Insurance Law Journal Association at the University of Connecticut School of Law. Periodicals postage paid at Hartford, Connecticut. Known office of publication: 55 Elizabeth Street, Hartford, Connecticut 06105-2209. ***Printing location: Western Newspaper Publishing Company, 929 West 16th Street, Indianapolis, Indiana 46202.***

Please visit our website at http://www.insurancejournal.org or see the final page of this issue for subscription and back issue ordering information.

Postmaster: Send address changes to Connecticut Insurance Law Journal, 55 Elizabeth Street, Hartford, Connecticut 06105-2209.

The Journal welcomes the submission of articles and book reviews. Both text and notes should be double or triple-spaced. Submissions in electronic form are encouraged and should be in Microsoft™ Word™ version 97 *format or higher. Citations should conform to the most recent edition of* A UNIFORM SYSTEM OF CITATION, *published by the Harvard Law Review Association.*

It is the policy of the University of Connecticut to prohibit discrimination in education, employment, and in the provision of services on the basis of race, religion, sex, age, marital status, national origin, ancestry, sexual preference, status as a disabled veteran or veteran of the Vietnam Era, physical or mental disability, or record of such impairments, or mental retardation. University policy also prohibits discrimination in employment on the basis of a criminal record that is not related to the position being sought; and supports all state and federal civil rights statutes whether or not specifically cited within this statement.

Cite as CONN. INS. L.J.

CONNECTICUT INSURANCE LAW JOURNAL

VOLUME 27 2020–2021 NUMBER 2

UNIVERSITY OF CONNECTICUT
SCHOOL OF LAW

FACULTY AND OFFICERS OF ADMINISTRATION
FOR THE ACADEMIC YEAR 2020-2021

Officers of Administration

Thomas Katsouleas, Ph.D., *President, University of Connecticut*
Carl W. Lejuez, Ph.D., *Provost and Executive Vice President for Academic Affairs*
Eboni S. Nelson, J.D., *Dean, School of Law*
Paul Chill, J.D., *Associate Dean for Clinical and Experiential Education*
Darcy Kirk, J.D., *Associate Dean for Academic Affairs, Associate Dean for Library and Technology and Distinguished Professor of Law*
Leslie C. Levin, J.D., *Associate Dean for Research and Faculty Development*
Karen L. DeMeola, J.D., *Assistant Dean for Finance, Administration and Enrollment*

Faculty Emeriti

Robin Barnes, B.A., J.D., *Professor of Law Emerita*
Loftus E. Becker, Jr., A.B., LL.B., *Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Phillip I. Blumberg, A.B., J.D., LL.D. (Hon.), *Dean and Professor of Law and Business, Emeritus*
John C. Brittain, B.A., J.D., *Professor of Law Emeritus*
Deborah A. Calloway, B.A., J.D., *Professor of Law Emerita*
Clifford Davis, S.B., LL.B., *Professor of Law Emeritus*
Richard S. Kay, A.B., M.A., J.D., *Wallace Stevens Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Lewis S. Kurlantzick, B.A., LL.B., *Zephaniah Swift Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Hon. Ellen Ash Peters, B.A., Swarthmore College; LL.B., Yale University; LL.D., Yale University; University of Connecticut; et al.; *Visiting Professor of Law*
Hugh C. Macgill, B.A., LL.B., *Dean and Professor of Law Emeritus*
Patricia A. McCoy, B.A., J.D., *Professor of Law Emerita*
R. Kent Newmyer, Ph.D., *Professor of Law and History Emeritus*
Nell J. Newton, B.A., J.D., *Dean and Professor of Law Emerita*
Leonard Orland, B.A., LL.B., *Professor of Law Emeritus*
Jeremy R. Paul, A.B., J.D., *Dean and Professor of Law Emeritus*
Howard Sacks, A.B., LL.B., *Dean and Professor of Law Emeritus*
Eileen Silverstein, A.D., J.D., *Professor of Law Emerita*
Lester B. Snyder, B.S., LL.B., LL.M., *Professor of Law Emeritus*
James H. Stark, A.B., J.D., *Roger Sherman Professor of Law Emeritus and Oliver Ellsworth Research Professor of Law*
Kurt A. Strasser, B.A., J.D., LL.M., J.S.D., *Phillip Blumberg Professor of Law Emeritus*
Colin C. Tait, B.A., LL.B., *Professor of Law Emeritus*
Carol Ann Weisbrod, J.D., *Professor of Law Emerita*
Nicholas Wolfson, A.B., J.D., *Professor of Law Emeritus*

Faculty of Law

Jill C. Anderson, B.A., University of Washington; J.D., Columbia University; *Professor of Law*
Paul Bader, B.A., Duke University; J.D., Mercer University Walter F. George School of Law; *Assistant Clinical Professor of Law*
Jon Bauer, A.B., Cornell University; J.D., Yale University; *Richard D. Tulisano '69 Human Rights Scholar and Clinical Professor of Law*
Mary Beattie, B.A., Providence College; J.D., University of Bridgeport; *Assistant Clinical Professor of Law and Director, Academic Support*
Bethany Berger, B.A., Wesleyan University; J.D., Yale University; *Wallace Stevens Professor of Law*
Robert L. Birmingham, A.B., J.D., Ph.D. (Econ.), Ph.D. (Phil.), University of Pittsburgh; LL.M., Harvard University; *Professor of Law*

Kiel Brennan-Marquez, B.A., Pomona College; J.D., Yale University; *Associate Professor of Law and William T. Golden Scholar*

Sara C. Bronin, B.A., University of Texas; M.Sc., University of Oxford (Magdalen College); J.D., Yale University; *Thomas F. Gallivan, Jr. Chair in Real Property Law and Faculty Director, Center for Energy and Environmental Law*

Paul Chill, B.A., Wesleyan University; J.D., University of Connecticut; *Associate Dean for Clinical and Experiential Education and Clinical Professor of Law*

John A. Cogan, Jr., B.A., University of Massachusetts Amherst; M.A., University of Texas; J.D., University of Texas School of Law; *Associate Professor of Law and Roger S. Baldwin Scholar*

Mathilde Cohen, B.A., M.A., L.L.B., Sorbonne-École Normale Supérieure; LL.M., J.S.D., Columbia University, *Professor of Law*

Diane F. Covello, B.S., University of Kansas; J.D., Duke University School of Law; *Assistant Clinical Professor of Law and Co-Director, Intellectual Property and Entrepreneurship Law Clinic*

Anne C. Dailey, B.A., Yale University; J.D., Harvard University; *Evangeline Starr Professor of Law*

Miguel F. P. de Figueiredo, B.A., Johns Hopkins University; M.A., University of Chicago; Ph.D., University of California, Berkeley; J.D., Yale University; *Associate Professor of Law and Terry J. Tondro Research Scholar*

Jessica de Perio Wittman, B.A., State University of New York at Stony Brook; B.A, M.L.S., State University of New York at Buffalo; J.D., Seattle University School of Law; *Associate Professor of Law, Cornelius J. Scanlon Scholar and Director, Law Library*

Timothy H. Everett, B.A., M.A., Clark University; J.D., University of Connecticut; *Clinical Professor of Law*

Todd D. Fernow, B.A., Cornell University; J.D., University of Connecticut; *Professor of Law and Director, Criminal Law Clinic*

Richard Michael Fischl, B.A., University of Illinois; J.D., Harvard University; *Professor of Law*

Timothy Fisher, B.A., Yale University; J.D., Columbia University; *Dean and Professor of Law*

Valeria Gomez, B.A., Belmont University; J.D., University of Tennessee College of Law; *William R. Davis Clinical Teaching Fellow*

Hillary Greene, B.A., J.D., Yale University; *Zephaniah Swift Professor of Law*

Mark W. Janis, A.B., Princeton University; B.A., M.A., Oxford University; J.D., Harvard University; *William F. Starr Professor of Law*

Darcy Kirk, A.B., Vassar College; M.S., M.B.A., Simmons College; J.D., Boston College; *Distinguished Professor of Law, Associate Dean for Academic Affairs and Associate Dean for Library and Technology*

Peter R. Kochenburger, A.B., Yale University; J.D., Harvard University; *Associate Clinical Professor of Law, Executive Director of the Insurance LL.M. Program and Deputy Director of the Insurance Law Center*

James Kwak, A.B., Harvard College; Ph.D., University of California at Berkeley; J.D., Yale Law School; *Professor of Law*

Alexandra D. Lahav, A.B., Brown University; J.D., Harvard University; *Ellen Ash Peters Professor of Law*

Molly K. Land, B.A., Hamline University; J.D., Yale; *Professor of Law*

Leslie C. Levin, B.S.J., Northwestern University; J.D., Columbia University; *Associate Dean for Research and Faculty Development and Joel Barlow Professor of Law*

Peter L. Lindseth, B.A., J.D., Cornell University; M.A., M. Phil, Ph.D., Columbia University; *Olimpiad S. Ioffe Professor of International and Comparative Law and Director, International Programs*

Joseph A. MacDougald, A.B., Brown University; M.B.A., New York University; J.D., University of Connecticut; M.E.M., Yale University; *Professor-in-Residence; Executive Director, Center for Energy and Environmental Law; and Kurt Strasser Fellow*

Brendan S. Maher, A.B., Stanford; J.D. Harvard University; *Connecticut Mutual Professor of Law and Director of the Insurance Law Center*

Jennifer Brown Mailly, A.B., Brown University; J.D., Ohio State University; *Assistant Clinical Professor of Law and Field Placement Program Director*

Barbara S. McGrath, B.A., Yale University; J.D., University of Connecticut; *Executive Director, Connecticut Urban Legal Initiative, Inc.*

Willajeanne F. McLean, B.A., Wellesley College; B.S., University of Massachusetts; J.D., Fordham University; LL.M., Free University of Brussels; *Distinguished Professor of Law*

Thomas H. Morawetz, A.B., Harvard College; J.D., M.Phil., Ph.D., Yale University; *Tapping Reeve Professor of Law and Ethics*

Jamelia Morgan, B.A., M.A., Stanford University; J.D., Yale University; *Associate Professor of Law and Robert D. Glass Scholar*

Minor Myers, B.A., Connecticut College; J.D., Yale University; *Professor of Law*

Ángel R. Oquendo, A.B., M.A., Ph.D., Harvard University; J.D., Yale University; *George J. and Helen M. England Professor of Law*

Sachin S. Pandya, B.A., University of California, Berkeley; M.A., Columbia University; J.D., Yale University; *Professor of Law*

Richard W. Parker, A.B., Princeton University; J.D., Yale University; D.Phil., Oxford University; *Professor of Law, Director of the Semester in DC Program and Policy Director, Center for Energy and Environmental Law*

Lisa Perkins, B.S., J.D., Michigan State University; LL.M., Georgetown University Law Center; *Clinical Professor of Law and Director, Tax Clinic*

Richard D. Pomp, B.S., University of Michigan; J.D., Harvard University; *Alva P. Loiselle Professor of Law*

Jessica S. Rubin, B.S., J.D., Cornell University; *Clinical Professor of Law and Director, Legal Practice Program*

Susan R. Schmeiser, A.B., Princeton University; J.D., Yale University; Ph.D., Brown University; *Professor of Law*

Peter Siegelman, B.A., Swarthmore College; M.S.L., Ph.D., Yale University; *Phillip I. Blumberg Professor of Law*

Julia Simon-Kerr, B.A., Wesleyan University; J.D., Yale Law School; *Professor of Law*

Douglas M. Spencer, B.A., Columbia University; M.P.P., J.D., Ph.D., University of California Berkeley; *Professor of Law and Public Policy*

Martha Stone, B.A., Wheaton College; J.D., LL.M., Georgetown University; *Director, Center for Children's Advocacy*

Stephen G. Utz, B.A., Louisiana State University; J.D., University of Texas; Ph.D., Cambridge University; *Roger Sherman Professor of Law*

Steven Wilf, B.S., Arizona State University; Ph.D., J.D., Yale University; *Anthony J. Smits Professor of Global Commerce and Professor of Law*

Richard A. Wilson, BSc., Ph.D., London School of Economics and Political Science; *Gladstein Chair and Professor of Anthropology and Law*

Adjunct Faculty of Law

Anne D. Barry, B.S., University of Connecticut; M.S., Union College; J.D., University of Connecticut; *Adjunct Professor of Law*

James W. Bergenn, B.A., Catholic University; J.D., Columbia University; *Adjunct Professor of Law*

Michael A. Cantor, B.S., J.D., University of Connecticut; *Adjunct Professor of Law*

Thomas O. Farrish, B.A., J.D., University of Connecticut; *Adjunct Professor of Law*

William D. Goddard, B.A., M.B.A., Dartmouth College, J.D., University of Connecticut; Adjunct *Professor of Law*

Andrew S. Groher, B.A., University of Virginia; J.D., University of Connecticut; *Adjunct Professor of Law*

Wesley Horton, B.A., Harvard University; J.D., University of Connecticut; *Adjunct Professor of Law*

John J. Houlihan, Jr., B.A., Providence College; J.D., St. John's University; *Adjunct Professor of Law*

Nancy Kennedy, B.A., University of Massachusetts; J.D., University of Connecticut; *Adjunct Professor of Law*

Daniel Klau, B.A., University of California; J.D., Boston University; *Adjunct Professor of Law*

John Lawrence, B.S., Washington and Lee University; J.D., University of Virginia; *Adjunct Professor of Law*

Erik T. Lohr, B.S., Thomas A. Edison State College; J.D., University of Connecticut; *Adjunct Professor of Law*

Thomas S. Marrion, A.B., College of the Holy Cross; J.D., University of Connecticut; *Adjunct Professor of Law*

Joseph Mirrione, B.A., Marist College; J.D., Vermont Law School; *Adjunct Professor of Law*

Thomas B. Mooney, B.A., Yale University; J.D., Harvard University; *Adjunct Professor of Law*

Cornelius O'Leary, B.A., Williams College; M.A., Trinity College; J.D., University of Connecticut; *Adjunct Professor of Law and Mark A. Weinstein Clinical Teaching Fellow*

Rosemarie Paine, B.S., Southern Connecticut State University; J.D., University of Connecticut; *Adjunct Professor of Law*

Humbert J. Polito, Jr., A.B., College of the Holy Cross; J.D., University of Connecticut; *Adjunct Professor of Law*

Leah M. Reimer, B.S. Baylor University; J.D., University of Connecticut; Ph.D., Stanford University; *Adjunct Professor of Law*

Patrick J. Salve, B.S., J.D., University of Pennsylvania; *Adjunct Professor of Law*

Carl Schiessl, B.A., Trinity College; J.D., University of Connecticut; *Adjunct Professor of Law*

Hon. Michael R. Sheldon, A.B., Princeton University; J.D., Yale University; *Adjunct Professor of Law*

Sandra Sherlock-White, B.A., Central Connecticut State University; J.D., Western New England College; *Adjunct Professor of Law*

Jay E. Sicklick, B.A., Colgate University; J.D., Boston College; *Adjunct Professor of Law*

Walter C. Welsh, B.S., Tufts Engineering; J.D., University of Connecticut; LL.M., New York University; *Adjunct Professor of Law*

CONNECTICUT INSURANCE LAW JOURNAL

VOLUME 27 2020–2021 NUMBER 2

CONTENTS

ARTICLES

NOTES

COURTING DISASTER: THE UNDERAPPRECIATED RISK OF A CYBER INSURANCE CATASTROPHE

KENNETH S. ABRAHAM[*]
DANIEL SCHWARCZ[**]

TABLE OF CONTENTS

[*] David and Mary Harrison Distinguished Professor of Law, University of Virginia School of Law.

[**] Fredrikson & Byron Professor of Law, University of Minnesota Law School. For helpful comments and suggestions, we thank Kelly Castriotta, Jay Kesan, Asaf Lubin, Alan Rozenshtein, Shauhin Talesh, Josephine Wolff and participants in the symposium on The Role of Law and Government in Cyber Insurance Markets co-hosted by the University of Connecticut School of Law and University of Minnesota Law School.

INTRODUCTION

Cyberattacks—what most people call "hacking"—have become almost routine.[1] They are accomplished through various techniques: botnets, browser hijacks, denial of service attacks, ransomware, rootkits, trojans, viruses, and worms, among others.[2] Some are highly public.[3] Others, especially those involving ransoms, often are kept private. Public or private, cyberattacks can cause significant disruption, economic loss, and invasion of privacy.[4] In most cyberattacks, these costs are borne principally

[1] The "cyberattack" label is contested by some, who have suggested that it should only apply to scenarios wherein virtual services are actually sabotaged or disrupted but not to all forms of cyber espionage or data breaches. *See, e.g.*, Luke Irwin, *What's The Difference Between A Data Breach And A Cyber Security Incident?*, IT GOVERNANCE EUROPEAN BLOG (Oct. 10, 2019), https://www.itgovernance.eu/blog/en/whats-the-difference-between-a-data-breach-and-a-cyber-security-incident (discussing the distinction between cyberattacks and cyber incidents). Because nothing substantive in this Article turns on these distinctions, we use the term "cyberattack" throughout to broadly refer to all malicious cyber activity.

[2] *See generally Hacker*, Malwarebytes, https://www.malwarebytes.com/hacker.

[3] *See* Kayla Matthews, *Spookier than Ghosts: 5 of the Biggest Cyber Attacks in 2019*, VXCHNGE (Oct. 31, 2019), https://www.vxchnge.com/blog/biggest-cyberattacks-2019.

[4] Cybercrime costs worldwide are expected to hit $6 trillion in 2021. *See Looking*

by a small number of victims—typically businesses, as well as non-profit and governmental organizations.

Cyberattacks have the potential, however, to simultaneously cause very large losses to numerous firms across the globe, thus resulting in a cyber "catastrophe." To date, there have been only a couple events that could even plausibly be characterized as cyber catastrophes: the NotPetya attack (which caused about $10 billion in global losses)[5] and the WannaCry attack (which caused about $4 billion in global losses),[6] both of which occurred in 2017.[7] But there are plausible reasons for believing that a future cyberattack could produce worldwide losses that are larger by an order of magnitude or greater than the losses associated with these attacks, with many analysts warning that "the next pandemic may be cyber."[8]

The very real prospect of unprecedented cyber catastrophes looms large for the insurance industry. While insurers are well equipped to cover risks that are likely to impact a discrete number of policyholders at any given time, they have much more difficulty covering correlated risks that could produce massive aggregate losses

---

Beyond the Clouds: A U.S. Cyber Insurance Industry Catastrophe Loss Study, GUY CARPENTER, http://www.guycarp.com/insights/2019-guy-carpenter-cybercube-cyber-catastrophe-loss-study.html (last visited Mar. 26, 2021).

[5] *See* Rich Tehrani, *NotPetya: World's First $10 Billion Malware*, APEX TECH. SERVS. (Oct. 28, 2017), https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm.

[6] *See* Jonathan Berr, *"WannaCry" Ransomware Attack Losses Could Reach $4 Billion*, CBS NEWS (May 16, 2017, 5:00 AM), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses. WannaCry was particularly visible with respect to the U.K. National Health Service, which was forced to cancel over 19,000 appointments and incurred an estimated £92 million in losses. *See* U.K. Department of Health and Social Care, *Securing Cyber Resilience in Health And Care: Progress Update October 2018*, GOV.UK (Oct. 11, 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf.

[7] The SolarWinds attack, which first came to light in late 2020, also appears to have impacted a broad swath of entities, including at least nine federal agencies and 100 private companies. *See* Dustin Volz, *More SolarWinds Hack Victims Yet to Be Publicly Identified, Tech Executives Say*, WALL ST. J. (Feb. 23, 2021, 7:50 PM), https://www.wsj.com/articles/senate-panel-probes-solarwinds-hack-to-learn-how-big-how-broad-hit-was-11614086918. But the full scope of the damage caused by the hack has yet to become clear as of the time of this writing. *See id.*

[8] *See, e.g.,* Jamil Farshchi & Samantha F. Ravich, *The Next Pandemic May Be Cyber—How Biden Administration Can Stop It*, THE HILL (Jan. 22, 2021, 11:00 AM), https://thehill.com/opinion/cybersecurity/535364-the-next-pandemic-may-be-cyber-how-biden-administration-can-stop-it.

relative to their total capital. For instance, $100 billion in covered losses from a cyberattack would severely wound the insurance industry,[9] and covered losses two or three times that amount could bring the industry, or at least some of its participants, to its knees.

Of course, not all of a future cyber catastrophe's costs will be insured. But a central message of this Article is that a much larger portion of these costs could prove to be covered than is currently anticipated. In the wake of the Covid-19 pandemic, for example, insurers had to recognize the possibility—unlikely though it may have seemed a month or two earlier—that they would be responsible for a trillion dollars or more of economic losses putatively covered under Business Interruption insurance.[10] Although insurers are ultimately unlikely to have to pay the lion's share of these losses,[11] they could be much less fortunate in the event of a large-scale catastrophic cyber loss.[12]

In fact, traditional forms of insurance are at risk of being subject to massive claims for damage to tangible property resulting from cyberattacks, a prospect that is often labelled "silent cyber" risk. Insurers that issue traditional policies lacking express cyber coverage almost certainly do not intend this result and have not planned for it. Although property/casualty insurers are updating their traditional non-cyber policies to limit such silent cyber coverage, these policies still frequently cover the risk that cyberattacks will result in physical loss or damage to tangible property, or liability therefrom.[13] And many policies in consumer-oriented lines,

---

[9] Recent estimates suggest that total policyholder surplus in the United States property/casualty industry amounted to roughly $772 billion in mid-2020. *See Property/Casualty Insurance Industry Suffered Largest-Ever Drop in Surplus in the First Quarter of 2020*, VERISK (July 28, 2020), https://www.verisk.com/press-releases/2020/july/propertycasualty-insurance-industry-suffered-largest-ever-drop-in-surplus-in-the-first-quarter-of-2020.

[10] One insurance industry estimate of projected uninsured business interruption losses by small businesses in the U.S. was $220–$383 billion per month. Andrew G. Simpson, *P/C Insurers Put a Price Tag on Uncovered Coronavirus Business Interruption Losses*, INS. J. (March 30, 2020), https://www.insurancejournal.com/news/national/2020/03/30/562738.htm.

[11] *See* Jef Feeley & Katherine Chiglinsky, *Insurers Winning Most, But Not All, COVID-19 Business Interruption Lawsuits*, INS. J. (Nov. 30, 2020), https://www.insurancejournal.com/news/national/2020/11/30/592047.htm.

[12] *See infra* Parts II & III (discussing the difficulties that insurers face in limiting their exposure to a large-scale catastrophic cyber loss).

[13] *See infra* Part II.

such as auto and homeowners coverage, do not contain any cyber exclusions due to the historic absence of cyber claims in these domains.[14]

Catastrophe risk is also a major problem for insurers that provide express cyber insurance coverage, either through endorsements to traditional coverage or stand-alone cyber policies. Unlike traditional property/casualty coverage, these policies affirmatively cover various losses associated with cyberattacks and the compromise of electronic data. For that reason, cyber insurers are highly attuned to the risk of catastrophic loss from a massive cyber event. Historically, this awareness has caused cyber insurers to resist covering anything close to the full scale of the cyber risk facing their policyholders. Ironically, however, this result has blunted public and private efforts to plan for a catastrophic cyberattack and mitigate the risk of its occurrence, both by limiting insurers' incentives to improve cybersecurity and by creating the illusion that a large percentage of cyber risk is covered.[15] Although insurers continue to do little to mitigate cyber catastrophe risk, they are increasingly taking on greater amounts of cyber risk by issuing more policies in response to skyrocketing demand.[16] In some cases, insurers have also loosened their historic insistence on artificially low policy limits.[17] In short, both traditional forms of insurance and new forms of cyber insurance are courting disaster.

This Article demonstrates and explains how and why these predicaments have come about. Part I lays the foundation for the analysis by explaining why the risk of catastrophic loss generally poses a problem for insurers. Coverage of catastrophic cyber loss is not immune from this difficulty. Part II analyzes the kinds of cyberattacks that could implicate traditional auto, property, and liability insurance policies, the ways in which the losses resulting from these attacks could be catastrophic, and the insurance coverage implications of these losses. Although physical damage to cars, computers, smart devices, and connected appliances are not what we typically envision when we think about cyberattacks, some or all of these forms of loss could plausibly result from a cyberattack.[18] And physical damage, including loss of use of tangible property and any resulting revenue losses, is exactly what traditional insurance policies cover. This is the area in which insurers

---

[14] *See id*.

[15] *See infra* Part III.C.

[16] *See id.*

[17] *See id.*

[18] *See, e.g.*, Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 426 (2018) (noting that the only form of coverage that CGL policies can provide for cyber events is "liability from physical damage to hardware, which is unusual in most cyber incidents").

are likely to be most seriously underestimating their risk of loss. These are low-probability risks, to be sure. But as this Part shows, they are not no-probability risks.

Part III analyzes insurance that specifically covers loss resulting from cyberattacks. Most, but not all, of this coverage is directed at data compromise and its consequences, rather than at the type of physical damage to tangible property that is covered by traditional insurance policies. Although cyber insurers are well aware of the risk of a catastrophic cyber event, the two primary tools that insurers traditionally use to limit the extent to which catastrophe risk is covered—coverage exclusions and selective underwriting—remain uniquely ineffective in the cyber insurance setting. Historically, this reality has caused cyber insurers to manage catastrophic risk by purchasing reinsurance and insisting on monetary policy limits that are set well below policyholders' actual risk levels. But as more insurers and reinsurers enter the cyber insurance space, limits management is being used less and less, causing this bulwark against catastrophic cyber insurance loss to erode. Just as importantly, managing catastrophe risk by insisting on artificially low policy limits has important costs of its own, leaving even firms covered by cyber insurance substantially exposed to cyber risk while blunting insurers' capacity and incentive to press for effective cybersecurity measures.

Part IV identifies and analyzes several alternative approaches to protecting traditional insurance from catastrophic cyber loss and encouraging new forms of cyber insurance to provide increased coverage without exposing insurers to excessive financial risk. The first is more substantial reinsurance of cyber risks. The second is development of more robust capital market mechanisms for providing long-term financial backup of cyber insurance exposures. And the third is government-funded backup of cyber insurers, either by providing lender-of-last-resort commitments or directly reinsuring cyber insurers for catastrophic losses. Each has strengths and weaknesses that we identify.

I. INSURANCE AND THE PARADOX OF CATASTROPHIC LOSS

The term "catastrophic loss" is not a term of art, but a general notion that refers to loss that is unusually severe.[19] A more technical or nuanced definition usually is unnecessary because nothing operational turns on whether a loss is considered catastrophic. A loss or set of losses may be economically catastrophic without being catastrophic for insurers if the portion of the loss covered by insurance is small. For insurers, an event may be designated as a catastrophe, for example, when covered

[19] This is the definition employed, for example, by the Insurance Information Institute. *See Spotlight on: Catastrophes—Insurance Issues*, INS. INFO. INST. (Apr. 28, 2020), https://www.iii.org/article/spotlight-on-catastrophes-insurance-issues.

claims are expected to reach a certain dollar threshold, such as $25 billion.[20]

In our view, however, there is an additional, implicit feature of this and most other definitions of catastrophic loss. In particular, a catastrophic loss or set of losses must not only be severe, but also comparatively unexpected or surprising in some sense. By this we mean simply that, *ex ante*, a catastrophic loss must be perceived as a low-probability event. Otherwise, the loss would not be, as the definition requires, "unusually" severe.

This requirement that a catastrophic loss must be perceived to be low probability *ex ante* does not mean that it must be wholly unexpected or surprising. A 500-year flood is, after all, something we expect to occur once every 500 years on average. In fact, the most significant catastrophic losses for the insurance industry have involved low-probability/high-severity losses arising out of occurrences that were far from completely surprising—hurricanes, earthquakes, terrorist attacks, and pandemics are all reasonably likely to occur over a long enough time horizon.[21]

Economic theory suggests that insurance is most valuable to insureds when it covers the risk of potentially catastrophic loss, rather than the risk of small, predictable losses.[22] But most losses that would be catastrophic for a potential policyholder are not catastrophic for an insurer. A fire that destroyed a single home would be a highly unusual, extremely severe loss for the homeowner, but would be routine for an insurer that covered this loss.

For insurers, however, covering the risk of widespread catastrophic loss is more complicated. It would be virtually unprecedented for a single policyholder to suffer a loss that would be catastrophic for its insurer. The nearest thing to such a loss was the destruction of the World Trade Center towers on 9/11, which resulted in a property loss to the towers' owners of more than $7 billion.[23] But dozens of property insurers had already spread the risk of a single insured loss to the World Trade Center by covering different dollar layers of that risk,[24] and, in at least some cases,

---

[20] *Id*.

[21] *Id*. And losses that develop over time, such as those involving liability arising out of the use of asbestos or environmental cleanup liability under the federal "Superfund" Act, may have been largely unexpected early in their development, but quickly came to be highly likely. Many and perhaps most catastrophic losses do not come out of the blue but are in fact expected in one or the other sense. S*ee* Richard Zeckhauser, *Insurance and Catastrophes*, 20 GENEVA PAPERS ON RISK & INS. THEORY 157, 157 (1995).

[22] KENNETH S. ABRAHAM, THE LIABILITY CENTURY: INSURANCE AND TORT LAW FROM THE PROGRESSIVE ERA TO 9/11 234 (2008).

[23] KENNETH S. ABRAHAM & DANIEL SCHWARCZ, INSURANCE LAW & REGULATION 43 (7th ed. 2020).

[24] *See* SR Int'l Bus. Ins. Co. v. World Trade Ctr. Props., LLC, 467 F.3d 107, 115–16 (2d Cir. 2006).

partially reinsuring this risk. That is the pattern that is followed throughout the property/casualty insurance industry when a single, potentially large, risk is insured.

Consequently, catastrophic loss usually does not arise from a loss suffered by a single insured. Rather, that threat is due principally to the phenomenon of correlated risk. Correlated risk exists when a single event may result in losses among a large number of victims. Earthquakes and hurricanes pose a correlated risk, as they are likely to injure large numbers of people and damage much property when they occur. When correlated losses occur, they are much more likely to be catastrophic than losses resulting from uncorrelated risks. Correlated risk is therefore much more difficult to insure than uncorrelated risk. For this reason, most private insurers stopped insuring against flood risk some decades ago, and they typically only sell limited earthquake insurance that must be separately purchased and underwritten, often only with government backup. Similarly, some business interruption insurers exclude coverage for economic losses caused by viruses, which can produce a pandemic.[25] Other correlated risks, such as war and nuclear hazard, are also typically excluded from property and liability insurance coverage.[26]

This explains the danger that correlated risks will result in catastrophic losses for insurers, but does not really explain why, for the necessary premium, insurance could not handle such a loss. For example, why should an insurer not be able to collect sufficient premiums to insure against the risk that, once every one-hundred years, there will be a particular $50 billion loss involving 10 million victims? The insurer need only collect an annual premium of $50 (leaving aside administrative expenses and income on invested premiums) from each potential victim in order to cover the risk that the victim will suffer a $5,000 loss that year.

The answer is that the insurer will not have collected enough money to pay for the insured loss until one hundred years have elapsed. Paying out $5,000 to one victim in Policy Year 1 after having collected only a $50 premium, for example, is easy—the insurer suffers only a $4,950 loss, and in the meantime has collected premiums from other insureds whom it has not had to pay. But paying out $50 billion in Policy Year 1 to all 10 million victims, after having collected only $500 million in premiums, would generate $49.5 billion in losses, and render the insurer insolvent if this were its only product. To insure a low-probability, correlated risk of this sort therefore requires an insurer to have access to the capital necessary to pay claims that occur before the insurer has been able to collect premiums equal to the full

---

[25] *See* Feeley & Chiglinsky, *supra* note 11.

[26] *See, e.g.*, Adam F. Scales, *A Nation of Policyholders: Governmental and Market Failure in Flood Insurance*, 26 MISS. COLL. L. REV. 3, 9 (2006); Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L. J. 783, 784 (2005); ABRAHAM & SCHWARCZ, *supra* note 23, at 212, 470.

potential cost posed by the risk. In oversimplified terms, the insurer must be able to borrow $49.5 billion to pay claims if the $50 billion loss occurs in the first year, with the understanding that it will pay off this loan over the next 99 years.

Thus, in principle, correlated risk is insurable, if the insurer has sufficient access to capital to enable it to engage in intertemporal risk-spreading.[27] But in practice, access to capital, in the form of reinsurance, private capital markets, or government backup, has not been sufficient to enable insurers to cover many forms of catastrophic risk.

The difficulty of insuring against correlated risk is compounded by several additional considerations. First, contrary to what we assumed in our hypothetical, estimating the risk of low-probability events is extremely difficult, particularly for risks that may change over time due to factors like climate change or technological development. Insurers typically cannot know, as our hypothetical insurer did, that the probability of the insured event occurring in a single policy year is exactly one percent (one loss every one-hundred years). Setting accurate premiums for insurance against correlated risk is therefore a dicey proposition, which exacerbates the reluctance of reinsurers and private capital markets to provide the necessary access to capital for insurers to provide this form of insurance. Second, potential policyholders tend to underestimate the risk that low-probability catastrophic events will occur, thus reducing demand for coverage and consequently their willingness to pay for it.[28] Third, when a catastrophic event does not materialize in the early years after an insurer has covered that risk, insurers face various difficulties in saving and investing the premiums they have collected to pay future claims when a catastrophe does materialize, due to tax, accounting, regulatory, and corporate governance considerations.[29] Given these difficulties, it is no surprise that private insurers generally seek to avoid covering correlated risks.

Of course, the legitimate difficulties that private insurers face in covering correlated risks do not make such coverage any less valuable to individuals. To the contrary, coverage against risks that could imperil a substantial percentage of a person's or firm's wealth is often immensely valuable to the prospective insured, irrespective of how such risks might impact others. The social benefits of such coverage likely extend further, as insurance coverage of catastrophic risk can help entire economic regions or industries to bounce-back more quickly and robustly from national catastrophes.

---

[27] *See* Dwight M. Jaffee & Thomas Russell, *Catastrophe Insurance, Capital Markets, and Uninsurable Risks*, 64 J. RISK & INS. 205, 207 (1997).

[28] *See* Howard Kunreuther & Mark Pauly, *Neglecting Disaster: Why Don't People Insure Against Large Losses?*, 28 J. RISK & UNCERTAINTY 5, 5 (2004).

[29] *See* Jaffee & Russell, *supra* note 27, at 209–13.

For these reasons, government programs designed to facilitate or affirmatively provide insurance against catastrophic risks are commonplace. Important examples in the U.S. include the Terrorism Risk Insurance Act and the Federal Flood Insurance Program.[30] The key advantage that national governments have over private insurers when it comes to covering catastrophic risks is that they are well equipped to engage in intertemporal risk-spreading through capital markets: National governments in general, and the U.S. government in particular, can easily and cheaply borrow by issuing bonds when large catastrophes necessitate doing so, while (at least in theory) paying off these debts over time.

II. COVERAGE FOR CATASTROPHIC CYBER LOSS UNDER TRADITIONAL INSURANCE POLICIES

A catastrophic cyberattack could have a significant impact on a wide variety of traditional insurers who did not issue cyber-specific insurance policies. For instance, such an attack could plausibly increase claims under Crime/Fidelity policies, Error & Omissions policies, and Director & Officers policies. But the likelihood that a cyberattack could result in potentially catastrophic silent cyber coverage is almost certainly greatest with respect to auto, property, and general liability insurance policies, even though many losses occasioned by a cyberattack would not result in coverage under these types of policies. In particular, a cyberattack that resulted in extensive physical loss or damage to tangible property could cause property/casualty insurers issuing traditional policies to be the subject of claims that they did not anticipate and may not believe are covered. We doubt that insurers that have issued general auto, property, and liability insurance policies are prepared for these kinds of catastrophic cyberattack claims.[31] Many of those claims, however, would in our view have some, and perhaps considerable, plausibility. Consequently, these claims could, under some circumstances, be devastating not just for the directly impacted policyholders, but also for the general property/casualty insurers who cover them.

That is how it was when CGL insurers found, in the 1970s and 1980s, that policies they had issued in prior years covered unexpected liabilities for long-latency

---

[30] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2341 (codified as amended in scattered sections of 12, 15, and 28 U.S.C.). For discussion of the Federal Flood Insurance Program, *see* Jennifer Wriggins, *Flood Money: The Challenge of U.S. Flood Insurance Reform in a Warming World*, 119 PENN. ST. L. REV. 361 (2014).

[31] *See* N.Y. Dep't of Fin. Servs., Insurance Circular Letter No. 2 (2021) (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02 ("Cyber risk likely has not been quantified or priced into [non-cyber] policies, which exposes insurers to unexpected losses.").

injury and property damage resulting from exposure to asbestos.[32] That is how it was after the U.S. Congress enacted CERCLA in 1980, imposing massive liability for the cost of environmental cleanup on companies that had disposed of hazardous waste in the decades before this liability came into being. These companies sought coverage from the insurers that had issued them liability insurance during these prior decades, before either the companies or the insurers even imagined that such liability would exist, let alone be covered by past insurance.[33] And that is how it was when commercial property insurers were sued by the owner of the World Trade Center for $7 billion in coverage that his company had purchased a little more than a month before 9/11, when destruction on this scale was not even contemplated.[34] Tens of billions more were undoubtedly paid for business interruption and life insurance claims arising out of the 9/11 attacks. No one predicted these disasters, but insurers had to pay billions of dollars when they occurred. Few today seem to be predicting an analogous, catastrophic cyber insurance loss for insurers that have issued traditional property/casualty insurance policies, but it could occur.[35]

There are several prerequisites for a cyber catastrophe to result in highly correlated losses for insurers that have issued traditional property/casualty policies. First, a cyberattack would have to cause catastrophic loss involving the physical injury to, or loss of use of, tangible property that these policies cover. This possibility constitutes *damage risk*. Second, for third-party insurance claims, the losses would have to result in liability, or potential liability resulting in settlement, on the part of some third party or parties who did not commit the cyberattack but tortiously facilitated or failed to prevent it. This is *liability risk*. Third, a loss or liability must be covered, or potentially covered, by general insurance policies under which a claimant or claimants are insured, because the policy does not contain a cyber-specific exclusion extending to physical injury or loss of use arising from a cyberattack. This is *coverage risk*.

Our point here is not to predict cyberattacks or their scope, but to envision plausible loss scenarios involving catastrophic damage to tangible property or loss of use of that property, which counts as covered property damage under most policies. One of the things we know from the past is that cyber systems are

---

[32] *See* ABRAHAM, *supra* note 22, at 158–59.

[33] *Id*. at 159–62.

[34] *Id*. at 198.

[35] UK regulators are one exception: they recently identified silent cyber loss from traditional property/casualty polices as a potential threat to insurer solvency. *See Recent Clarifications in Traditional Insurance Lines*, MARSH 2 (June 2020), https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/silent-cyber-recent-clarifications-in-traditional-insurance-lines-slides.pdf.

sometimes more vulnerable to outside interference than their owners and users believe. A common adage, widely quoted and variously attributed, is that there are two kinds of companies, those that have been hacked, and those that will be hacked.[36] Another thing we know from the past is that the ingenuity of hackers does not have obvious limits. The lesson we draw is that the potential for mass cyber disaster that may result in physical damage to or loss of use of tangible property may well be greater than some insurers are openly admitting.

As we will see, for purposes of assessing the catastrophic cyber risk covered by traditional property/casualty insurance policies, the particular manner in which a cyberattack occurs is likely to be less important than the kind of harm or damage it causes. Even the perpetrators of a cyberattack sometimes do not know the extent of the damage it will cause, since it may involve the spread of a virus or similar malware around the world. Moreover, part of our point is that the technical details regarding the manner in which an attack may occur probably have not been anticipated, because defenses against anticipated forms of attack are stronger than against unanticipated forms. Specifying the different possible ways that a cyberattack might produce physical damage or loss of use to tangible property is therefore the appropriate prerequisite to understanding the implications of a cyberattack causing catastrophic loss for insurers that have issued traditional property/casualty insurance policies.

A. DAMAGE RISK: THE POTENTIAL FOR CYBERATTACKS TO CAUSE CATASTROPHIC PHYSICAL DAMAGE TO OR LOSS OF USE OF TANGIBLE PROPERTY

Traditional forms of insurance cover loss or liability for "physical damage" to tangible property and its consequences.[37] Conventional "physical damage" to tangible property consists of easily observable physical alteration of that property from perils like fire and water. In theory, a cyberattack could produce this result relatively directly, by, for instance, taking control of a computer's CPU and overclocking it so as to cause the computer to over-heat and, in the extreme, to actually catch on fire. A more plausible way that a cyberattack could produce

[36] FBI Director Robert Mueller said that in 2012, but he probably was not the first to do so. *See* Robert S. Mueller, III, Dir., FBI, Address at RSA Cyber Security Conference (March 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[37] In addition, the Personal and Advertising Injury provision of CGL insurance policies cover certain forms of intangible loss that might under some circumstances result from cyberattacks. We discuss these potential liabilities and coverage below. *See infra* Part II.C.

observable physical damage to tangible property is by altering a computer's functioning in ways that physically alter tangible property controlled by the computer. Perhaps the most famous example of such a cyberattack was Stuxnet, which the U.S. used to physically destroy Iranian nuclear enrichment tubes.[38] Alternatively, an autonomous vehicle that crashed due to an alteration in the vehicle's code that was introduced by a cyberattack would fall into this category.[39]

Traditional property/casualty insurance policies also typically cover "physical loss" to tangible property. Caselaw interpreting the phrase "physical loss" varies as to how complete an impairment to a physical object's use must be before coverage is triggered.[40] However, there is little dispute that "physical loss" occurs when tangible property has been rendered wholly inoperable for its intended purpose, even if there is no physical alteration to the property itself. Cyberattacks can, and often do, produce this type of damage. For instance, a cyberattack can "brick" computers by encrypting, deleting, or otherwise corrupting key data such that the computer becomes wholly inoperable, resulting in "loss of use" of the computer. This is how NotPetya worked, for example: it encrypted computers' file system tables, which contain information about how the hard drive is partitioned, thus rendering infected computers unusable.[41]

Below we describe three scenarios in which cyberattacks could cause catastrophic loss of the type covered by traditional property/casualty insurance policies: physical injury to, or loss of use of, tangible property. We then provide rough estimates of the potential losses that could result.[42]

---

[38] *See generally* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014).

[39] *See infra* Part II.A.1.

[40] *See, e.g.*, Port Auth. v. Affiliated FM Ins. Co., 311 F.3d 226, 230 (3d Cir. 2002).

[41] *See, e.g.*, ABRAHAM & SCHWARCZ, *supra* note 23, at 694–707 (defining "property damage" to mean "physical injury to, destruction of or loss of use of tangible property").

[42] Exactly how a mass cyberattack would take place may matter for certain purposes, but for the purpose of identifying plausible scenarios, generic hypotheticals will do. It is worth noting, however, that various cyberattacks in the past have caused clear physical harm. For instance, the Stuxnet worm destroyed hundreds of Iranian nuclear centrifuges. *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; *see also* 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, 396 (2015) (describing alleged physical damage to a steel mill as a result of a cyberattack).

1. Motor Vehicles

Modern motor vehicles are full of computers. These computers communicate through the vehicle's controller area network, or CAN,[43] and control numerous elements of its operation. A car's engine computer alone regulates the fuel injectors, adapts idle speed, monitors the ignition system, and delivers electrical commands to the transmission and camera systems. Managing these complex tasks, as well as others, like reading the oxygen sensor and turning the cooling system on and off, typically requires advanced computing systems.[44]

Whether a hacker with no physical connection to a conventional vehicle could access its computer systems directly at present is unclear. But it is only a matter of time before all new vehicles communicate with computers outside the vehicle. Certainly, the self-driving cars of the future, with built-in connectivity to outside sources, are likely to be vulnerable to direct hacking, as a recent joint report by the European Union Agency for Cybersecurity and the European Commission's Joint Research Centre concluded.[45] In any event, millions of current vehicles have Bluetooth systems that are connected to the driver's or owner's smart phone. Bluetooth is a clear potential port of entry for hacking into a vehicle. In addition, a number of auto insurers now offer devices that continuously monitor driving behavior.[46] These plug into the On-Board Diagnostics Type 2 (OBD-II) port of the vehicle and stream driving safety data to the insurer. Finally, telematic services that

---

[43] *See* Mark Samuels, *Controller Area Network (CAN) Vulnerability Puts Vehicles at Risk*, SEC. INTEL. (Aug. 1, 2017, 2:15 PM), https://securityintelligence.com/news/controller-area-network-can-vulnerability-puts-vehicles-at-risk/.

[44] *See How Does the Engine Computer in a Car or Truck Work?*, CAR COMPUT. EXCH. (Feb. 4, 2019), https://carcomputerexchange.com/blog/how-car-computers-work (noting that cars typically need at least a 32-bit, 40 MHz processor to manage these tasks).

[45] *See generally* EUROPEAN UNION AGENCY FOR CYBER SECURITY & EUROPEAN COMMISSION'S JOINT RESEARCH CENTRE, CYBERSECURITY CHALLENGES IN THE UPTAKE OF ARTIFICIAL INTELLIGENCE IN AUTONOMOUS DRIVING (2021), https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving. Tesla cars, for instance, routinely receive software updates through WIFI, leaving them vulnerable to hacking. Indeed, Teslas have been hacked in competitions aimed at exposing vulnerabilities in these cars that can subsequently be patched. *See* Fred Lambert, *Hackers Crack Tesla Model 3 in Competition, Tesla Gives Them the Car*, ELECTREK (Mar. 23, 2019, 4:32 PM), https://electrek.co/2019/03/23/tesla-model-3-hacker-competition-crack.

[46] *See* Steven John, *'What is Bluetooth?': A Beginner's Guide to the Wireless Technology*, BUS. INSIDER (May 20, 2020, 9:30 AM), https://www.businessinsider.com/what-is-bluetooth.

communicate to third parties when a vehicle experiences an emergency are another possible avenue for hacking. Examples include OnStar (for General Motors vehicles only)[47] and Verizon Hum.[48]

Consistent with these vulnerabilities, several lawsuits have been filed against large automobile manufacturers alleging that their vehicles are defectively designed because they are vulnerable to hacking. These suits allege that the "Uconnect system," which facilitates control over many automobiles' phone, navigation, and entertainment systems, can allow hackers to take remote control over the vehicle.[49] Indeed, a 2015 article in WIRED magazine described how two researchers successfully used this vulnerability to take remote control over a vehicle while it was being driven on the highway.[50] To date, courts have dismissed these suits on standing grounds, emphasizing that automobiles vulnerable to this form of hacking have not yet, in fact, been maliciously hacked.[51] But the risk of such hacking remains a reality.

A successful hack of an automobile could plausibly produce at least two different types of physical loss or damage. First, it is certainly possible that a cyberattack on automobiles could cause car accidents by, for instance, disabling safety features, creating driver distractions, or affirmatively causing an impacted vehicle to brake or accelerate. Second, a cyberattack could render a car wholly unusable by disabling critical computer functions necessary for the car's safe operation. Even if such inoperability could be remedied by vehicle repair, it would involve significant property damage.

Of course, a cyberattack on a single or small number of vehicles poses no significant chance of catastrophic physical damage. But an attack that caused a large increase in accidents before it was discovered, or that disabled millions or tens of millions of vehicles, could conceivably result in catastrophic property damage, particularly if it significantly reduced, or completely destroyed, the value of the impacted vehicles.[52]

---

[47] *See Welcome to OnStar*, ONSTAR, https://www.onstar.com/us/en/home/ (last visited on Mar. 7, 2021).

[48] *See Now You Can Talk to Your Car*, HUM, https://www.hum.com/ (last visited Mar. 7, 2021).

[49] *See, e.g.*, Flynn v. FCA US LLC, No. 15-CV-855-SMY, 2020 WL 1492687 (S.D. Ill. Mar. 27, 2020); Cahen v. Toyota Motor Corp., 717 F. App'x 720 (9th Cir. 2017).

[50] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[51] *See* Flynn, 2020 WL 1492687; Cahen, 717 Fed. App'x 720.

[52] There might also be operational losses—collisions, for example—that occurred at the moment that hacking disabled a vehicle if it were in motion at the time.

2. Computers and Smart Devices

Recent estimates suggest that there are currently about 2 billion computers in the world, including servers, desktops, and laptops (but not including smart devices or connected appliances).[53] Hacking of these computers is obviously a reality already. Not only the computers of individuals, but also those of large companies, organizations, and governments have been and continue to be vulnerable to attack. Most such attacks appear to involve only loss of access to data—which for most purposes is not tangible property. But computers themselves and their components—hard drives, for example—are tangible property. So too are cloud-based servers.

An attack that caused millions of conventional computers to become wholly inoperable—like such an attack on millions of vehicles—could involve very significant direct losses, as well as potentially enormous consequential economic losses. But cyberattacks that targeted internet connected devices other than conventional computers could also produce physical loss or damage. For instance, a cyberattack could render smart devices such as iPhones wholly inoperable. Similarly, a cyberattack on computerized and internet connected products—such as refrigerators, ovens, air conditioners, smart home hubs, and hot water heaters[54]—could not only render these devices inoperable, but could also produce more conventional physical damage to the homes and commercial buildings they serve.[55] Alternatively, these appliances could be manipulated to overconsume electricity at a time of peak load and disable a power grid, causing massive amounts of property damage.[56]

---

[53] *See How many Computers Are There in The World?*, SCMO (Aug. 9, 2019), https://www.scmo.net/faq/2019/8/9/how-many-compaters-is-there-in-the-world#:~:text=In%202019%2C%20there%20were%20over,servers%2C%20desktops%2C%20and%20laptops.

[54] According to one estimate, once these devices are taken into account there will be roughly 25–50 billion internet connected devices on earth by 2025. Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference,* 69 DUKE L. J. 583, 593 (2019) (citing MCKINSEY GLOB. INST., THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE 1, 17 (June 2015)).

[55] *See* Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 459 (2019) (discussing the increasing susceptibility of ordinary household items to hacking).

[56] Andy Greenberg, *How Hacked Water Heaters Could Trigger Mass Blackouts*, WIRED, (Aug. 13, 2018, 7:00 AM) [hereinafter *Hacked Water Heaters*], https://www.wired.com/story/water-heaters-power-grid-hack-blackout.

3. Some Back-of-the-Envelope Cost Calculations

Some quick calculations that communicate orders of magnitude are worth considering to provide a sense of what is at stake. Over 200 million private passenger automobiles are insured in the United States.[57] If a cyberattack rendered ten percent of them (twenty million) permanently inoperable or otherwise in need of repair, and the decline in value per vehicle averaged $10,000, the total loss would be approximately $200 billion. To put that sum in perspective, it is almost ten times the amount of Travelers' shareholder equity.[58] Similarly, there are over 250 million smart phone users in the United States.[59] If a cyberattack damaged one hundred million phones, at an average cost of $500 per phone, with a consequent economic loss suffered by ten million business phone users of $5,000 per user, that would be a total of $50 billion in property damage and an additional $50 billion in economic loss, or a total of $100 billion.

Losses of a similar order of magnitude could be expected if millions of personal and business computers were physically damaged by a cyberattack. If ten million business computers were physically damaged by an attack, and the average business suffered $5,000 per computer in consequential economic losses, the cost of the attack for these economic losses alone would be $50 billion. As for damages stemming from appliances connected to the internet shutting down a portion of the power grid, losses of the same order of magnitude would not be surprising. One study found that an attack on 42,000 appliances could leave thirty-eight million people without power.[60] In short, a cyberattack causing physical damage to tangible property, plus the consequential economic loss that could result from such an attack, could easily be financially catastrophic.

B. TRADITIONAL FIRST-PARTY INSURANCE: COVERAGE RISK

We can divide the coverage claims that might arise under traditional first-party property insurance into three categories: claims involving automobiles covered by auto insurance; claims involving home computers, personal smart devices, and

---

[57] INSURANCE INFORMATION INSTITUTE, INSURANCE FACT BOOK 87 (2019).

[58] TRAVELERS, 2018 ANNUAL REPORT 1, https://s26.q4cdn.com/410417801/files/doc_financials/annual/2018/2d3f85d5-18bb-f5bd-2f62-50463ea3b46c.pdf.

[59] *See* S. O'Dea, *Number of Smartphone Users in the United States from 2018 to 2025 (in millions)*, STATISTA (Mar. 19, 2021), https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/.

[60] *See Hacked Water Heaters*, *supra* note 56.

appliances covered by homeowners insurance; and claims involving business computers and consequent economic loss covered by commercial property insurance.

1. Auto Insurance: Claims Seeking Coverage for Damage to the Insured Vehicle

The principal auto loss scenario we envisioned above is a massive cyberattack that rendered millions of vehicles inoperable. Ordinary auto insurance policies would likely cover the damage resulting from such an occurrence. As an initial matter, an attack would trigger coverage under Part D of the Insurance Services Office's (ISO) auto policy, which is the presumptive standard-form policy for many large national insurers. This policy provides coverage for "Damage to Your Auto" in the following terms:

> We will pay for direct and accidental loss to "your covered auto" or any "non-owned auto," including their equipment, minus any deductible shown in the Declarations."[61]

This coverage is divided into "collision" and what was called "comprehensive" coverage in the past but is now referred to as "other than collision." "Collision" covers operational losses, and "other than collision" covers losses caused by any of ten specified causes of loss, one of which is "[m]alicious mischief or vandalism."[62] Although individual insurers' auto insurance policies often differ in various ways from the ISO policy, virtually all policies mirror these basic features: they cover "accidental" losses to covered autos, including "malicious mischief or vandalism" for those who have paid for "other than collision" coverage.[63]

---

[61] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 701.

[62] *Id*.

[63] Some states, like Nevada, make current auto insurance policies easily available online in one place. *See generally Policy Forms Used by the 10 Largest Private Passenger Automobile Insurance Groups in Nevada*, NEV. DIV. OF INS., http://doi.nv.gov/Consumers/Automobile-Insurance/Auto-Insurance-Policy-Forms. Like the ISO policy, the major auto insurers in the state all require the loss to be "accidental" and cover malicious mischief and vandalism under the other than collision coverage. *See, e.g.*, State Farm Insurance, State Farm Car Policy Booklet 16 (emphasis omitted), https://doi.nv.gov/uploadedFiles/doinvgov/_public-documents/Consumers/9828A.pdf ("Loss means: 1. direct, sudden, and accidental damage to; or 2. total or partial theft of a

Collisions could arise from a cyberattack involving vehicles in operation at the time of the attack. But most of the vehicles impacted by a cyberattack would either be in operation and become inoperable without any collision, or would simply become inoperable when not in use. Either way, the resulting losses would produce "other than collision" claims for coverage. In particular, they would constitute loss caused by either "[t]heft or larceny" or "[m]alicious mischief or vandalism."[64] Notably, such claims would generally not be subject to a deductible, which typically applies only to "collision" rather than "other than collision" coverage.

Auto insurers might contest these claims on the ground that cyberattacks do not constitute "accidental loss" as required by the insuring provision quoted above, because the perpetrators of cyberattacks intend to cause harm. In the context of "collision" and "other than collision" coverage provisions, however, the requirement that loss be "accidental" cannot plausibly be interpreted in this way. Part D of the ISO policy provides that "[l]oss caused by the following is considered other than 'collision': . . . 3. Theft or larceny; . . . 7. Malicious mischief or vandalism. . . ." Standing alone, this provision only provides that these types of losses, whether or not they are accidental, do not count as collision. But this language—as well as similar language in virtually all other auto insurance policies—is well understood to result in coverage for these types of losses, as evidenced by decades of insurer payments. Because "[t]heft," "larceny," "[m]alicious mischief," and "vandalism" to an insured vehicle usually involve intentional, destructive acts committed by third parties, it follows that intentional acts by third parties can indeed constitute "accidental" loss, as required in the policy's initial grant of coverage. In any event, what matters is not whether claims for coverage under the "other than collision"

---

covered vehicle. . . . Any loss caused by missiles, falling objects, wind-storm, hail, fire, explosion, earthquake, water, flood, total or partial theft, malicious mischief, vandalism, riot, civil commotion, or hitting or being hit by a bird or an animal is not a Loss Caused By Collision."); Geico, Nevada Family Automobile Insurance Policy 8 (emphasis omitted), https://doi.nv.gov/uploadedFiles/doinvgov/_public-documents/Consumers/A-30-NV.pdf ("Loss means direct and accidental loss of or damage to: (a) The auto, including its equipment . . . . We will pay for each loss, less the applicable deductible, caused other than by collision, to the owned or non-owned auto. This includes breakage of glass and loss caused by: . . . (n) malicious mischief; (o) vandalism."); Progressive DRIVE Insurance, Nevada Auto Policy 14, https://doi.nv.gov/uploadedFiles/doinvgov/_public-documents/Consumers/ Auto/Progressive/9611A.NV.0814.2c.pdf (including similar language).

[64] ABRAHAM & SCHWARCZ, *supra* note 23, at 701. Many, if not most, cyberattacks will be caused by theft, malicious mischief, or vandalism. As a leading cyber security website says that "Hackers are motivated by personal gain, to make a statement, or just because they can." *See* MALWAREBYTES, *supra* note 2.

provision are certain to succeed, but whether they have a plausible chance of success. The latter seems hard to dispute.

In addition, if there happened to be a large number of accidents involving vehicles that were being operated when a cyberattack occurred, the collision coverage provided by auto insurance policies would likely provide coverage. Collision is defined in the ISO auto policy, as well as most proprietary policies, as the "upset" of a vehicle or its "impact with another vehicle or object."[65] There are no relevant limitations on this coverage, aside from the "accidental loss" requirement that also applies to "other than collision" coverage. Because this is all-risk coverage, there is no reference to such possible causes as vandalism and malicious mischief, as there is in connection with "other than collision" coverage. Insurers' arguments that a cyberattack is not "accidental" would therefore potentially be stronger as applied to collision coverage, taken in the abstract. But it is implausible that the physical consequences of a cyberattack could be considered "accidental" for purposes of "other than collision" but not for collision coverage. We think that the two kinds of claims would have to rise or fall together, and that they would rise rather than fall.

Of course, this analysis would be dramatically altered for auto insurance policies that contained an explicit exclusion for cyber-related losses. Many CGL and commercial property insurers are indeed incorporating explicit cyber-loss exclusions into their policies.[66] Moreover, some auto insurers in the U.K. are reportedly including explicit cyber exclusions or affirmative cyber coverage in their policies.[67] At present, however, the vast majority of U.S. auto insurance policies do not appear to include cyber-specific exclusions.[68] For instance, as of 2018, none of the top ten auto insurers in Nevada, which makes such policies publicly available online in a single location, specifically exclude coverage for cyber incidents.[69]

In our view, there are at least three important reasons that most auto insurers do not explicitly exclude coverage for cyber losses. The first is that, to date, there has not been a major cyberattack that has impacted vehicles in any widespread way. As a result, auto insurers may be reluctant to incur the regulatory costs and consumer

---

[65] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 701.

[66] *See infra* Part II.B.3.

[67] *See* MARSH, *supra* note 35.

[68] *See* Sample ISO Auto Insurance Policy, in ABRAHAM & SCHWARCZ, *supra* note 23, at 692–707 (containing no cyberattack exclusion).

[69] *See* NEV. DIV. OF INS., *supra* note 63 (collecting "free, downloadable copies of private passenger automobile insurance policy forms and mandatory amendatory endorsements offered by the 10 largest insurance groups writing private passenger automobile insurance in Nevada").

backlash that might accompany adding these exclusions to their policies. Second, insurers do not have a marketing reason to explicitly exclude coverage for cyber incidents impacting vehicles because they do not sell separate cyber-specific insurance policies for vehicles. By contrast, one important reason insurers in other coverage lines have gone to such lengths to explicitly exclude silent cyber coverage from traditional policies is to create an opportunity to sell cyber-specific policies that fill this gap in coverage. Third and finally, unlike the U.K., most U.S. insurance regulators have not highlighted the prospect that silent cyber coverage could create solvency risks for traditional property/casualty insurers.[70]

2. Homeowners Insurance: Claims for Coverage of Damage to Personal Computers, Devices, and Appliances

Personal devices run the gamut from smart phones, to personal computers, to smart home hubs, to implanted medical devices, to smart appliances. But the coverage analysis that applies to them under the most common type of consumer-oriented insurance policies is similar. In most cases, cyberattacks that cause direct physical loss or damage to personal devices are covered by consumers' homeowners and renters insurance policies.

The ISO Homeowners and Renters policies generally cover "personal property owned or used by the insured while it is anywhere in the world"[71] caused by any of a series of specified "perils," including "Vandalism or Malicious Mischief." However, "Property Not Covered" includes "Portable electronic equipment that: (a) Reproduces, receives or transmits audio, visual, and data signals; and (b) is designed so that it may be operated from a power source other than a 'motor vehicles' electrical system."[72] Equipment that satisfies sub-paragraph (a) but not (b) is subject to a $1,500 sublimit rather than being completely outside coverage.[73]

Some personal devices would arguably fall into the "Property Not Covered" category (i.e. smart phones), but some would not (i.e. smart refrigerators and desktop computers that are not "portable"). However, the use of the term "signals" at the end of the first clause raises questions about its application at all. While all the devices

---

[70] *See* MARSH, *supra* note 35. A notable exception is that the New York Department of Financial Services recently released a "Cyber Insurance Risk Framework," which encourages insurers to "Manage and Eliminate Exposure to Silent Cyber Insurance Risk." N.Y. Dep't of Fin. Servs., *supra* note 31.

[71] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 202 (citing the ISO Homeowners Policy).

[72] *Id*. at 203.

[73] *Id.*

in question do receive and transmit "signals," that is not the term that would ordinarily be applied to what they do; instead, these devices send and receive data. It would have been easy enough for insurers to draft a clause that more clearly applied to smart phones and smart devices. As it stands, the clause seems like an out-of-date effort to address non-digital devices such as radar detectors and portable radios.

In any event, anything that is not "portable" falls outside the clause, no matter how it is interpreted. Heavy appliances are not portable, nor are desktop computers. Losses caused by a cyberattack that damaged heavy appliances or desktop computers would consequently fall within the coverage provided by homeowners and renters policies. Millions of these items could be damaged by a mass cyberattack, although much of the loss would be subject to a deductible that could render a sizable number of potential claims moot.

Many policies do not employ the ISO limitation to "portable" equipment, but instead apply a special sublimit to "computers" and "electronic data processing equipment."[74] The typical sublimit of $5,000 is sufficiently large to cover most personal losses, even after subtracting a deductible. But just as under the ISO form language, most large smart appliances would not fall within these provisions because they are not "portable."

As indicated above, this analysis could clearly be altered to the extent that the applicable insurance policy explicitly contained a cyber exclusion. However, as with ordinary personal auto insurance policies, most homeowners insurance policies currently do not appear to contain any such cyber exclusions, although there are some notable exceptions.[75]

---

[74] *See id.*

[75] For instance, some Farmers homeowners insurance policies—which in many ways provide systematically less coverage than other insurers' policies—exclude coverage for loss which is caused by or results from "Malfunction or Failure of Software or a Computer System, . . . whether or not a result of error or malicious activities." Farmers Insurance, Farmers Smart Plan Home Policy Nevada 27 (2015), https://doi.nv.gov/uploadedFiles/doinvgov/public-documents/Consumers/Home/Farmers/56-5640_6-15.pdf. Similarly, some Liberty Mutual/Safeco homeowners policies exclude coverage for "liability arising from any transmission, upload or download, whether intentional or not, of computer code, programs or data." Safeco Insurance, Safeco Homeowners Policy 17 (2009), http://docs.nv.gov/doi/documents/home_policies/LibertyMutualForms/HOM-7030.pdf. Such cyber-specific exclusions do not, however, appear to be widespread in most homeowners insurance policies. *See* NEV. DIV. OF INS., *supra* note 63.

3. Commercial Property Insurance: Damage to Business Computers and Consequential Business Interruption Losses

Whether a cyberattack that caused direct physical loss or damage to commercial property would be covered depends on the language of the underlying insurance policy. Particularly important to this inquiry is whether the policy contains a cyber-specific exclusion, and the extent to which such an exclusion specifically extends to physical loss or damage caused by a cyberattack.

Standard commercial insurance policies typically cover "direct physical loss or damage" to covered property, including personal property, with the exception of electronic data.[76] However, computers themselves are not included in the exception.[77] For named-peril policies, covered causes of loss include "[v]andalism, meaning willful and malicious damage to, or destruction of, the described property."[78] While there are no obviously applicable exclusions, the exclusion pertaining to "[w]ar, including undeclared or civil war," could conceivably limit coverage under some circumstances.[79] Policies that word the exclusion differently, to include "hostile or warlike action," could also be interpreted to exclude certain forms of cyber terrorism.[80] That issue is now being litigated.[81] Many policies also contain terrorism exclusions applicable to certain certified acts of terrorism.[82] But no such certification has ever occurred.[83] In our view, physical damage to business computers resulting from a cyberattack would be covered under standard policies,

---

[76] Depending on the language in the policy, it may even include data and software as covered property. *See* Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co., 435 F.Supp.3d 679, 681 (D. Md. 2020) (finding that a businessowners policy that defined "Covered Property" to include "Electronic Media and Records (Including Software)" covered loss of access to business's data and software as a result of a ransomware attack).

[77] ISO Building and Personal Property Coverage Form 2-3 CP 00 10 06 07 (2007) *at* http://colonyins.com/uwweb/forms/CP0010.pdf.

[78] ISO Causes of Loss—Broad Form 1 CP 10 20 06 07 (2007) *at* http://www.colonyins.com/uwweb/Forms/CP1020.pdf.

[79] *See* Josephine Wolff, *"Cyberwar by Almost any Definition": NotPetya, the Evolution of Insurance War Exclusions, and their Application to Cyberattacks*, CONN. INS. L. J. (forthcoming, 2021).

[80] *Id*.

[81] For further discussion of this issue, *see* Part III.A, *infra*.

[82] *See* Jack P. Gibson, *Terrorism Insurance Coverage for Commercial Property—A Status Report*, INT'L RISK MGMT. INST. (June 2002), https://www.irmi.com/articles/expert-commentary/terrorism-insurance-coverage-for-commercial-property-a-status-report.

[83] Nehal Patel, *Cyber and TRIA: Expanding the Definition of an "Act Of Terrorism" to Include Cyber Attacks*, 19 DUKE L. & TECH. REV. 23, 27 (2021).

subject to deductibles that vary in amount and any applicable cyber exclusions.

In contrast to auto and homeowners insurance policies, many commercial property insurance policies have indeed begun to exclude cyber losses. One recent report noted that ISO's commercial property program rules required the attachment of a cyber incident exclusion endorsement to all policies in a majority of states starting in February, 2021.[84] Similarly, Gen Re has reported that a number of different types of insurers have begun to file with state regulators new exclusions aimed at limiting possible cyber-related coverage in non-cyber policies.[85] Additionally, New York's Department of Financial Services recently released a Cyber Insurance Risk Framework that calls on insurers issuing a variety of policies, including errors and omissions, burglary and theft, general liability, and product liability insurance, to identify and eliminate silent cyber coverage.[86] But even under many cyber exclusions, fires or explosions that result from a cyber incident apparently are covered and, depending on the exclusion an insurer selects, so too are ensuing losses from other covered causes that result from a cyber incident.[87]

Depending on the scale of a cyberattack, there could be very sizable coverage risk for policies that do not have cyber-specific exclusions. First, such an attack could plausibly result in widespread damage to computers. If the mechanism of the cyberattack caused a fire, explosion, or over-heating of a device, then such losses might even be covered by commercial property policies with a cyber-specific exclusion. However, we think that an even more significant coverage risk for commercial policies—particularly if they do not contain an explicit cyber exclusion—is that a cyberattack could produce consequential economic losses that

---

[84] *See Cyber Incident Exclusion Endorsements and Status of Business Income COVID-19 Litigation in Commercial Property Insurance*, INT'L RISK MGMT. INST. (Nov. 2020), https://www.irmi.com/whats-new/product-update/cyber-incident-exclusion-endorsements-and-business-income-loss-covid-19-litigation-cpi?utm_source=IRMI+Newsletters&utm_campaign=97fd2a0140-EMAIL_CAMPAIGN_2020_11_04_02_37_COPY_01&utm_medium=email&utm_term= (last visited Mar. 7, 2021); Erik S. Knutsen & Jeffrey W. Stempel*, The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses,* 122 PA. ST. L. REV. 645, 670 (2018).

[85] *See* Molly Corbett & Mindy Pollack, *Are Absolute Cyber Exclusions Coming to the Market to Address "Silent Cyber" Concerns? Some Insurers are Speaking Up*, GENRE (May 20, 2020), https://www.genre.com/knowledge/blog/cyber-exclusions-coming-to-the-market-some-insurers-are-speaking-up-en.html.

[86] *See* N.Y. Dep't Fin. Servs., *supra* note 31.

[87] *See, e.g.*, Cyber Incident Exclusion Endorsements, *supra* note 84.

would be associated with physical loss or damage to computers.[88] Most large businesses purchase business interruption (BI) and contingent business interruption (CBI) insurance to accompany their commercial property insurance. This insurance is designed to cover the economic losses that the insured suffers as a result of damage to its own property (BI), or as a result of damage to the property of another party, usually the customer(s) or supplier(s) of the insured (CBI).

Although BI and CBI are not written on fully standardized forms, the policy language is often similar. They cover revenue lost due to interruption of the insured's business as a result of a peril included in the property insurance policy that causes direct physical loss or damage to an insured's property or to other property. The classic case is a fire that damages the insured's or customer's factory and shuts down production. The insured's property insurance policy would cover the damage to the factory. While the factory was inoperable, the insured would also lose revenue, which BI would cover. If a fire at a supplier's or customer's property caused a loss in the insured's revenue, CBI would cover that.[89]

Damage to the computers of the insured, or those of the insured's customers or suppliers, would result in analogous coverage rights. Thus, if the insured loses revenue as a result of "physical damage" to its own computers, consisting of either observable physical injury or loss of use of those computers, then its BI policy potentially covers that loss of revenue. And if the insured loses revenue as a result of physical damage to the computers of a supplier or customer, its CBI policy covers that loss of revenue. BI and CBI claims arising out of cyberattacks that physically damage computers pose not only legal issues, but factual issues as well. This might include whether there has been physical damage to covered, tangible property, or to the property of a customer or supplier; whether the damage was caused by a peril not excluded by the insured's property insurance policy; whether the damage resulted in a necessary interruption of business; or what percentage of loss occurred as a result of the interruption of business, as opposed to other causes occurring during the period when the business was interrupted (for example, a downturn in the economy generally, severe weather, etc.).[90] Although standard BI policy forms exclude or limit coverage "when a suspension of operations is caused by destruction or corruption of electronic data, or any loss or damage to electronic data," this

[88] *See* GUY CARPENTER, *supra* note 4, at 17–19 (indicating that "widespread data loss" would be one of the largest categories of loss arising out of a catastrophic cyberattack).

[89] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 245–46.

[90] *See id.* at 245.

restriction notably does not extend to suspensions of operations resulting from physical loss or damage to computers.[91]

In the wake of the COVID-19 pandemic, cascades of claims and suits alleging that insurers have wrongfully denied BI and CBI claims have been filed.[92] In addition to posing problems of proof, these suits raise classic legal questions surrounding coverage generally, such as the meaning of "physical loss or damage" to property, and questions of concurrent causation.[93] Given the sums that would be at stake in claims for coverage of BI and CBI after a catastrophic cyberattack, insurers can be expected to identify a host of analogous hurdles in connection with claims for coverage of losses resulting from such an attack. But in contrast to the COVID-19 claims for BI losses, where the core coverage questions are in dispute, we predict that many claims for coverage of physically damaged or unusable computers caused by a cyber attack would be successful and uncontroversial.

C. TRADITIONAL LIABILITY INSURANCE: LIABILITY RISK AND COVERAGE RISK

Cyberattacks are typically launched by parties that are not amenable to suit, have no liability insurance covering them, or both. But other parties do have liability insurance and might be the subject of lawsuits by the victims of a cyberattack. There would be numerous classes of potential defendants in such lawsuits, and therefore numerous classes of policyholders with potential claims for coverage under their liability insurance policies. For example, internet or cellular service providers whose software enabled an attack; the manufacturers of devices that were a port of entry for an attack; the manufacturers and sellers of the hardware or equipment that was damaged by an attack; providers of software that was vulnerable in a way that permitted a cyberattack; and cybersecurity firms whose services failed to prevent an attack. These policyholders' Commercial General Liability (CGL) insurance policies would be the main potential source of coverage of liability for the property damage in question. Below we first identify the forms of liability these defendants might incur (liability risk), and then link these liabilities to the forms of liability insurance that may cover them (coverage risk).

---

[91] *See* ISO Properties, Inc., Business Income (And Extra Expense) Coverage Form CP 00 30 04 02 (2001), https://www.propertyinsurancecoveragelaw.com/files/file/CP00300402.pdf.

[92] *See Covid Coverage Litigation Tracker*, PENN L., https://cclt.law.upenn.edu/.

[93] *See id.*

1. Liability Risk

Because of the presumed unavailability of cyber attackers, efforts to impose liability for losses caused by cyberattacks would have to focus on the parties who "enabled" the attack. Such enabling behavior might occur through an alleged failure to exercise reasonable care to prevent an attack, the manufacture of a product that was susceptible to cyberattack due to a claimed design defect, or the provision of services that allegedly facilitated the attack.[94] Whether such lawsuits would be successful would depend on the facts associated with a particular attack and the way that the applicable standards of care and other elements of tort liability were applied to the different possible defendants. But depending on these factors and the evidence that could be adduced, these suits could be plausible.

a. Liability for Cyberattack Resulting in Bodily Injury or Property Damage

First, a company whose product was either damaged in a cyberattack or operated as a vector for such an attack could be held liable if it acted negligently or its product was defectively-designed.[95] Under either liability standard, a court would likely apply a cost-benefit or risk-utility standard that focused on the company's technological capacity to take additional precautions against an attack and the costs of taking such precautions.[96] Additionally, liability would require that the particular way in which the attack occurred was reasonably foreseeable. Courts might supplement or inform these inquiries by drawing from the Federal Trade Commission's (FTC) cybersecurity rules issued under the agency's authority to police unfair and deceptive trade practices,[97] state laws governing cybersecurity,[98]

[94] *See generally* Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435 (1999).

[95] *See* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 210 (2017) ("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.").

[96] *See, e.g.*, *In re* Toyota Motor Corp., 754 F. Supp. 2d 1145 (C.D. Cal. 2010) (suit involving allegedly defective software in motor vehicle).

[97] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[98] *See, e.g.,* A.B. 375, 2021 Cal. Assemb., Reg. Sess. (Cal. 2018).

or industry standards for cybersecurity.[99] Under any approach, a significant amount of expert testimony would be required since the relevant inquiries are not matters with which ordinary people are familiar and because there is no single accepted industry standard for safeguarding products against cyberattacks.

Second, the plaintiff would have to prove factual causation. This would involve demonstrating that the particular precautions or design change—the omission of which was alleged to have breached the standard of care—would have prevented the attack from being successful or would have reduced its severity. This element of the claim would also involve technological complexity and expert testimony.

Third, the proximate cause and duty requirements would have to be satisfied. This would depend in part on the reasonable foreseeability of the attack and its overall characteristics, but would probably require a legal ruling as well. The issue would be whether the defendant had a duty to prevent, attempt to prevent, defend against, or mitigate the attack in question. In the past, courts have often required that there be a "special relationship" for a defendant to have a duty to protect an individual from harm caused by a third party, but that requirement seems to be dissolving.[100] Rulings regarding the duty of universities and property owners[101] to take reasonable steps to protect residents and others from third-party intruders, and the duty of product manufacturers to anticipate and protect users against product misuse, provide support for this contention. But there is a split of authority about the extent of such duties that could militate against a holding in favor of potential plaintiffs.

b. Data Loss and Economic Loss

Cyberattacks resulting in physical damage to hardware will also involve loss of or interference with data, otherwise they would not be "cyber" attacks at all. Lawsuits alleging liability for destruction of data or failure to maintain data security

[99] For instance, a company's failure to comply with a standard like the ISO 27001, a widely accepted international standard for information security management, could indicate negligence. *See An Introduction to ISO 27001 (ISO27001)*, THE ISO 27000 DIRECTORY, http://www.27000.org/iso-27001.htm (last visited Mar. 21, 2021); Daniel Benoliel, *Toward A Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J. L. & TECH. 435, 437 (2015).

[100] KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 263–64 (5th ed. 2017).

[101] Addis v. Steele, 648 N.E.2d 773, 778 (Mass. App. Ct. 1995) (finding inn liable to guest for damage suffered from arson); Posscai v. Wal-Mart Stores, Inc., 752 So.2d 762, 766 (La. 1999) (requiring retail store to take reasonable measure to protect patrons from criminal acts of third parties).

would pose a number of legal issues. First, in general, there is no liability in tort for negligently causing pure economic loss under the "economic-loss rule."[102] One of the rationales for the rule is that the law of torts should not intervene when contracts can allocate the risk of economic loss.[103] In many of the loss scenarios we have envisioned, the parties are already in a direct or indirect contractual relationship. Moreover, many of the relevant contracts contain provisions addressing and limiting liability for damages on the part of internet services providers, cloud providers, or Internet of Things products.[104]

Second, even where there is no contract or possibility of a contractual relationship, the economic loss rule often precludes liability in negligence for pure economic loss, on the ground that liability in such situations threatens to be catastrophic, whereas victims themselves can insure against their losses through first-party insurance. For example, the driver who negligently blocks access to a bridge is not liable to businesses on the other side of the bridge for the economic losses they suffer as a result of the inability of their customers to reach them.[105] But in some states, there is liability for economic loss that is the consequence of negligently risking violent damage to tangible property, even if such damage or injury does not occur.[106] Some cyberattacks might fall into this exception, where it was in force, but many would not. Few attacks involving data loss alone would seem to qualify.

Third, all of this assumes that data loss constitutes pure economic loss within

---

[102] *See* Seely v. White Motor Co., 403 P.2d 145, 152 (Cal. 1965); *see also* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 874 (1986); RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 3 (AM. L. INST. 2020); Ward Farnsworth, *The Economic Loss Rule*, 50 VAL. U. L. REV. 545, 554–55 (2016).

[103] *See* RESTATEMENT (THIRD) OF TORTS, *supra* note 102, at § 1 cmt. c.; All-Tech Telecom., Inc. v. Amway Corp., 174 F.3d 862, 865 (7th Cir. 1999).

[104] *See* Asaf Lubin, *Public Policy & The Insurability of Cyber Risk*, 6 J. L. & TECH. TEX. (forthcoming 2021), https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=3452833 (describing how cloud service providers generally use exculpatory clauses in their contracts with firms); Asaf Lubin & Meirav Furth Matzkin, *The Case for Cybersecurity Policies* (forthcoming), https://csrcl.huji.ac.il/sites/default/files/csrcl/files/database.pdf (finding that the vast majority of publicly traded IoT companies have provisions in their terms of services that significantly or completely remove their liability to consumers for data breaches and other cyber related harms caused by breaches and attacks concerning their products).

[105] *See, e.g.*, 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1104 (N.Y. 2001).

[106] *See, e.g.*, Pointe at Westport Harbor Homeowners' Ass'n v. Engineers Nw., Inc., P.S., 376 P.3d 1158, 1162 (2016) (adopting the hazardous defect exception to the economic loss rule).

the meaning of the economic loss rule. Such an assumption is far from clear. Data may not be tangible property, but loss of data is arguably not only an economic loss. Rather, it might also be understood as loss of a thing, albeit an intangible thing, and economic loss may result from the loss of that thing.[107] Whether there would be liability in tort for such consequential loss, we believe, is an open question.

Fourth, it is common for cyberattacks not only to destroy data or block access to it, but to allow attackers to gain access to confidential data that businesses maintain about their customers.[108] Lawsuits by customers for losses from the resulting invasion of privacy, direct economic loss, or concerns about future harms like identity theft, pose novel issues of liability that do not fall squarely within the economic loss rule.[109]

Finally, even when a cyberattack causes physical damage and therefore may qualify for conventional tort liability, it may be accompanied by data loss. If either form of loss would be sufficient to cause some, or all, of a plaintiff's consequential economic losses, then tort liability under the economic loss rule is unclear. This is the problem of multiple sufficient causes, or "overdetermined" causation.[110] If there is no liability for failing to prevent the data loss, is the defendant liable for the losses that either the data loss or the damage to tangible property were independently capable of causing? The tendency of the courts is to hold that there is such liability,[111] but the rulings are not definitive, nor plentiful enough, for us to be confident of this outcome.

In sum, it is hazardous to venture a prediction about the outcomes of tort lawsuits that might be brought in the wake of the various forms of cyberattacks that cause physical damage to tangible property. For our purposes, however, the important point is that it would be hazardous to predict that all such possible lawsuits would

---

[107] *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2094 (2004); Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?,* 85 TEX. L. REV. 783, 786 (2007).

[108] *See, e.g.,* In re Anthem, Inc. Data Breach Litigation, No. 15-MD-02617, 2017 WL 3730912 at *1 (N.D. Cal. Aug. 8, 2017); Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 5, 2015), https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html; Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (July 20, 2015), https://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html.

[109] *See* Kenneth S. Abraham & G. Edward White, *Torts Without Names, New Torts, and the Future of Liability for Intangible Harm*, 68 AM. U. L. REV. 2089, 2136–38 (2019).

[110] *See* ABRAHAM, *supra* note 22, at 134.

[111] *Id.* at 134–36.

fail. The liability risk associated with a catastrophic cyberattack resulting in physical damage to tangible property is realistic and potentially very large.

2. Coverage Risk: Insurer Liability under CGL Insurance Policies

As we discussed above regarding first-party insurance, the extent to which CGL insurance policies would cover lawsuits alleging physical damage to tangible property arising from a catastrophic cyberattack would depend on the specific policy language of commercial defendants' policies. But many CGL policies might provide this type of coverage.

The insuring agreement in typical CGL insurance policies covers liability for "damages" incurred "because of bodily injury and property damage."[112] Liability claims for bodily injury or property damage, or loss of use of tangible property, would be made under these provisions. In our experience, virtually every policyholder who purchases CGL insurance pays part of its premium for coverage of the "Products and Completed Operations" hazard,[113] and therefore has coverage of liability for injury or damage caused by its products. This is the predominant form of insurance covering products liability in the U.S.[114] CGL policies also contain a "business-risk" exclusion applying to coverage for "property damage to your product arising out of it or any part of it."[115]

The term "property damage" is defined in standard-form CGL policies not to include electronic data.[116] The standard-form CGL policy contains an electronic data exclusion, but that exclusion does not extend to physical damage to tangible property.[117] The policy also incorporates a duty to defend suits seeking damages covered by the policy, which would apply to any suit that alleged liability for such damage, even if there were other, non-covered allegations.[118]

In addition, CGL policies cover liability for "personal and advertising injury,"

---

[112] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 467.

[113] *See id.* at 465.

[114] There is also freestanding products liability insurance, or products liability insurance provided by endorsement to CGL policies, but it pales in significance to the insurance provided under CGL policies. *See* A.M. BEST CO., 2020 BEST'S AGGREGATES AND AVERAGES – PROPERTY/CASUALTY 5 (2020), http://www3.ambest.com/aggavg/pc/20/data/2020BAAPC_001-008_CumulativeUnderwritingDirect.pdf (indicating that only $4.166 billion in premiums were paid for separate products liability insurance in 2019).

[115] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 471.

[116] *Id.* at 481.

[117] *Id.* at 471.

[118] *Id.* at 467.

including publication of material that "violates a person's right to privacy."[119] There has been litigation over coverage under this provision for data breach liability.[120] But more recent versions of the policy now exclude coverage of liability "arising out of any access to or disclosure of any person's or organization's confidential or personal information," which would seem to preclude most coverage of liability for data breach.[121] Consequently, the meaning and application of the policy provision governing liability for bodily injury and property damage[122] and the associated provisions quoted above would be the central issues in claims for coverage of liability for the consequences of a catastrophic cyberattack.

Also essential to evaluating the availability of coverage under CGL policies for suits seeking coverage for a catastrophic cyberattack resulting in extensive physical loss or damage would be the existence of cyber-specific exclusions in these policies. Many CGL insurers now explicitly limit coverage for liability involving cyberattacks, though the language of these exclusions varies. The ISO exclusion, for instance, only limits coverage for suits seeking damages involving the disclosure of data, the inability to access data, or the loss of use of such data.[123] Coverage for suits alleging liability for physical loss or damage caused by a cyberattack is not excluded.[124] However, some CGL insurers limit coverage for suits seeking damages caused by a cyberattack even when those damages arise out of physical loss or damage to tangible property.[125]

---

[119] *Id.* at 472.

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

[121] *See* Podolak, *supra* note 42, at 387 (quoting INS. SERV. OFF. INC., FORM CG 21 06 05 14 (2013)).

[122] For example, Target has sued its insurer, Chubb, alleging that its liability for data breach to millions of customers constitutes "loss of use" of tangible property—the customers' credit cards—and is therefore covered. *See* Complaint at 1–2, Target Corp. v. Ace Am. Ins. Co., 2019 WL 6245504 at *1 (D. Minn. Nov. 15, 2019) (No. 0:19-cv-02916).

[123] *See* Ins. Servs. Off Inc., Commercial General Liability CG 21 06 05 14 (2013), https://www.techriskreport.com/wp-content/uploads/sites/26/2019/05/ISO-Form-CG-21-06-05-14.pdf.

[124] *Id.*

[125] *See Two New London Market Model Cyber Exclusion Clauses*, INS. J. (June 6, 2019), at https://www.insurancejournal.com/news/international/2019/06/06/528540.htm (discussing new Lloyds "Cyber Loss Absolute Exclusion Clause," which "provides market participants with an option to exclude in the broadest possible manner any loss arising from the use of a computer system, network or data").

a. Internet and Cellular Service Providers, Makers of Port-of-Entry Devices, Software Suppliers, and Cybersecurity Firms

Firms that manufacture or supply internet and cellular services, port-of-entry devices, software, or cybersecurity may provide the route through which a cyberattack on internet or cell-connected equipment occurs. Alternatively, these companies' products or services may fail to prevent an attack that ultimately damages equipment. Unless these entities' CGL policies contain explicit cyber exclusions,[126] their liability for damage to such equipment would fall squarely within CGL policies' coverage of liability for "damages because of . . . property damage." In addition, the damage ordinarily would not be to the policyholder's own product and therefore would not fall within the business-risk exclusion.

Once there has been damage to any of the tangible property in question, the policies would also cover liability for consequential damages, including the economic losses that result from such property damage.[127] As indicated above, the potential for consequential economic losses is greater for commercial plaintiffs than ordinary individuals, but even the latter might generate substantial losses if, for example, temporary rent for an alternative residence is involved due to damage to hot water heaters, ovens, or other appliances that render the residence uninhabitable.

Virtually the same analysis applies to port-of-entry devices, such as smart phones and hardware that wirelessly connects smart appliances and automobiles to the Internet. The main issue would be whether the makers of these items are liable in tort for enabling or failing to prevent cyberattacks. Once such an attack damages property other than the devices themselves, standard-form CGL policies would provide coverage of liability for this damage and its consequences.

b. Manufacturers and Sellers of Damaged Hardware and Equipment

In contrast to the policyholders we have just discussed, firms that manufactured

---

[126] *See* Part II.C.2, *supra*.

[127] The problem of multiple sufficient causes, or "overdetermined" causation that we referenced earlier in connection with liability risk may also have coverage implications. Suppose that a consequential loss resulting from covered liability for property damage would have occurred even in the absence of property damage because of data loss. This issue is analogous to the problem of concurrent causation in property insurance, where an anti-concurrent question clause now addresses the issue. In the absence of a similar clause in liability insurance policies, we think that policies would be interpreted to provide coverage in this situation.

or sold hardware or equipment that was damaged in a cyberattack are unlikely to be covered under their CGL policies for any liability resulting from such an attack. As we noted earlier, policies patterned on the ISO CGL insurance policy contain a business risk exclusion for "'property damage' to 'your product' arising out of it or any part of it."[128] If a manufacturer or seller of hardware or equipment were liable for damage to its product due to a cyberattack, that would constitute property damage to the product "arising out of it or any part of it," though of course it would also arise out of the cyberattack. But that is a conventional situation to which this exclusion applies. Consider a car manufacturer held liable because the vehicle was not sufficiently capable of withstanding a collision with another vehicle. The exclusion would apply to a suit alleging that the manufacturer was liable for resulting damage to the vehicle on the ground that it was defective.

On the other hand, the business risk exclusion in the ISO CGL policy would not apply to damage to property other than the insured's product, such as the car manufacturer's liability for damage to the other vehicle involved in the collision. The same analysis would apply to manufacturers of computers, smart appliances, and other hardware or equipment damaged by a cyberattack. The manufacturer's liability for damage to the product itself would not be covered by its CGL policy, but the business risk exclusion would not apply to liability for any bodily injury or property damage that was caused by or resulted from damage to the insured's product.

We indicated earlier that in general there is no liability in negligence for pure economic loss. To the extent that an insured did incur such liability, however, it probably would not be covered by the bodily injury and property damage provisions of CGL policies. Damage to electronic data does not constitute property damage under CGL policies; consequently, whether data loss is considered economic loss or something else is immaterial. There is an argument that we cannot dismiss out of hand that there would be coverage of liability for economic loss resulting from damage to the insured's product. The business risk exclusion, like all CGL exclusions, is introduced by the phrase, "This insurance does not apply to."[129] Thus, liability for "property damage" to the insured's product is not merely excluded; the policy does not "apply" to such liability. Consequently, it could be argued that the insurance agreement's grant of coverage of liability for "damages because of . . . property damage" does not "apply" to "property damage" to the insured's product. If that is the case, then the insuring agreement also does not apply to damages incurred "because of . . . property damage" to the insured's product. That would include economic loss resulting from property damage to the insured's product.

But we would not completely rule out the possibility that courts would hold that

---

[128] ABRAHAM & SCHWARCZ, *supra* note 23, at 471.

[129] *See id.* at 468.

this is not the proper way to interpret the effect of the exclusion, and that liability for economic loss resulting from damage to the insured's own product would be covered. If the courts held that there was tort liability for this economic loss, and then held that this liability was covered, CGL insurers' liability in the event of a catastrophic cyberattack could be enormous.

III. CATASTROPHIC COVERAGE AND CYBER INSURANCE

Part II suggested that traditional property/casualty insurers are exposed to potentially catastrophic silent-cyber risk because they have failed to fully appreciate the ways in which cyberattacks could result in covered losses.[130] That Part did not, however, analyze cyber insurance policies, which explicitly cover a range of first and third-party losses that may arise from cyberattacks, but do not generally cover property damage or bodily injury.[131] Covered first-party losses under cyber insurance policies may include costs stemming from business interruption, data restoration, computer forensic services, consumer notifications, public relations efforts, and ransom payments.[132] The third-party coverage included in typical cyber insurance policies often extends to civil liability for compromising individuals' personal data or facilitating network security failures, as well as statutory fines pursuant to certain data privacy laws.[133]

In contrast to many traditional property/casualty insurers, cyber insurers have devoted extensive time and resources to understanding the possibility of catastrophic cyber risks.[134] But as this Part makes clear, cyber insurers face unique challenges to

---

[130] As we indicated in the Introduction, this type of coverage of cyber risk by general insurance policies that do not specifically mention cyber risks is often described as "silent cyber" coverage.

[131] *See* Talesh, *supra* note 18, at 427 (outlining coverages commonly available in cyber policies).

[132] *See* Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones*, Content Analysis Of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 5–6 (2019).

[133] *Id.* at 6; Lubin, *supra* note 104, at 56–62 (discussing coverage of statutory fines).

[134] *See, e.g.*, Davis Hake, Andreas Kuehn, Abagail Lawson & Bruce McConnell, *Cyber Insurance and Systemic Market Risk*, EASTWEST INST. (June 5, 2019) [hereinafter EASTWEST INST.], https://www.eastwest.ngo/cyberinsurance; *see generally* Daniel M. Hofmann & Steve Wilson, *Advancing Accumulation Risk Management in Cyber Insurance*, THE GENEVA ASS'N. (Aug. 2018), https://www.genevaassociation.org/sites/default/files/research-topics-document type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance_0.

reducing their exposure to catastrophic risk. Section A explains this contention, by exploring the difficulties cyber insurers face in using coverage restrictions to limit their exposure to catastrophic risk. In particular, it shows that coverage terms in cyber insurance policies are limited in their capacity to reliably and verifiably distinguish catastrophic cyber losses from the more ordinary cyber insurance losses that must be covered to meet customer demand. Section B turns to a second key tool that insurers often use to limit their exposure to catastrophic risk: underwriting criteria that limit coverage of potentially correlated risks. Here too, the unique nature of cyber risk—which is not bound by geography or industry—limits this conventional safeguard against coverage for catastrophic cyber loss. Finally, Section C shows how these realities have historically played an important role in undermining the growth of cyber insurance markets, causing cyber insurers to insist on monetary policy limits that are set well below policyholders' actual risk exposures. It also shows that increased competition among insurers and reinsurers to offer coverage in the high-growth field of cyber insurance is gradually eroding this final bulwark against the risk of catastrophic insured cyber loss.

A. THE DIFFICULTY OF RESTRICTING COVERAGE TO LIMIT CATASTROPHIC RISK IN CYBER INSURANCE

Coverage restrictions—either in the initial grant of coverage or, more commonly, in exclusions—are one of the most important mechanisms that insurers conventionally use to limit their exposure to potentially catastrophic loss. Insurers use a variety of different types of coverage restrictions and exclusions to limit their exposure to catastrophe risk. The first, and most common, strategy is for policy provisions to limit coverage when specific physical mechanisms cause a loss and those mechanisms are likely to result in catastrophic losses. For example, general property insurance policies exclude coverage for floods and earthquakes.[135] Similarly, business interruption coverage requires that physical loss or damage to covered property cause a business interruption, a requirement that avoids covering loss resulting from declining economic conditions, which produce correlated losses. A second approach—exemplified by exclusions for acts of war—limits coverage based on the motivations or identity of third parties that are involved in causing a loss when those third parties are particularly likely to be motivated by the desire to cause catastrophic losses. Finally, a less common strategy is to limit coverage for

pdf; Trevor Maynard & George Ng, *Counting the Cost: Cyber Exposure Decoded*, LLOYDS 7 (Jul. 10, 2017), https://cyberpolicymagazine.com/images/pdf-downloads/counting_the_cost_cyber_attack.pdf.

[135] *See* ABRAHAM & SCHWARCZ, *supra* note 23, at 211.

certain types of losses that, however they are caused, are particularly likely to be catastrophic in nature. But each of these three traditional approaches to crafting coverage exclusions for potentially catastrophic losses is ineffective or limited when it comes to potential cyber catastrophes.

1. Excluding by Physical Mechanism that Causes Loss

The dominant approach that is used in traditional property/casualty insurance policies to limit exposure to catastrophe risk is to exclude coverage for losses that are caused by specific physical mechanisms that are particularly likely to result in correlated losses. This conventional approach to managing catastrophe risk is usually effective because most of the correlated losses that these policies would otherwise cover are associated with physical processes that can be described with specificity. For instance, by excluding from coverage losses caused in whole or in part by earth movement or flooding, general property insurers are able to substantially reduce their exposure to catastrophe risk by identifying particular physical processes that, when they occur, are highly likely to simultaneously impact a significant number of policyholders. Just as importantly, these exclusions preserve the core of the coverage that ordinary policyholders reasonably expect, such as coverage for losses caused by ordinary fires and storms.

But unlike in traditional insurance settings, it is often difficult or impossible for cyber insurers to identify and exclude from coverage the causal mechanisms of potentially catastrophic cyber risks without eviscerating coverage for ordinary cyberattacks that policyholders demand. Various different frameworks exist for classifying and sub-classifying different types of cyberattacks.[136] And only a few types of cyberattacks—particularly malware[137] and perhaps denial of service

[136] *See, e.g.*, Jeff Melnick, *Top 10 Most Common Types of Cyber Attacks*, NETWRIX BLOG (Oct. 8, 2020), https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks; *2016 Cost of Cyber Crime Study & The Risk of Business Innovation*, PONEMON INST. (2016), https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf (describing eight types 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).

[137] Broadly defined, malware consists of software that is installed on targets' computer systems without their consent. Malware has catastrophic potential because of its ability to propagate throughout the victim's network and spread across different firms through various means, such as through malicious script that is implanted on insured websites, software updates that are pushed out to individual computers, or phishing attacks.

attacks[138]—realistically have the potential to generate catastrophic losses.[139] Yet these types of cyberattacks are also among the most common that individual policyholders face: a 2016 study focusing on over 200 large organizations across the globe found that approximately 99% of them had experienced malware, and about half had experienced denial of service attacks.[140] For these reasons, cyber insurers could not craft coverage exclusions that isolated these types of attacks without undermining the core protections that cyber insurance promises policyholders.

Nor is it feasible for cyber insurers to exclude coverage for subtypes of malware and denial of service attacks that are particularly likely to generate catastrophic, rather than more ordinary, policyholder losses. That is because all such cyberattacks—ranging from a temporary denial of service attack on a small company's website to massively destructive malware that destroys the functionality of millions of computers across the globe— ultimately rely solely on digital means to target another computer or network of computers.[141] The vast majority of such attacks will not produce anything close to catastrophic losses, and the small subset of such attacks that may produce catastrophic losses cannot be easily predicted ahead of time based on simple distinctions that can be clearly described *ex ante* in contract language. Instead, their catastrophic potential often turns on numerous, unpredictable, and difficult to specify details regarding the code that underlies the attack and the means by which that code propagates within networks and across organizations.[142]

These common mechanisms of ordinary and potentially catastrophic cyberattacks are well illustrated by the NotPetya cyberattack, which caused approximately $10 billion of damage. That attack, likely devised by Russian government hackers, targeted computers that were using a popular Ukrainian accounting software known as M.E.Doc. Although intended to cause disruption within Ukraine, the attack quickly spread internationally, impacting hundreds of

---

[138] Denial of Service attacks seek to overwhelm a system's resources so that it cannot respond to service requests. Among other things, such attacks have catastrophic potential because of their ability to make critical online tools or utilities unavailable.

[139] *See* Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth: Expanding Stand-alone Policy Adoption among Middle Market Businesses*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html. Cyberattacks that rely solely on the targeting of individuals, specific property, and individual passwords almost certainly pose limited catastrophic risk for insurers because they cannot be easily aggregated at mass scale.

[140] *See* PONEMON INST., *supra* note 136.

[141] *See* P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 68–70 (2014).

[142] *Id.*

major companies across the globe.[143] Like non-catastrophic malware attacks, however, NotPetya consisted of malicious code that targeted one relatively common piece of software (Microsoft Windows) and was disseminated to different networks through updates to other software (M.E.Doc).[144] Not even the virus's designers, it seems, anticipated the scale of the damage that the virus would cause, a supposition best illustrated by the fact that the virus ultimately caused substantial loss to a Russian state oil company.[145]

To be sure, the catastrophic potential of cyberattacks can sometimes be linked to the mechanisms by which they cause loss. For instance, cyberattacks that target broad-based utilities can produce highly correlated losses by depriving numerous firms of necessary services. Examples of such attacks include a 2016 denial of service attack that cut off internet access to many across the globe for several hours and several malware attacks that interrupted the power supply of Ukrainian cities.[146] For this subset of potential cyberattacks, exclusions that target causal mechanisms of loss are likely to be workable. Indeed, most cyber insurers exclude coverage of losses that are attributable to the failure of broad-based utilities or internet services that are not under the policyholder's control. An illustrative provision excludes coverage for "electrical, mechanical, Internet, telecommunication, cable or satellite failure, fluctuation or outage not under the operational control of the Insured, however caused, including any electrical power interruption, short-circuit, surge, brownout or blackout."[147]

---

[143] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM) [hereinafter *The Untold Story of NotPetya*], https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world; JOSEPHINE WOLFF, CYBER-INSURANCE POLICY: RETHINKING INTERNATIONAL RISK FOR THE INTERNET AGE (forthcoming 2021).

[144] *See The Untold Story of NotPetya*, *supra* note 143. Once NotPetya gained a foothold on a computer with M.E.Doc, it gained remote access to unpatched computers using Windows. This, in turn, allowed it to gain access to other computers on the same network, even if they were patched with a security update.

[145] *Id*.

[146] *See* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 210 (2017).

[147] XL Catlin, 2018–2019 Cyber Liability Policy 20 (2017), https://www.mtcounties.org/wp-content/uploads/risk-sharing/pct/policies/2018-2019/2018-2019-cyber-liability-policy-xl-catlin.pdf. For more examples, *see* Philia. Indem. Ins. Co., Cyber Security Liability Coverage Form 12 (2012), https://www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form36-8835.pdf (excluding coverage for any "failure, outages, or disruption of power, utility

services, satellites, or telecommunications external services not under your direct operational control, including but not limited to electrical disturbances, surge, brownout, or blackout"); Beazley, BEAZLEY INFOSEC 16 (2017), https://www.beazley.com/documents/TMB/Policies/beazley-tmb-infosec-policy.pdf (excluding coverage "with respect to the First Party Loss insuring agreements" for "3. failure or malfunction of satellites or of power, utility, mechanical or telecommunications (including internet) infrastructure or services that are not under the Insured Organization's direct operational control"); N. Star Mut., Cyber Liability Insurance Coverage Part Endorsement 4 (2016), https://northstarmutual.com/UserFiles/Documents/forms/policyforms/Current/CF-2123%2003-16.pdf (excluding coverage for any "'claim' based upon, arising out of, resulting from, in consequence of, or in any way involving: 1. Satellite failures; 2. Electrical or mechanical failures and/or interruptions including, but not limited to, electrical disturbance, spike, brownout, or blackout; or 3. Outages to gas, water, telephone, cable, telecommunications or other infrastructure, unless such infrastructure is under your direct operational control and such 'claim' is otherwise covered under Coverage Agreement F or Coverage Agreement H"); HSB Eng'g Ins., HSB Cyber Insurance 21, https://www.constructaquote.com/media/1519/hsbeil_cyber_policy_wording.pdf ("The following exclusions apply to the whole of your policy. We will not pay for any claim, cost or loss caused by or resulting from the following: . . . 11. Telecommunications systems Atmospheric or environmental conditions causing temporary interference with any satellite signal."); Vero Liability, Cyber Liability Policy Wording 7, https://www.veroliability.co.nz/documents/wordings/cyber-policy-wording.pdf (excluding coverage for "Supply/Infrastructure Failures based upon, directly or indirectly arising from, or attributable to any satellite failures, electrical or mechanical failures and/or interruption including, but not limited to, electrical disturbance, spike, brownout or blackout, outages to gas, water, telephone, cable, telecommunications, or other infrastructure, unless such infrastructure is under the Insured's operational control and such claim is as a direct result of any Cyber Event"); URB, Cyber Insurance Endorsement 6 (2016), https://www.enia.com/Content/factsheets/Cyber%20Liability%20CL-100%20Endorsement.pdf (excluding coverage for any "claim based upon, arising out of, resulting from, in consequence of, or in any way involving: 1. Satellite failures; 2. Electrical or mechanical failures or interruption including, but not limited to, electrical disturbance, spike, brownout, or blackout; or 3. Outages to gas, water, telephone, cable, telecommunications or other infrastructure, unless such infrastructure is under your direct operational control and such claim is otherwise covered under Coverage F"); Zurich, Cyber, Security and Privacy Protection Insurance 21–22 (2018), https://www.zurich.com.au/content/dam/au-documents/business-insurance/financial-lines/security-and-privacy-protection/security-and-privacy-protection-insurance-policy.pdf (excluding coverage for "[f]ailure of utilities based upon, arising out of or attributable to any mechanical or electrical failure, interruption or outage, however caused, including any electrical power interruption or surge, brownout, blackout, short circuit, over voltage, or

But exclusions for loss caused by the disruption of broad-based utilities or internet services only limit coverage for one sub-type of potentially catastrophic cyber risk—and a potentially narrow one, at that. Many, if not most, cyberattacks with the potential to cause widespread, catastrophic losses do not attempt to disable broad-based internet functionalities or the utilities on which they rely. To the contrary, they often rely on the internet and associated utilities to transmit malicious code to numerous firms' computers, exploiting common software vulnerabilities.[148] NotPetya is once again illustrative.

Moreover, coverage exclusions for disruptions to some of the most important broad-based internet utilities run the risk of substantial over-breadth, which has tended to limit policyholders' willingness to accept these exclusions. To illustrate, several cyber insurers have excluded coverage for losses that are attributable to "cloud service provider failure."[149] From insurers' perspective, such an exclusion makes sense because the failure of a major cloud service provider does indeed represent one of the most likely ways in which a catastrophic cyber loss could occur given that the vast majority of global cloud services outside of China are only provided by three firms—Amazon, Microsoft, and Google.[150] But policyholders (who, at least in the cyber insurance setting, are often advised by highly sophisticated intermediaries that monitor competing policy terms)[151] have largely balked at such exclusions because the increasing importance of cloud services means that they also have a substantial potential to apply to ordinary, non-catastrophic losses that policyholders expect to be covered. Consider, for instance, a temporary and partial disruption at a cloud provider, which resulted in a small number of firms experiencing several weeks of business interruptions. That is precisely the kind of loss that policyholders buy cyber insurance coverage to protect against.

---

power fluctuation or outage to gas, water, telephone, cable, satellite, telecommunications, the internet or any component thereof including hardware or software or any other infrastructure," with limited exceptions).

[148] EASTWEST INST., *supra* note 134, at 5.

[149] *See, e.g.*, AIG, CYBEREDGE 2.0 2016, at 11 (2016), https://www.aig.co.il/wp-content/uploads/CyberEdge-2.0.pdf (excluding coverage for cloud services provider failure, but then offering this coverage as an optional endorsement); s*ee also* Lubin, *supra* note 104, at 6 (noting that such exclusions for cloud services failure are not common).

[150] *See, e.g.,* GUY CARPENTER, *supra* note 4, at 14.

[151] *See, e.g.*, Rawan Aljamal, Ali El-Mousa & Fahed Jubair, *A Comparative Review of High-Performance Computing Major Cloud Service Providers*, 9 INT'L CONF. ON INFO. & COMMC'N SYS. 181, 181–86 (2018).

2. Restricting Coverage by Type of Loss, However It Is Caused

A second potential strategy that insurers can use to limit their exposure to catastrophe risk is to restrict coverage for specific types of losses that policyholders may experience, irrespective of how that loss is caused. For instance, some property/casualty insurers exclude or limit coverage for losses "consisting of" potentially catastrophic forms of damage, such as mold or nuclear damage, irrespective of the underlying cause of that damage.

Adopting this strategy is difficult for cyber insurers because the harms that policyholders may experience in a catastrophic event are identical to the harms they may experience in a standard cyberattack. Cyberattacks can be divided into three categories based on the type of harm they cause.[152] First, availability attacks are designed to prevent access to a network. Second, cyberattacks can target confidentiality, seeking to extract sensitive information. Third, cyberattacks can target a computer system's integrity by modifying code so as to alter the processes or perceptions of individuals or mechanical processes that rely on computer information to make decisions.

Unfortunately for cyber insurers, each of these three types of harms from cyberattacks can result in either ordinary or catastrophic losses, depending on innumerable variables. For instance, an availability attack can vary from a simple denial of service that can disrupt a company's website for a short time, to a lengthy attack that can disrupt the operations of a firm's critical infrastructure for weeks or months.[153] Similarly, a confidentiality attack can result in a relatively limited and well-modeled set of losses, such as the breach of consumers' credit card information.[154] In other cases, however, such an attack can result in the disclosure of sensitive corporate secrets.[155] Finally, while integrity attacks may have the most potential for catastrophic effect, these too can vary significantly in the scale of the losses they produce, ranging from altering the appearance of websites to producing mass blackouts.

Perhaps even more importantly, all three of these types of harms can, depending on the underlying cyberattack and networks through which those attacks propagate, impact only a single target or numerous firms, the latter resulting in highly correlated

---

[152] *See* SINGER & FRIEDMAN, *supra* note 141, at 70–71.

[153] *Id.* at 70.

[154] Data breaches involving sensitive consumer information, like credit card numbers, are relatively well modelled because there is now twenty years of fairly robust data on the types of economic harms that these hacks produce.

[155] Some cyber insurers have indeed experimented with coverage exclusions for the cyber theft of intellectual property.

(and potentially catastrophic) losses. Thus, an availability attack can take down a single firm's website or, conceivably, could limit the availability of an entire category of firms using particular software or internet protocols. Likewise, a cyberattack could extract confidential information from a single firm, or it could compromise confidential information held by firms within an entire industry that, for instance, use the same software. It is for these reasons that cyber insurance policies do not typically contain any exclusions that target the types of harm caused by a cyberattack.[156]

An alternative way to distinguish among different types of losses that a cyberattack can cause is to focus on potential methods of responding to those harms through insurance payments. Indeed, cyber insurance policies generally provide varying coverage amounts for different types of first-party costs or losses that may result from a cyberattack. These include costs related to investigating the cause of an attack; restoring ordinary business services; mounting a public relations campaign to manage reputational harms; paying ransoms demanded by cyber attackers, and compensating policyholders for business interruption losses.[157] Similarly, cyber insurance policies have historically divided potential third-party losses that may arise from a cyberattack into different categories, including liability stemming from compromising a client's or third party's confidential data; propagating malware; abetting a denial of service attack; failing to provide authorized access to data; and defamation or invasion of privacy.[158]

Although these categories of costs and losses provide a helpful mechanism for cyber insurers to structure policy limits (a topic to which we shall return later),[159] they do not provide a workable mechanism for formulating coverage exclusions that are aimed at limiting an insurer's exposure to potentially catastrophic losses. This is because each of these types of losses can result either from an individualized and ordinary cyberattack or from a cyberattack that simultaneously impacts numerous firms at once, thus producing correlated losses. To be sure, some types of losses may be more likely to be correlated in this way than others. For instance, simulations of cyber catastrophes suggest that business interruption losses are particularly likely to be correlated across different firms, and thus to produce potentially catastrophic losses.[160] But these types of losses also figure prominently in ordinary,

---

[156] *See* Romanosky et al., *supra* note 132, at 7.

[157] *Id.* at 5–6.

[158] *Id.* at 6.

[159] *See infra* Part III.C.

[160] *See* GUY CARPENTER, *supra* note 4, at 14 ("[I]t is notable that business interruption (BI) costs, caused when supply chains stall or factories are offline, feature heavily in the

individualized cyberattacks. Consequently, cyber insurers have no viable way of excluding coverage for these types of losses without undermining the protection against risk that their policies are, in fact, designed to cover.

3. Excluding by Motivation of Persons or Entities Causing the Loss

A third strategy that insurers sometimes use to limit their exposure to catastrophe risk is to exclude coverage for losses that are caused by actors with certain types of motivations, agendas, or capacities. This approach is common in standard property/casualty insurance policies, which typically exclude coverage for losses that are caused by acts of war or governmental actions. It also mirrors terrorism exclusions that were added to many policies in the wake of 9/11.[161]

This approach to limiting coverage for catastrophic risks makes some sense because certain types of actors are much more likely to be motivated by the desire to cause catastrophic losses.[162] The goal of terrorist attacks, after all, is precisely to cause catastrophic losses that will garner significant attention and produce fear.[163] Similarly, the aim of warring countries is often to cause catastrophic losses to the enemy so as to disrupt their economies and induce them to surrender. And while government actions often are not aimed at causing catastrophic losses, the generality of many governmental mandates and the sheer power of government to impose losses on large groups of people creates the possibility of massively correlated losses.

Linking coverage to the types of hackers behind an attack makes sense for a

---

catastrophe costs. The BI components of cyber insurance have evolved rapidly in the last few years, and the take-up by purchasers has increased as the awareness of the criticality of systems has grown. The low-frequency and high-severity aspects of catastrophic BI events affirm this improving understanding of these exposures.").

[161] *See, e.g.*, Boardman, *supra* note 26, at 803.

[162] As Tom Baker puts it: "[O]rdinary cyber events are more like ordinary crime and negligence and, typically, are not intended to destroy the businesses affected. When the perpetrator acts with intention, the objective typically is theft or ransom. When the objective is theft, the perpetrator tries hard not to disrupt the business; where the object is ransom, the perpetrator needs to provide credible evidence that the disruption can be undone, or the business will not pay the ransom. By contrast, state sponsored or encouraged cyberattacks are more like terrorism: the objective is permanent destruction, greatly increasing the business interruption loss, the costs of rebuilding the system, and the data restoration loss." Tom Baker, *Back to the Future of Cyber Insurance*, 3 PRO. LIAB. UNDERWRITING SOC'Y J. 1, 5–6 (2019).

[163] *See* Boardman, *supra* note 26, at 804 n.112.

second reason as well: only certain type of hackers—which are often labelled as Advanced Persistent Threats (APTs)—are likely to have the technical capacity to unleash cyberattacks that have the potential to cause catastrophic losses. Doing so often requires exploiting so-called "zero-day" vulnerabilities—those which are unknown to the software vendors at the time of the attack.[164] Discovering and exploiting such zero-day vulnerabilities is hardly the norm for amateur hackers; it requires an immense amount of technological savvy and resources, often by actors with a significant relationship with a State.[165]

For these reasons, cyber insurers make frequent use of these types of exclusions to attempt to limit their catastrophe risk exposure. According to one recent survey, approximately 75% of cyber insurance policies sold on the admitted market exclude coverage for an "act of terrorism, war, or military action."[166] Other policies simply exclude attacks committed by a "government entity or public authority."[167]

Unfortunately for cyber insurers, this approach is, at best, only of limited effectiveness when it comes to mitigating their exposure to catastrophe risk, for several key reasons. First, it is often difficult or nearly impossible to reliably identify the perpetrators of cyberattacks.[168] A lengthy literature explores the technical difficulties associated with attribution of cyberattacks, which stem in large part from

---

[164] *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, 787–99 (2016).

[165] To be sure, the role between states and private actors is often blurred in the context of zero-day vulnerabilities, with states sometimes looking to purchase such vulnerabilities from hackers in black and gray markets rather than discovering these vulnerabilities themselves. *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 482 (2017).

[166] Daniel W. Woods & Jessica Weinkle, *Insurance Definitions of Cyber War*, 45 GENEVA PAPERS ON RISK & INS. (ISSUES & PRAC.) 639, 645 (2020); Romanosky et al., *supra* note 132, at 7.

[167] *See* ORGANIZATION FOR ECONOMIC COORDINATION AND DEVELOPMENT, THE ROLE OF PUBLIC POLICY AND REGULATION IN ENCOURAGING CLARITY IN CYBER INSURANCE COVERAGE 18 (2020), at www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-EncouragingClarity-in-Cyber-Insurance-Coverage.pdf.

[168] Gloria Gonzalez, *Cyberattack Coverage Dispute Hinges on War Exclusion Argument*, BUS. INS. (Apr. 10, 2019), https://www.businessinsurance.com/article/20190410/NEWS06/912327806/Cyberattack-coverage-dispute-hinges-on-war-exclusion-argument ("Very seldom is there going to be sufficient evidence to actually prove the war exclusion" because malicious actors are "sophisticated enough that everything is anonymized and you're not going to see it."); Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies*, 129 YALE L.J.F. 64, 68 (2019).

increasingly sophisticated technologies that can hide a perpetrator's identity.[169] For instance, a hacker may launch an attack from a botnet consisting of multiple unwitting victims' computers.[170] While it may be possible to identify the means by which an attack is launched, it is much more difficult to determine where they originate.[171] And even if the particular location from which an attack originated can be identified, determining who was operating those computers and whether they were acting under the control or support of a government is even more difficult.[172] Indeed, in many cases this line between state-sponsored and individual hacking is deliberately blurred.[173] Governments may "crowd-source" cyberattacks or rely on private groups to design or launch them, while private actors may be motivated by patriotic or national interests.[174]

For these reasons, government intelligence agencies are currently the primary entities capable of reliably attributing cyberattacks to specific actors.[175] The problem, however, is that government attributions carry uncertain weight in court, because the underlying intelligence on which they are based is typically classified.[176] As a result it is difficult if not impossible for insurers and policyholders to independently scrutinize these claims of attribution. This is particularly problematic because intelligence agencies may face political pressures to attribute cyberattacks to foreign governments for strategic reasons, especially when the evidence is murky. And while certain non-governmental actors are increasingly developing the ability

---

[169] *See, e.g.*, SINGER & FRIEDMAN, *supra* note 141, at 72–76; William C. Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AM. J. INT'L. L. UNBOUND 191 (2019).

[170] *See* SINGER & FRIEDMAN, *supra* note 141, at 73.

[171] *Id.*

[172] *Id.*

[173] Ariel E. Levite & Wyatt Hoffman, *A Moment of Truth for Cyber Insurance*, LAWFARE INST. (Feb. 7, 2019, 9:21 AM), https://www.lawfareblog.com/moment-truth-cyber-insurance ("Unlike physical attacks, the dividing lines between state-sponsored or state-abetted cyber aggression and organized cybercrime are far more (and often deliberately) blurred," meaning that "even when it is possible to attribute a cyberattack to a malicious perpetrator, it is much harder to confidently establish that a nation-state is complicit").

[174] *See* Singer & Friedman, *supra* note 141, at 74–75.

[175] *See* Lubin, *supra* note 104, at 44; Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520 (2020) (exploring a decentralized approach to attributing cyberattacks that relies on collaboration among various non-governmental actors).

[176] *See* Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AM. J. INT'L. L. UNBOUND 213, 215 (2019).

to attribute cyberattacks, the nature of attribution by these entities is still highly contested, implicating a range of unsettled legal and political issues, including the relevant evidentiary standards for making attribution.[177]

These difficulties of attribution are on vivid display in the high-profile, and ongoing, case of *Mondelez Intl. Inc. v. Zurich Am. Ins. Co.*[178] The plaintiff-policyholder in this case, Mondelez, is a major corporation that manufactures a variety of snack and beverage products. It purchased from Zurich a property insurance policy with $100 million policy limits that specifically included cyber coverage, including business interruptions resulting from cyberattacks.[179] In mid-2017, Mondelez—like numerous large companies across the world—was crippled by the NotPetya attack, which ultimately destroyed approximately 1,700 of the company's servers and 24,000 of its laptops, causing massive disruptions in Mondelez's operations.[180] After a year of investigations, Zurich denied Mondelez's claim in its entirety on the basis of a war exclusion in its policy,[181] relying substantially on statements from several governments, including the U.S., attributing

---

[177] Eichensehr, *supra* note 175, at 523.

[178] *See* Complaint, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., 2018 WL 4941760 (Ill. Cir. Ct.) (Trial Pleading); s*ee* WOLFF, *supra* note 143, at ch. 5.

[179] *See* Mondelez, *supra* note 178 (noting that the policy's trigger of coverage included coverage for "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction").

[180] *See* Brian Corcoran, *What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict*, LAWFARE (March 8, 2019, 8:00 AM), https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict.

[181] That exclusion applied to all:

> [L]oss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> . . .
>
> 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
>
> (i) government or sovereign power (de jure or de facto);
>
> (ii) military, naval, or air force; or
>
> (iii) agent or authority of any party specified in i or ii above.

Mondelez, *supra* note 178, at 4.

the NotPetya attack to the Russian government. Because the insurer bears the burden of proof in demonstrating the application of an exclusion, it remains to be seen how or whether the insurer will be able to convince the court as a factual matter that Russia was indeed the culprit in the NotPetya attack.[182]

A second key reason that exclusions linked to the motivations of cyberattackers are of limited effectiveness is that, even when the perpetrators of a cyberattack can be identified, determining whether the attack amounted to an act of war or terrorism is both immensely complicated and largely unaddressed in existing caselaw. Although courts have occasionally faced interpretive questions regarding whether the acts of a government constituted "war" under the terms of an insurance policy exclusion,[183] the sparsity of precedent and the lack of maturity in cyber insurance markets means that there is no current precedent on when and if cyberattacks can constitute acts of war or terrorism.[184] Numerous questions on this front remain open, including whether an act of war or terrorism requires physical in addition to economic harm, whether it matters if the primary targets of the cyberattack were private or public entities, and whether it is necessary for the ultimate purpose of the attack to be "coercion and conquest."[185]

Here too, the *Mondelez* case vividly demonstrates the difficulties of establishing when a governmental act constitutes war or terrorism. Even assuming that Zurich can successfully demonstrate that Russia launched the NotPetya attack, it faces an additional hurdle in showing that this attack constituted an Act of War. Mondelez, for instance, has argued that characterizing a cyberattack in this way is "unprecedented," as no insurer has ever invoked this exclusion outside the context of "conventional armed conflict or hostilities."[186] Mondelez has also argued that the exclusion's application to the NotPetya loss was ambiguous in light of "Zurich's failure to modify that historical language to specifically address the extent to which

---

[182] Merck also suffered damage in the NotPetya attack and brought suit against its insurers. *See* Merck & Co., Inc. v. Ace Am. Ins. Co., No. UNN-L-002682-18, 2018 WL 8415885 (N.J. Super. Aug. 2, 2018).

[183] *See, e.g.*, Pan Am. World Airways v. Aetna Cas. and Sur. Co., 505 F.2d 989, 1012 (1974); Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp.1460 (S.D.N.Y. 1983); Sherwin-Williams Co. v. Ins. Co. of the State of Pa., 863 F. Supp. 542 (N.D. Ohio 1994).

[184] *See* Charles J. Dunlap Jr., *"Cybervandalism" or "Digital Act of War?" America's Muddled Approach to Cyber Incidents Will Not Deter More Crises*, 42 N.C.J. INT'L L. 989–90 (2017); WOLFF, *supra* note 143, at ch. 5.

[185] *See* Thomas Reagan & Matthew McCabe, *NotPetya Was Not Cyber "War"*, MARSH (Aug. 2018), https://www.mmc.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html; WOLFF, *supra* note 143, at ch. 5.

[186] *See* Mondelez, *supra* note 178, at 4.

it would apply to cyber incidents."[187] Given these complexities in applying exclusions linked to war or terrorism in the cyber-insurance setting, some cyber policies have begun to exclude coverage for all cyberattacks launched by a state, irrespective of whether they constitute an act of war or terrorism.[188]

A third key limitation of cyber insurance exclusions for acts of war or terrorism is that it is not even clear how well such acts truly correlate with catastrophic risk. In some cases, non-state cyberattackers may be motivated by the desire to cause large-scale harms in order to promote change or generate attention. For instance, the prominent hacking group Anonymous has coordinated a broad range of wide-scale cyberattacks, most of which are motivated by the apparent goal of limiting government censorship.[189] Just as importantly, state-sponsored cyberattacks may be designed not to cause catastrophic loss but to harm particular companies, as was North Korea's apparent hack of Sony Pictures in response to its development of a movie, The Interview, which mocked the country's leader.[190] Additionally, states may frequently prefer to launch cyberattacks that do not cause wide-spread disruptions, as this strategy can reduce the risk of retaliation.

All of this is important for two independent reasons. The first, and more obvious, is that cyber insurers' exclusions for warfare, terrorism, and government action often fail to limit coverage for catastrophic risk while preserving coverage for non-catastrophic risks. Second, this very fact is increasingly causing policyholders to seek coverage that does not contain these exclusions.[191] This is particularly true for sizable policyholders, which often extensively evaluate their coverage options with the help of highly sophisticated advisers. Additionally, because the cyber insurance market is experiencing so much growth and new entry, these policyholder preferences are having a substantial impact on the terms of policies, which have been becoming increasingly more favorable for policyholders as insurers compete for business.[192] The very public, and costly, feud between Mondelez and Zurich

---

[187] *Id.*

[188] *See* Lubin, *supra* note 104, at 42 n.187.

[189] *See* Gabriella Coleman, *Anonymous in Context: The Politics and Power behind the Mask*, CIGI INTERNET GOVERNANCE PAPERS, Sept. 2013.

[190] Stephan Haggard & Jon R. Lindsay, *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*, 117 E.-W. Ctr. 1, 1–2 (2015).

[191] *See* Daniel W. Woods & Jessica Weinkle, *Insurance Definitions of Cyber War*, 45 GENEVA PAPERS ON RISK & INS. 639 (2020).

[192] *See* GUY CARPENTER, *supra* note 4, at 7 ("Increasing competition as new entrants seek to take advantage of the growth potential has created pressure on rates as well as an expansion of available coverage."); *EU-U.S. Insurance Dialogue Project: The Cyber*

regarding the war exclusion will likely only increase consumer interest in policies that forego this exclusion.

B. THE DIFFICULTY OF USING UNDERWRITING TO LIMIT CATASTROPHE RISK IN CYBER INSURANCE

When insurers cannot confidently use coverage exclusions to limit their exposure to catastrophic risk, they can often fall back on a second strategy: using underwriting criteria that limit their coverage of potentially correlated risks. To illustrate, a property insurer might cap its aggregate coverage of coastal homes in Florida because of the prospect that these homes could all be damaged by the same hurricane, thus resulting in catastrophic losses notwithstanding exclusions for flooding. Similarly, individual property insurers in California have recently begun limiting their exposure in areas that are prone to wildfires, given their inability to limit coverage for fire loss.[193] And a D&O liability insurer might decide to only insure a limited number of companies in any particular industry.

Unfortunately for cyber insurers, this approach to limiting their catastrophic risk exposure is also severely hampered by the unique nature of cyber risk.[194] This is because correlated cyber risks cannot be easily categorized by geographic region, industry, or any other policyholder characteristic that can be efficiently identified in the underwriting process. Consequently, while cyber insurers typically engage in extensive underwriting to attempt to assess individual applicants' cyber exposures,[195] no amount of underwriting can confidently assure them that the risks posed by any one of their cyber insurance policyholders are not highly correlated

---

Insurance Market, EUR. INS. & OCCUPATIONAL PENSIONS AUTH. 6 (Oct. 31, 2018), https://www.eiopa.europa.eu/sites/default/files/publications/other_documents/181031_eu-us_project_cyber_insurance_white_paper_publication.pdf (noting that "increasing competition and a limited understanding of the risks" is causing "broadening coverage, terms, and conditions").

[193] *See* Christopher Flavelle, *As Wildfires Get Worse, Insurers Pull Back from Riskiest Areas,* N.Y. TIMES (Aug. 20, 2019), https://www.nytimes.com/2019/08/20/climate/fire-insurance-renewal.html.

[194] *See generally* Kjartan Palsson, Steinn Gudmundsson & Sachin Shetty, *Analysis of the Impact of Cyber Events for Cyber Insurance*, 45 GENEVA PAPERS ON RISK & INS. (ISSUES AND PRAC.) 564 (2020) (noting that "[t]he mass adoption of cyber insurance will be predicated on the ability to conduct quantitative risk assessment").

[195] *See generally* Jason R.C. Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith & Sadie Creese, *The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes*, 2020 INT'L CONF. ON CYBER SITUATIONAL AWARENESS, DATA ANALYTICS & ASSESSMENT (2020).

with the risks posed by other policyholders.[196] This is true even if a company's policyholders operate in different industries, across different parts of the world, using different types of computer systems.

Consider geography first, which is by far the most common mechanism that most insurers use to diversify their risk exposures. Indeed, geographic diversity of insured risks is one of the bedrock principles of the global reinsurance industry.[197] But, unlike virtually all other insured risks, cyber risks are not geographically bound.[198] As Singer and Friedman explain:

> [A] cyberattack is not constrained by the usual physics of traditional attacks. In cyber space, an attack can literally move at the speed of light, unlimited by geography or political boundaries. Being delinked from physics also means it can be in multiple places at the same time, meaning the same attack can hit multiple targets at once.[199]

The NotPetya cyberattack is once again starkly illustrative of this reality. In addition to disabling Mondelez—a multi-national snack production and distribution company—the attack infected the computer systems of numerous international companies across the globe hours after it was launched. Severely impacted firms included the large Ukrainian bank Oschadbank; the U.S. pharmaceutical giant Merck; the Danish shipping company Maersk; a major chocolate manufacturer located in Tasmania; FedEx's European subsidiary TNT Express; French construction company Saint-Gobain; British manufacturer Reckitt Benckiser; and Russian state oil company Rosneft.[200] The NotPetya attack spread so broadly because it gained entry to a firm's network if any computer within that network contained the M.E.Doc software, and then replicated within that network by taking advantage of known vulnerabilities within the Microsoft Operating System.[201]

---

[196] *See* Hofmann & Wilson, *supra* note 134, at 6–7 (exploring the difficulties cyber insurers have in using underwriting to assess accumulation risk).

[197] *See* J. David Cummins & Mary A. Weiss, *The Global Market for Reinsurance: Consolidation, Capacity, and Efficiency*, *in* PAPERS ON FINANCIAL SERVICES 195 (Robert E. Litan & Anthony M. Santomero eds., 2000).

[198] *See* GUY CARPENTER, *supra* note 4, at 8 ("Cyber aggregation events are not necessarily discrete attacks that affect only limited geographies or individual insureds.").

[199] SINGER & FRIEDMAN, *supra* note 141, at 68–69.

[200] *The Untold Story of NotPetya*, *supra* note 143.

[201] *See id.* According to the Guy Carpenter study, service interruption exploiting a

The unsuitability of using policyholder location to diversify risk, moreover, is not simply a byproduct of the fact that cyberattacks can aggregate across different geographically diverse firms nearly instantaneously, by exploiting vulnerabilities in common software or operating systems. Location is also unsuitable because firms across the globe increasingly rely on other potential "single points of failure" besides software that can cause losses to quickly aggregate across firms, such as reliance on the same sources of cloud services (such as Amazon, Microsoft, and Dropbox) and email services (such as Google's Gmail).[202] As a result, an attack on any single major firm could produce massive insurance losses across the globe. Recent simulations by the risk specialist firm Guy Carpenter, for instance, suggest that an attack on a major cloud service provider could result in insured losses of approximately $14 billion, principally due to the resulting business interruptions that large companies would experience.[203] Similarly, an attack on a major email provider could result in nearly $20 billion in insured losses, principally due to investigative and response costs, as well as legal liability.[204]

Efforts to diversify cyber risk exposures based on non-geographic criteria—such as by industry, which can serve as a useful diversification tool in coverage lines like D&O insurance—are also of only limited effectiveness in curbing cyber catastrophe risk exposure, for many of the same reasons we have just identified.[205] Simulations of potential cyber catastrophes reveal that insured losses would cross-cut a broad array of industries, with the magnitude of losses principally based on firms' revenues.[206] This is because firms and employees across different industries rely on

---

day zero vulnerability—in other words, a vulnerability that had not previously been discovered and patched by the operating system provider—in a popular operating system could result in insured losses of approximately $24 billion, once again due principally to business interruption costs. GUY CARPENTER, *supra* note 4, at 19.

[202] *See* GUY CARPENTER, *supra* note 4, at 16, 20.

[203] *See id.* According to one survey, more than 80% of firms indicated they would be relying on cloud storage as of 2020. *See* Louis Columbus, *83% Of Enterprise Workloads Will Be In The Cloud By 2020*, FORBES (Jan. 7, 2018, 7:36 PM), https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/?sh=13ef64416261.

[204] *See* GUY CARPENTER, *supra* note 4, at 20.

[205] Firms across various industries purchase cyber insurance. These include firms specializing in information technology, financial services, retail, healthcare, and industrials.

[206] In Guy Carpenter's simulations, losses due to the various cyber catastrophe scenarios were spread across industries in relative proportion to premiums. Similarly, the firms experiencing the greatest losses were those with the largest revenues, regardless of industry sector. GUY CARPENTER, *supra* note 4, at 14.

the same types of computers, software, network connections, and cyber-defense strategies.[207] Once again the NotPetya cyberattack illustrates this point: recall that the virus crippled firms across a wide array of industries, including shipping, manufacturing, and medical care.

The trans-industry nature of cyber risk is also demonstrated by cyber insurers' actual underwriting practices, which, for most cyber insurers, do not vary significantly by industry.[208] For instance, one recent survey found that only about 25% of sampled cyber insurers used different types of security questionnaires for different types of applicants.[209] Similarly, the actual questions that insurers ask of applicants in these questionnaires are generally not industry-specific, focusing on more general considerations like IT Security Budget/Spending; past cybersecurity incidents; organizational policies and procedures regarding cybersecurity; extent of outsourcing of network, computer system, or information security systems; types of confidential/sensitive data collected and stored; size and number of major clients; and types of cybersecurity measures, like firewalls and data encryption technology.[210]

Of course, cyber insurers have some means of underwriting to limit their exposure to correlated risk. They can, and sometimes do, take into account factors that might suggest possible aggregation risk, such as an applicant's reliance on potential single points of failure like cloud services,[211] or its reliance on one particular type of hardware or software.[212] Similarly, cyber insurers can, and do,

---

[207] *See* Hofmann & Wilson, *supra* note 134, at 15–16. In fact, it is currently not possible to diversify on the basis of operating system or cloud provider because there are only two or three options for each of these.

[208] Admittedly, this reality may simply demonstrate that cyber insurers are not being sophisticated enough in their underwriting. But to some extent, this point is similar to ours: the difficulty that most cyber insurers currently face in distinguishing cyber risk factors that differ across industry is a practical reality in today's marketplace.

[209] *See* Romanosky et al., *supra* note 132, at 8. At least one cyber insurer, however, used separate "questionnaires for Technology Professionals, Accounting and Financial Professionals, and Small Firm Accounting and Financial Professionals." *See id.*; *see also* Daniel Woods, Ioannis Agrafiotis, Jason R.C. Nurse, & Sadie Creese, *Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms*, 8 J. INTERNET SERVS. & APPLICATIONS 1, 3 (2017) (discussing information that cyber insurers use in underwriting, much of which is not specific to different industries, as well as the use of standardized underwriting forms that use questions that are not relevant to some applicants).

[210] *See* Romanosky et al., *supra* note 132, at 8.

[211] *See* Nurse et al., *supra* note 195, at 4.

[212] *See* Hofmann & Wilson, *supra* note 134.

attempt to model and predict the risk of such correlated losses.[213] Our primary point here is simply that these techniques for limiting exposure to aggregation risk through underwriting are only partially effective, and are likely to remain so in the near future.[214]

C. LIMITS MANAGEMENT AND THE CYBER INSURANCE GAP

The unique difficulties cyber insurers face in using such conventional techniques as coverage restrictions and underwriting to limit their exposure to catastrophic loss helps to explain a central feature of cyber insurance markets: cyber insurers typically insist on setting policy limits that are well below policyholders' economic exposures to cyber risk.[215] As Tom Baker explains, such "limits management" by cyber insurers includes insisting on limits for:

> the amount of the cover provided to any particular customer against any particular set of risks; the amount of cover provided to each customer segment against a set of risks; the amount of cover provided overall against a set of risks; and the relationship of all these things to the other risk and customer segments of the insurer.[216]

By setting artificially low policy limits for individual policyholders, groups of related policyholders, and groups of related risks, cyber insurers can partially protect themselves against the prospect that massively correlated policyholder losses will jeopardize their solvency.[217]

---

[213] *See, e.g.*, Rainer Böhme & Gaurav Kataria, *Models and Measures For Correlation In Cyber-Insurance (*Workshop of Economic Information Security, No. 3, 2006), https://econinfosec.org/archive/weis2006/docs/16.pdf; Hofmann & Wilson, *supra* note 134, at 16–17.

[214] *See* Nurse et al., *supra* note 195, at 4.

[215] *See, e.g*., *The Betterley Report: Cyber/Privacy Insurance Market Survey – 2020* (June 2020) (copy on file with the authors); Talesh, *supra* note 18, at 426 (noting that "some insurers offering cyber insurance limit their coverage to under $20 million"). This approach to limiting exposure to cyber catastrophe risk is not unprecedented: for instance, the National Flood Insurance Program limits coverage to $250,000 in order to limit its exposure to catastrophe risk. But in most coverage lines, insurance is typically available up to policyholders' potential losses, thus facilitating the transfer of risk that is at the heart of the insurance relationship.

[216] *See* Baker, *supra* note 162, at 4.

[217] *Id.*

However, there are various indications that cyber insurers' insistence on artificially low policy limits is loosening or becoming less of a practical barrier. Although cyber insurance markets are subject to many of the same cycles as other insurance markets, they have experienced substantial growth in recent years.[218] Recent estimates predict that written premiums will continue to grow at a substantial, if uneven, pace, averaging around 25% annually.[219] These trends have caused some insurers to offer higher policy limits than they previously did, though here too trends are cyclical and uneven.[220] Perhaps even more importantly, brokers and cyber insurers are increasingly willing and able to build large towers of cyber insurance coverage in ways that were previously difficult or impossible.[221]

---

[218] *See* GOV'T ACCOUNTABILITY OFF., Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, 5 (May 20, 2021), https://www.gao.gov/products/gao-21-477. To illustrate, cyber insurance premiums doubled between 2015 and 2017, *see* Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html; they are on pace to double again between 2017 and 2020. GUY CARPENTER, *supra* note 4, at 7 ("According to some estimates, the global market volume for cyber insurance will grow to USD 8 to 9 billion by 2020 – more than twice that of 2017.").

[219] *See* MARQUAL IT SOLUTIONS PVT. LTD, GLOBAL CYBER INSURANCE MARKET (2019–2025).

[220] *Compare* O'Brien et al., Looking Beyond the Clouds: A U.S. Cyber Insurance Industry Catastrophe Loss Study, MARSHMCLENNAN (last visited Mar. 21, 2021), https://www.mmc.com/insights/publications/2020/october/looking-beyond-the-clouds--a-u-s--cyber-insurance-industry-catas.html ("Increasing competition as new entrants seek to take advantage of the growth potential has created pressure on rates as well as an expansion of available coverage."), with GAO REPORT, *supra* note 218 (noting reports from industry insiders that insurers are reducing coverage limits for some industry sectors). For instance, according to leading insurance broker Marsh & McLennan, cyber policy limits grew substantially in 2018, with "average limits purchased by all companies rising 11% to $20.9 million" and average limits increasing by more than 25%, to $62.4 million, for companies with $1 billion in revenue or more. *See generally Cyber Insurance Buyers as Awareness Grows*, MARSH (2019), https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html.

[221] *See, e.g.*, Katie Dwyer, *Cyber Insurance Capacity Could Quadruple in Six Years; Don't Let Your Coverage Lag*, RISK & INS. (Mar. 6, 2020), https://riskandinsurance.com/commercial-cyber-insurance-could-quadruple-in-six-years-dont-let-your-coverage-lag/; Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem. (reporting that in 2020, "the global insurance community saw the first cyber insurance program to exceed $1 billion — and the second").

Whatever the future may hold, cyber insurers' past insistence on aggressive limits management is one important explanation for the much-discussed "cyber insurance gap" between actual cyber risk and insurance coverage of this risk.[222] So too, of course, are demand-side forces: many firms continue to resist purchasing cyber insurance, notwithstanding their substantial exposure to cyber risk.[223] Taken together, these forces have resulted in total annual premiums for cyber insurance globally of only about $7.5 billion in recent years.[224] By contrast, total property/casualty insurance premiums are approximately 40 times that amount just in the United States.[225] For further context, firms globally spend approximately $120 billion on cybersecurity, according to Munich Re.[226] These figures help explain why the bulk of economic losses from NotPetya, which exceeded $10 billion, were not borne by the insurance industry: most of the victims of this attack either did not have cyber insurance coverage or had quite restrictive limits on such coverage.[227] For similar reasons, a 2017 simulation of cyber catastrophes found that total insured losses could range from between 7 to 17 percent of total economic costs, depending on the nature of the attack.[228]

This cyber insurance gap leaves many policyholders heavily exposed to cyber risk. Perhaps even more importantly, however, the gap also limits the capacity of the cyber insurance industry to promote effective cybersecurity.[229] It is difficult for

---

[222] To be sure, other factors also contribute to cyber insurers' insistence on low coverage limits, including the fact that available actuarial data to predict even the ordinary range of potential losses is limited. *See generally* U.S. CYBERSPACE SOLARIUM COMM'N, https://www.solarium.gov (last visited Mar. 6, 2021).

[223] *See* Johansmeyer, *supra* note 221 ("On the demand side, despite the spate of cyberattacks, some companies are buying less cyber insurance or not buying any at all.").

[224] *Id.* at 81.

[225] *Id.*

[226] *See Cyber Insurance: Risks and Trends 2020*, MUNICH RE (Apr. 14, 2020), https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2020.html.

[227] *See* GUY CARPENTER, *supra* note 4, at 6 (noting that the effect of NotPetya was "muted due to many of the compromised businesses being underinsured or not purchasing a cyber insurance product").

[228] *See* Maynard & Ng, *supra* note 134, at 48.

[229] *See* Kesan & Hayes, *supra* note 95, at 194 ("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 measures."); Talesh, *supra* note 18, at 17 (exploring how cyber insurers influence and potentially enhance cybersecurity). On the use of insurance to promote effective private

cyber insurers to insist on meaningful changes to policyholders' cybersecurity precautions if they are only covering a small percentage of the risks that may flow from a cyberattack to that firm. Relatively low coverage limits also make it harder for cyber insurers to insist that firms collect their own data regarding cyber exposure as part of the underwriting process.[230] Additionally, the relatively small amount of capital that insurers have devoted to cyber insurance means that collective insurance industry investment in understanding, protecting against, and informing others about cybersecurity is correspondingly limited.[231]

The flip side of the coin is that policyholders may have a stronger incentive to improve their cybersecurity if they cannot purchase sufficient cyber insurance. But cybersecurity is one arena in which the potential for insurers to reduce risk by acting as "private regulators" would seem to be significant.[232] Developing effective cybersecurity systems is both technically complex and resource intensive. Cyber insurers have strong market incentives to understand these cyber-defense systems, whereas cybersecurity is simply one among numerous challenges that policyholders face, and certainly not a profit-driver for most firms. Consequently, policyholders often do not have extensive knowledge of how to develop, implement, and maintain systems for promoting effective cybersecurity.

Cyber insurers are thus caught in a difficult bind. Continuing use of strong limits management means leaving short-term profits on the table while ignoring increasing demand for coverage, both of which limit the industry's capacity to improve cybersecurity. But relaxing limits management undermines the most effective bulwark the industry has against the risk of catastrophic losses, a result that could imperil cyber insurers' solvency in the future.

IV. POTENTIAL SOLUTIONS

The catastrophic cyber risk that exists for both traditional and cyber insurance policies identified in Parts II and III can be addressed in a number of ways. Some of

---

regulation more generally*, see* Shauhin Talesh, *Legal Intermediaries: How Insurance Companies Construct the Meaning of Compliance with Antidiscrimination Laws*, 37 L. & POL'Y 209 (2015); Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012).

[230] *See, e.g.*, Nurse et al., *supra* note 195, at 4 (explaining that cyber insurers can only collect limited information in underwriting when they are issuing policies for smaller firms, which require lower limits).

[231] *See* U.S. CYBERSPACE SOLARIUM COMM., *supra* note 222, at 81.

[232] *See* Talesh, *supra* note 18. *See generally* Ben-Shahar & Logue, *supra* note 229; John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539 (2017).

these measures have the potential not only to limit catastrophic risk for insurers, but to promote cyber insurance markets more generally, which can potentially produce additional benefits, such as improved cybersecurity. The first is more substantial reinsurance of cyber risks. The second is development of more robust capital market mechanisms for providing long-term financial backup of cyber insurance exposures. And the third is a government-funded backup, either in the form of a lender-of-last-resort or as a reinsurer. Each of these three approaches has its strengths and weaknesses.

A. MORE SUBSTANTIAL REINSURANCE

To date, reinsurance has played a major role in the development of cyber insurance markets.[233] There are various reasons that reinsurance has proven to be so vital to the industry's growth, including reinsurers' capacity to aggregate data from multiple insurers and employ their financial capacity to hire experts in cybersecurity who can help reliably model cyber risk. But from the perspective of "ceding insurers"—the primary and excess insurers that purchase reinsurance—reinsurance has proven so vital because it helps them to mitigate their risk of facing catastrophic losses that could wipe out their capital.

Consequently, more robust availability of cyber reinsurance could help promote growth in cyber insurance markets more generally. At present, one of the principal limitations on cyber reinsurance availability is that it is primarily offered through quota-share treaties, wherein insurers cede a specified percentage of their risk to the reinsurer.[234] By contrast, excess-of-loss reinsurance, which covers the ceding insurer for claims beyond a specified limit, appears to be less frequently employed in cyber-specific treaties.[235] Much like cyber insurers' own use of limits management, reinsurers' preference for quota-share coverage limits the extent to which they take on the prospect of catastrophic cyber risk.

Reinsurers' apparent unwillingness to take on a relatively large share of cyber catastrophe risk through excess-of-loss reinsurance forces cyber insurers to adopt techniques like limits management to reduce their own cyber catastrophe exposure. If reinsurers were willing to offer excess-of-loss coverage on reasonable terms, this would greatly expand the capacity of cyber insurers to offer coverage, since they could then more effectively diversify their own cyber catastrophe risk through

---

[233] *See* Anthony Cordonnier, *Could Cyber Risk be a Growth Engine For Reinsurance?*, SWISS RE (Aug. 30, 2019), https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/cyber-reinsurance/reinsurance-a-growth-engine-for-cyber.html.

[234] *Id.*

[235] *Id.*

reinsurance. Reinsurers could then further spread this risk through retrocession and the purchase of cyber-linked catastrophe bonds.[236]

Reinsurance could also help limit the risk posed by silent cyber coverage of the type we focused on in Part II. There is no public data at a level of detail that would enable us to determine how much reinsurance property/casualty insurers have purchased to protect themselves against silent cyber risk. It seems likely that, to the extent that insurers issuing traditional property/casualty coverage have underestimated their exposure to this risk, then so too have reinsurers. However, reinsurers' coverage of catastrophic cyberattacks producing physical damage or loss would depend on the structure of the underlying reinsurance agreements. Reinsurers that have entered into treaty arrangements with ceding insurers are much more likely to be exposed to this risk than those with facultative reinsurance arrangements.[237] This is because the automatic risk transfer that results from treaty arrangements will typically include any under-appreciated silent cyber risk, unless the treaty contains a specific cyber exclusion that is absent from the primary policies. By contrast, the very nature of facultative reinsurance arrangements requires insurers to identify and affirmatively decide to cede specific risks to a reinsurer. Irrespective of whether insurers or reinsurers currently bear the bulk of catastrophic silent cyber risk that can result in physical damage, it would be sensible for these entities to spread this risk more broadly into the global reinsurance and retrocession markets than they may be doing at present.

We can offer no "legal" solution to these problems; they are not amenable to any realistic legally mandated solution involving only the private market. Increased understanding of the risks involved may induce both insurers and reinsurers to offer more coverage, but that is an evolutionary process. The solution to the problem is time—the time necessary for adequate information to emerge and be of use. Whether there will be enough time for adequate insurance and reinsurance to develop before a catastrophic cyberattack occurs is therefore the critical, and unanswerable, question.

B. MORE ROBUST CAPITAL MARKET MECHANISMS

---

[236] *See* Christopher C. French, *Five Approaches to Insuring Cyber Risk*, 81 MD. L. REV. (forthcoming, 2021) (discussing the potential for catastrophe bonds to help spread the risk of a major cyber insurance attack).

[237] In treaty reinsurance agreements, insured risks that meet pre-specified criteria are automatically ceded to the reinsurer. ABRAHAM & SCHWARCZ, *supra* note 23, at 771–72. By contrast, facultative arrangements transfer specific risks that are likely to lead to large exposures.

We demonstrated in Part I that one of the principal obstacles to insuring against catastrophic loss is correlated risk, and that the central difficulty in insuring correlated risk is access to capital. Insuring against catastrophic loss —low-probability, high-severity loss—risks exposure to substantial claims before the insurer has collected sufficient premiums to pay these claims. In effect, insurers need access to loans or other forms of credit that will enable them to engage in the intertemporal risk spreading necessary to insure against catastrophic loss.

There are a variety of financial instruments that can provide the necessary capital. The paradigm instrument that has been used in practice to protect against catastrophic risk is a catastrophe bond, which is typically issued by a special purpose vehicle created by an insurer or reinsurer.[238] The bond pays a substantial rate of interest to the purchaser, but the debt obligation it represents is forgiven in part or in whole if a specified event of defined magnitude—a hurricane of sufficient magnitude when it strikes the U.S. coast, for example—materializes.[239] The triggering event may require proof of loss by the debtor (thus constituting an indemnity catastrophe bond), or it might simply be defined as an event that proxies for the occurrence of high-severity losses (thus constituting a parametric catastrophe bond).[240] Forgiveness of the debt enables the insurer to pay claims.[241]

To date, a small number of cyber-linked catastrophe bonds have been issued, though the market for these types of capital market instruments remains quite small.[242] Several factors contribute to this phenomenon.[243] Perhaps the most important is that unlike traditional catastrophe bonds, the triggering event for a cyber catastrophe bond has a strong potential to be correlated with more general financial

---

[238] *See* Steven L. Schwarcz, *Insuring the 'Uninsurable': Catastrophe Bonds, Pandemics, and Risk Securitization*, 99 WASH. U. L. REV. (forthcoming, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3712534.

[239] *See id.*

[240] *See* Michael Edesess, *Catastrophe Bonds: An Important New Financial Instrument,* ALT. INV. ANALYSIS REV., Q4 2015, at 6–7.

[241] *See generally* Schwarcz, *supra* note 238.

[242] *See* Syed Salman Shah & Ben Dyson, *Cyber Insurance-Linked Securities Have Arrived, But Market Still in Infancy*, S&P GLOB. MKT. INTEL. (Oct. 12, 2018), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurance-linked-securities-have-arrived-but-market-still-in-infancy-46915334; Hofmann & Wilson, *supra* note 134, at 9.

[243] Another relevant factor for indemnity-based cat bonds is the fact that traditional catastrophes do not result in liabilities that take time to assess and pay, whereas many cyber risks include liability and business interruption, which can take a longer time to settle. *See* Shah & Dyson*, supra* note 242.

instability.[244] Indeed, the possibility that a catastrophic cyberattack could trigger financial instability has become increasingly recognized in recent years.[245] Yet one of the primary selling points of traditional catastrophe bonds has long been that the risk of a natural catastrophe occurring is largely uncorrelated with financial market risks.[246] A more general difficulty with this solution for cyber insurance is that it relies on the same capital markets that have thus far shown only limited interest in financing insurers' other catastrophic exposures. Annual catastrophe bond expenditures are around only $10 billion, with roughly $28 billion in catastrophe bond capital outstanding.[247]

Another possibility is that alternative forms of protection against catastrophic cyber risk will become more available to insurers and reinsurers in the form of exchange-traded derivatives. These are standardized contracts whose payouts can be based on the occurrence of a future event, such as a catastrophic cyberattack.[248] They are listed and traded through exchanges such as the Chicago Board Options Exchange (CBOE) and the New York Mercantile Exchange (NYMEX), and cleared and settled by central counterparties such as CME Clearing Services and ICE Clear.[249] Like catastrophe bonds, such cybersecurity derivatives could in theory allow insurers to hedge the risk of a large payout on their insurance policies through capital markets.[250] Moreover, the instruments would offer the advantage to investors

---

[244] *Id.*

[245] *See, e.g.*, Jeremy C. Kress, Patricia A. McCoy, & Daniel Schwarcz, *Regulating Entities and Activities: Complementary Approaches to Nonbank Systemic Risk*, 92 S. CAL. L. REV. 1455, 1517–18 (2019); *Cybersecurity and Financial Stability: Risks and Resilience*, OFF. FIN. RESEARCH 1, 7–10 (Feb. 15, 2017), https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf; EUR. SYS. RISK BD., SYSTEMIC CYBER RISK 2–4 (Feb. 2020), https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9.

[246] *See* French, *supra* note 236 (discussing the potential for catastrophe bonds to help spread the risk of a major cyber insurance attack).

[247] *See Facts + Statistics: Catastrophe Bonds and Other Insurance-Linked Securities*, INS. INFO. INST. https://www.iii.org/fact-statistic/facts-statistics-catastrophe-bonds (last visited Mar. 26, 2021).

[248] Micah Schwalb, *Exploit Derivatives & National Security*, 9 YALE J. L. & TECH. 162 (2007).

[249] *See* Steven L. Schwarcz, *Regulating Derivatives: A Fundamental Rethinking*, 70 DUKE L.J. 545 (2020).

[250] For an early discussion of using derivatives to transfer cyber risk, *see* Schwalb, *supra* note 248. For a theoretical analysis of how derivatives can be structured to help hedge cyber-

looking to offer this protection of limiting the extent to which they would need to temporarily tie up substantial amounts of capital. But unlike cyber catastrophe bonds, exchange-traded cyber derivatives are not yet a reality, even though Over-The-Counter cyber derivatives (which are customized between two parties and not traded through an exchange) are not unheard of.[251]

The hypothetical nature of exchange-traded derivatives that can be used to hedge catastrophic cyber risk is likely linked to the difficulty of objectively determining when pre-specified conditions related to cybersecurity, like a catastrophic cyberattack, have occurred. But some recent developments, like new and more reliable measures of total insured losses arising from cyber events, can potentially support the development of robust derivatives markets for cyber risk.[252] Indeed, some industry insiders have even suggested the potential for developing financial instruments that can hedge silent cyber risk specifically by conditioning payout on the total amount of silent-cyber insurance payouts in a given year.[253]

As with the notion that greater involvement of reinsurance and retrocession markets could facilitate insurance against catastrophic cyber loss, there is no purely legal solution that will produce more robust capital market involvement in the insurance of catastrophic loss. More favorable tax and regulatory treatment might encourage such involvement, but of course that is true of almost any financial instrument for which there is a lethargic market. The question is which financial instrument is to be favored at the expense of others.

C. GOVERNMENT-FUNDED BACKUP

The third approach involves the federal government providing a backstop to the insurance industry against the risk of a catastrophic cyberattack, either in the form of a lender of last resort or by providing reinsurance. This strategy has already been attempted by one country, Singapore, which launched the first government-funded

---

risk, *see* Pankaj Pandey & Einar Snekkenes, *Using Financial Instruments to Transfer the Information Security Risks*, 8 FUTURE INTERNET 20 (2016).

[251] Some insurers and reinsurers may already seek to hedge cyber risk by purchasing Over the Counter Derivatives, which are customized between two parties. Indeed, the Solarium Report indicates that some insurers enter into derivative contracts with reinsurers. *See* U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 222, at 81.

[252] Hofmann & Wilson, *supra* note 134, at 10, 20.

[253] *See* Steve Evans*, ILS / ILW Retro Needed for Non-Affirmative Cyber: Johansmeyer, PCS*, ARTEMIS (June 26, 2020) https://www.artemis.bm/news/ils-ilw-retro-needed-for-non-affirmative-cyber-johansmeyer-pcs/.

cyber risk pool in 2018.[254]

1. Government as Lender of Last Resort

One form of government backup for cyber insurance markets is simply a version of more robust capital markets, designed to provide public capital when the private markets are not available to afford an insurer liquidity if it suffers a catastrophic cyber loss. This approach only makes sense if there is merely a temporary liquidity problem – that is, if there is reason to believe that the capital markets would supply necessary capital over the long term, but not in the short term.

Although public programs designed to facilitate insurance markets are not generally structured this way, using the government as a lender of last resort is extremely familiar in the banking context.[255] Indeed, one of the central roles of the Federal Reserve system is to provide banks with protection against liquidity risk by allowing them to borrow freely from the Fed's Discount Window.[256] To ensure that such borrowing is truly used as intended, Discount Window lending is generally offered only to solvent banks, at relatively high-rates, and against good collateral.[257]

At least part of the reason for the comparatively meager capital market involvement in catastrophe insurance may be uncertainty about the precise likelihood of a low-probability, high-severity loss. This is obviously an *ex ante* problem—insurers have no assurance *ex ante* that they will have access to capital *ex post*. This uncertainty may be part of what inhibits their willingness to cover catastrophic cyber loss. The main function of a government-as-lender-of-last-resort program would be to assure insurers that capital would be availability *ex post* so as to encourage them to insure catastrophic risk *ex ante*. In actuality, however, the program might or might not have to be called upon in the event of a catastrophic cyber loss, depending on the rapidity of the capital market's response *ex post.*

But of course, the government might be left holding the bag if the capital markets did not respond with long-term loans, and insurers were unable to pay off their government loans. The economic effect of such a development would be to

---

[254] *See* Steve Evans, *Singapore Launches First Commercial Cyber Risk Pool*, REINSURANCE NEWS (Oct. 29, 2018), https://www.reinsurancene.ws/singapore-launches-first-commercial-cyber-risk-pool/.

[255] *See* Dwight Jaffee & Thomas Russell, *Financing Catastrophe Insurance*: *A New Proposal*, *in* RISKING HOUSE AND HOME: DISASTERS, CITIES, PUBLIC POLICY 43–45 (John M. Quigley & Larry A. Rosenthal eds., 2008).

[256] *See* 12 U.S.C. § 347b(b)(1).

[257] *See* WALTER BAGEHOT, LOMBARD STREET: A DESCRIPTION OF THE MONEY MARKET (1877).

place the government in the position of being something like a reinsurer. It may be possible, however, to limit this risk by leveraging some of the government's experience operating as a lender of last resort to banks. For instance, to the extent that the government did make a loan to an insurer in the wake of a catastrophe, it would be sensible for it to take the insurer's assets as collateral. This could include not just the insurer's financial assets (as in banking), but also the intangible value associated with its policyholder relationships. Including the funds derived from these relationships as part of the government's collateral would reflect the fact that it would be continued payment of premiums from these ongoing relationships that the insurer (and government) would ultimately expect to pay off the loss arising from a catastrophe that occurred relatively early in the collection of premiums for that exposure.[258]

2. Government as Reinsurer

A second approach to government backup against cyber catastrophe risk—federal reinsurance—is one for which there is a strong precedent. Most notably, the Terrorism Risk Insurance Act (TRIA) was adopted to encourage insurers to offer coverage for the consequences of terrorism after 9/11.[259] The event triggering reinsurance under the Act is an attack certified as terrorism by several combined federal agencies, involving (as of 2020) more than $200 million in insured losses.[260] In 2016, the U.S. Treasury Department confirmed that acts of cyber terrorism are within the Act's purview.[261] When TRIA's trigger is met, insurers in eligible lines (which include cyber insurance) are eligible to recoup reinsurance for 80 percent of their claim payments beyond their deductible, which amounts to 20 percent of the insurer's previous year's direct earned premiums in TRIA-eligible lines.[262] Aggregate government and private insurer payouts for insured losses are capped at $100 billion annually.[263] Insurers do not pay any upfront premiums for this

[258] *See* Part I, *supra*.

[259] *See* Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002). The Act was originally scheduled to sunset in 2005, but it has subsequently been extended multiple times, most recently in 2019. Terrorism Risk Insurance Program Reauthorization Act of 2019, Pub. L. No. 116-94 (2019).

[260] GOV'T ACCOUNTABILITY OFF., TERRORISM RISK INSURANCE: MARKET IS STABLE BUT TREASURY COULD STRENGTHEN COMMUNICATIONS ABOUT ITS PROCESSES 5 (Apr. 20, 2020), https://www.gao.gov/products/GAO-20-364.

[261] Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 Fed. Reg. 95312 (Dec. 27, 2016).

[262] *See* GAO REPORT, *supra* note 260, at 5.

[263] *Id.* at 5–6.

protection, but the government is required to recoup *ex post* some of its payouts from insurers.[264] When its reinsurance and recoupment provisions are combined, TRIA looks very much like a somewhat long-term loan program, designed to encourage insurers to cover the consequences of terrorism. Insurers have done exactly that; and TRIA itself has never required the federal government to pay losses.[265]

Although TRIA already provides reinsurance for an act of cyber terrorism, this coverage is limited and the scope of its applicability to cyber terrorism is unclear. The former point is relatively straight-forward: most cyberattacks do not constitute terrorism under any plausible definition of that term. And while catastrophic cyberattacks are more likely to constitute terrorism than are non-catastrophic attacks, the protection against catastrophic cyber risk afforded by TRIA is nonetheless clearly limited, particularly since Acts of War were excluded from the definition of terrorism in the 2015 reauthorization of the Act.[266] The lack of clarity regarding TRIA's reinsurance of cyber terrorism stems from the fact that the Act's definition of terrorism—which requires an act to "have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States government by coercion"—was not crafted with cyberattacks in mind.[267]

Expanding federal reinsurance to apply to all cyber catastrophes, rather than just those that meet the definition of terrorism, would resolve these problems while increasing the capacity of cyber insurance markets. At the same time, such a change would create considerable difficulties. In particular, it would require a mechanism for quickly determining whether such an attack produced losses of a significant magnitude to qualify as catastrophic. Because at least some lines of cyber insurance involve long-tails of coverage, including business interruption and liability coverage, simple quantitative annual thresholds might not be easy to operationalize.

Nor is it clear that there is sufficient political will to invest in the creation of a new federal cyber catastrophe reinsurance program. The attacks on 9/11 provoked a sympathetic response from the nation. A number of special government programs—most notably the 9/11 Compensation Fund—were adopted on the crest of that sympathy. TRIA was another such program.

In the years that followed, however, the justification for adopting these special programs has been called into question. Why had we not adopted a compensation fund for the victims of the Oklahoma City bombing? Why do certain emergencies

---

[264] *Id.* at 4.

[265] *See id.* at 4.

[266] Terrorism Risk Insurance Program Reauthorization Act of 2015, Pub. L. No.114-1, 129 Stat. 3.

[267] *See* GAO REPORT, *supra* note 260.

produce loan programs rather than grants? The administrator of the 9/11 Compensation Fund himself, Kenneth Feinberg, expressed the view that nothing like the Fund would ever be adopted again.[268]

These developments suggest that proposals for government-backed lending or reinsurance are likely to be subject to the same considerations and skepticism. There are any number of potential risks for which the federal government could encourage insurance before they materialize in harm. What is special about cyberattacks, as opposed to other catastrophes, especially—in light of recent history—pandemics?[269] The argument for special treatment of hurricanes in Florida and earthquakes in California is plain. These are especially severe risks that are distinctive to those states. But cyber risk insurance is, arguably, no more deserving of special government encouragement than, say, pandemic risk.

Because it is difficult to know in advance which catastrophes are worthy of special treatment, governments typically wait until a disaster has occurred, assess its political, economic, and social consequences, and then determine what level and kind of support for the victims of the disaster is appropriate.[270] This produces somewhat inconsistent treatment over time, but so would enactment of some government reinsurance backup programs and not others. In short, whether to adopt government backup for cyber catastrophe insurance poses a basic problem of public policy that an analysis of insurance dynamics cannot itself resolve.

CONCLUSION

The risk of cyber loss is undeniable, and with that risk comes the lesser but real risk of highly-correlated and catastrophic cyber loss. Many traditional property/casualty insurance policies probably provide "silent" coverage of cyber risks that could result in physical loss or damage to property, including any consequential economic loss. Depending on the nature and scope of a cyberattack, general property/casualty insurance policies could thus be vulnerable to silent cyber coverage claims of catastrophic magnitude.

---

[268] *See* All Things Considered, *Lawyer Describes The Emotional Toll Of Calculating Victims' Compensation*, NPR, (Sept. 11, 2016), https://www.npr.org/2016/09/11/493526796/lawyer-describes-the-emotional-toll-of-calculating-victims-compensation.

[269] For instance, various proposed bills at the federal level would create a pandemic reinsurance program, though none have passed to date. *See, e.g.*, H.R.6983 – Pandemic Risk Insurance Act of 2020 (Introduced 05/22/2020)

[270] Faure V. Bruggeman et al., *The Government as Reinsurer of Catastrophe Risks?*, 35 GENEVA PAPERS ON RISK & INS. (ISSUES AND PRAC.) 369, 370 (2010).

Non-traditional, cyber insurance policies face a somewhat different challenge. Cyber insurers' efforts to limit their exposure to the risk of covering catastrophic loss has meant that the coverage they provide only partially meets the insurance needs of their actual and potential policyholders. And by virtue of the comparatively limited protection that cyber insurance provides, the insurers that provide it have limited ability to exercise strong influence over the risk-creating and risk-mitigating conduct of their policyholders.

In principle, the solution to these problems is supplying more capital to stand behind insurance against cyber risk, and especially catastrophic cyber risk, whether through more reinsurance, other forms of private capital, or government-crafted backup. But moving from principle to policy to implementation is easier to describe on paper than it is to achieve in practice. The first step, which we have tried to take in this Article, is to understand and appreciate the nature and scope of the problem.

A SEMANTIC FRAMEWORK FOR ANALYZING "SILENT CYBER"

KELLY B. CASTRIOTTA[1]

"New ideas must use old buildings."
Jane Jacobs, *The Life and Death of Great American Cities*

Insurers first developed property and casualty insurance policies prior to the internet, widespread computerization, the digital interconnectivity of electronic and mechanical devices, and the prolific use and transmission of electronic data. Many such insurance contracts did not expressly address cyber exposures at the time of their creation, leaving insurers and their customers to battle over contract interpretations for attritional cyber losses. In 2015, the Prudential Regulatory Authority (PRA) formally introduced a theoretical problem of "silent cyber" to the insurance industry, contemplating catastrophic cyber scenarios with not only a potentially powerful impact upon dedicated Cyber insurance portfolios, but also upon traditional insurance portfolios. The issue soon became a reality in the wake of the expansive insurance losses associated with the NotPetya attacks of 2017, as most insurable losses stemming from those attacks were ultimately recoverable under traditional insurance policies, as opposed to dedicated cyber insurance policies.

In response to the requests made by the PRA to insurers to put into action a plan to manage silent cyber, Lloyd's of London introduced a mandate to eliminate "silent cyber" on all Lloyds policies, charting a course for the transformation of insurers' contractual wording to more appropriately address cyber risk. This article discusses the general concerns around "silent cyber" as presented by the PRA, the challenges of defining cyber risk across the insurance industry, and steps taken to

---

[1] Kelly B. Castriotta, Esq, is Global Cyber Underwriting Executive at Markel Corporation (NYSE: MKL). The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of Markel Corporation or any of its subsidiaries or holdings. The information providing with this article does not and is not intended to constitute legal advice; instead, all content within is for general informational and academic research purposes only.

For helpful comments and suggestions, I thank attorneys-turned-insurance-gurus: Keith Bergin, David Finz, Joe Niemczyk, and Michael Rastigue. I also thank Daniel Schwarcz, Fredrikson & Byron Professor of Law, University of Minnesota Law School, for his contributions.

rectify the silent cyber issue. The article then explores the idea that the silent cyber problem is at its core a semantic one rather than one of risk perception. The article concludes by offering solutions as to a semantic framework under which to analyze and address "silent cyber."

TABLE OF CONTENTS

I. INTRODUCTION

Historic buildings are worth preserving not only because of their cultural significance, but because of the potential source of revenue from these attractions.[2] In many cases, it may make economic sense to rebuild certain architectural structures in the face of new environmental threats or newfound recognition of the ways that existing threats impact aging structures.[3] However, there are alternatives to a destroy

[2] *See* Zvonko Sigmund, Vedran Ivanokovic, & Alan Braun, *A Challenge of Retrofitting a Historical Building*, 2nd WTA International PHD Symposium Building Materials and Building Technology to Preserve the Built Heritage, at 1 (2011).

[3] *See* Tony Hutchinson, *Retrofitting is Expensive—Let's Demolish and Start Again,* THE GUARDIAN (Apr. 3, 2012), https://www.theguardian.com/housing-network/2012/apr/03/retrofit-expensive-demolish-unfit-homes.

and rebuild approach, one of which is retrofitting older buildings with new materials or design features.[4] Seismic retrofitting, for example, is the act of performing fengineering treatments such as preservation, rehabilitation, restoration and reconstruction, to improve a historic building's ability to withstand earthquakes.[5] The earthquake was once an underestimated threat to some buildings but with appropriate retrofitting, contemporary architects can maintain older buildings by implementing and layering emerging design technologies upon older ones, thereby maintaining the integrity of cultural structures.[6]

We can look at the issue of "silent cyber"[7] in a similar light. The insurance industry[8] has developed and maintained a prolific body of contractual architecture (policies) that has created a legacy of meaningful risk transfer products for customers. Among those products is the relatively emergent Cyber insurance policy, specifically designed to cover certain aspects of so-called "cyber risk." Taken as a whole, the insurance industry has historically paid losses associated with their insurance products and remained profitable.[9] As does happen occasionally in the architectural community, the insurance industry encounters emerging appreciation of the catastrophic[10] reach of specific threats. In recent years, one such concern is

---

[4] *See* Sigmund, *supra* note 2 at 2.

[5] *See id.* at 2.

[6] *See id*.

[7] When used as a noun, the term "silent cyber" will appear in quotations, but when used as an adjective, the phrase will appear without quotations.

[8] The phrase "insurance industry" when used throughout this article is to be construed broadly to include businesses that partake in the underwriting and procurement of insurance or reinsurance products, including by not limited to insurance companies, reinsurance companies, brokerage firms, agents of insurance, insurtech companies, and managing general underwriters.

[9] For a quick snapshot of 2020 profitability, *see, Visualizing the 50 Most Profitable Insurance Companies in the U.S.* (Aug. 10, 2020), https://howmuch.net/articles/top-50-most-profitable-us-insurance-companies-2020. For a historic view, *see,* James Lynch, *The Property/Casualty Landscape Profitability, Growth – Disruption?* (Sept. 26, 2016), https://www.iii.org/sites/default/files/docs/pdf/case-092616.pdf. For a forward-looking view, *see* Gary Shaw and Neal Baumann, *2021 Insurance Outlook: Accelerating Recovery from the Pandemic While Pivoting to Thrive* (Dec. 3, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/insurance-industry-outlook.html.

[10] When this article refers to "catastrophic" losses, this is generally intended to mean the same as correlated losses, systemic losses, or accumulated losses—all losses other than

the wide reach of cyber risk[11] and with it, fears as to whether the insurance industry will be able to withstand an event like a malware attack on the United States' power grid.[12] Compounding this fear is a recognition that perhaps "silent" cyber exposure will extend beyond the realm of monoline Cyber[13] insurance portfolios and threaten the sustainability of traditional[14] lines of insurance coverage. Specifically, the industry is concerned over risks that it failed to consider, and adequately price for cyber losses (attritional[15] or otherwise).

As such, the industry has a vast set of traditional risk transfer products not specifically engineered to withstand such cyber risk alongside an emerging set of contemporary risk transfer products (and in some cases, services) that have been intentionally created to addresses cyber risk. This article proposes that one[16] solution to the concerns regarding silent cyber is to "retrofit" traditional insurance products with language and other normative concepts borrowed from standalone Cyber products.

---

attritional losses. *See infra* at 15. I am aware that many contemporary modelers of cyber events distinguish between correlated events and systemic events; those distinctions are not entirely relevant to the discussion herein, so I will not address those in detail.

[11] *See Swiss Re highlights role of re/insurance in cyber risk,* REINSURANCE NEWS (Mar. 6, 2017), https://www.reinsurancene.ws/swiss-re-highlights-role-reinsurance-cyber-risk/.

[12] *See* TREVOR MAYNARD, ET. AL., LLOYD'S EMERGING RISK REPORT—2015, INNOVATION SERIES: THE INSURANCE IMPLICATIONS OF A CYBER ATTACK ON THE US POWER GRID. CENTRE FOR RISK STUDIES, UNIVERSITY OF CAMBRIDGE JUDGE BUSINESS SCHOOL (2015), https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloyds-business-blackout-scenario/.

[13] Herein when I refer to cyber-specific insurance policies, I will use a capitalized version of the word "Cyber." When I refer to cyber-as-a-peril (or hazard), I will utilize a lower-case version, "cyber."

[14] Generally in referring to "traditional lines" or "traditional property and casualty" insurance policies, I refer to the broad array of products to cover bodily injury, property damage, liability, and professional risk developed prior to 1990. Such policies responded to perils like fires, hurricanes, and tornadoes that did not necessarily implicate the prolific use of computers and computerized data as we know it today.

[15] What I mean by "attritional losses" are those losses other than losses associated with catastrophes. When I refer to expected losses, non-systemic losses, or non-catastrophic losses, I am referring to attritional loss.

[16] I do not maintain that this is the only solution. In fact, I am aware of a destroy-and-rebuild type of thinking within the insurance industry that suggests the Cyber product as well as traditional insurance products should be rebuilt bottom up; however, I am saying short of paradigmatic change on this level, there is a retrofitting solution available to us at this time.

Underpinning the thesis of this article is the observation that rather than simplifying the issue of "silent cyber" as a matter of risk perception (i.e., differing views over cyber risk in general), an insurer should view the problem as a foundationally semantic one. Namely, there is currently a lack of a collective semantic understanding across silos[17] within firms and across the insurance industry, creating ambiguity around how cyber risk may impact insurance portfolios. Specifically, there is a lack of a collective understanding as to what is intended by the following concepts: computer systems, data, cyber, cyber risk, cyber loss, silent cyber, and non-affirmative cyber.

In light of the foregoing, a prerequisite to solving the problem of "silent cyber" is the adoption of a consistent semantic framework to be implemented across an insurance firm enterprise. This approach will ultimately lead to better evaluation and quantification of cyber exposure within any specific firm's insurance portfolio and across the industry. The framework should be flexible enough to adapt to the evolution of the Cyber insurance product being sold in the marketplace today and in the future. In turn, this article will offer a definition of "silent cyber" that can be used to determine what should and should not be covered by non-Cyber policies. Such semantic framework focuses on the "nesting"[18] of Cyber and non-cyber policies, and emphasizes that losses that are covered by Cyber policies should not be covered by non-Cyber, and vice versa (unless done so with appropriate pricing and/or attention to overlapping coverage). Just as auto and homeowners policies "nest" together by covering mutually exclusive risks, the same should be true of Cyber and non-Cyber policies. To accomplish this, non-Cyber policies should continue to cover losses where cyber-as-a-peril is involved in the causal chain of a loss and there is a distinct

[17] There are several types of common "silos" that may be found in any one insurance firm, but the one I point to here is product-based. Insurance firms typically embrace organizational structures based on product lines (a.k.a. "Lines of Business"), broadly stated as follows: Professional Lines, Property Lines, and Casualty Lines. The Cyber product as a coverage traditionally falls within the organizational umbrella of Professional Lines, as it is a product offering coverage for financial losses with its origins in Technology Errors and Omissions coverage (responding to negligence claims for the implementation and functionality of technology as provided by software and other similar companies). *See infra* 22. Additionally, a Cyber product may also be packaged as an add-on to traditional coverage lines. As such, the inherent complexity of understanding, measuring, and correcting "silent cyber" within a single insurance firm stems from the fact that that cyber-as-a-peril is present across all product lines; and Cyber-as-a-product is organizationally housed in Professional Lines, but may also be sold as an add-on with other product lines.

[18] In this context, the "nesting" of sets of insurance policies refers to policies that, as a rule, compliment each other, by covering specific aspects of a risk, but not the same aspects of a risk.

physical alteration to the structure of tangible property. By contrast, traditional policies should not cover any losses that are in fact covered by current Cyber insurance policies.

The aforementioned assertions assume a general consensus that "silent cyber" is a massive risk for insurance firms and a problem that needs to be solved: 1) to defend the balance sheets of many insurance firms; and 2) to protect the current integrity of cyber insurance as a viable risk transfer vehicle.[19] These assumptions are supported by the research that the PRA[20] has conducted since 2015 on the issue of "silent cyber." The article ends with prescriptive view of how to view cyber risk: by embracing the Cyber insurance product framework that the industry readily has at its disposal. To reach this conclusion, this article will examine the current semantic frameworks offered (as set forth by the PRA and other regulatory bodies), the problems with having disparate frameworks for such, and offer potential solutions to be implemented on a firm-by-firm basis.

II. CYBER AS A COVERAGE

Given that Cyber coverage is new (relative to the history of traditional insurance products), a short history of the coverage offering will provide some context as to what earlier iterations of policies offered to customers and how that has changed, in a collective sense.[21] This lends support to the argument that, despite varieties of Cyber insurance forms in today's marketplace, there exists a base level expectation of Cyber coverage offering in the insurance industry, and that such offering at some level reflects a certain picture of what constitutes cyber risk and cyber loss from the perspectives of the insurer and the consumer.

---

[19] *See* Letter from Chris Moulder, Dir. of Gen. Ins., Bank of England, PRA, to CEO [of various insurers], at 1 (Nov. 14, 2016), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2016/cyber-underwriting-risk.pdf (stating "The PRA's work found an almost universal acknowledgement of the loss potential of cyber exposures endemic in 'silent cyber.'")

[20] *See generally What is the Prudential Regulation Authority (PRA)?*, https://www.bankofengland.co.uk/KnowledgeBank/what-is-the-prudential-regulation-authority-pra. The PRA is a regulatory body that is part of the Bank of England established after the financial crisis of 2007. *Id*.

[21] *See* Andrea Wells, *What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now.* INS. J. (Mar. 1, 2018). Many claim to have invented the first standalone cyber policy.

In the United States, dedicated Cyber insurance policies of the 1990s were policies that covered online media, while others were errors in data processing (EDP) policies.[22] The early prototypes of cyber liability insurance policies contained insuring agreements (or "coverage parts") which generally evolved from professional liability policies for software and media risks.[23] In the early 2000s, online media policies started to cover unauthorized access, network security, data loss, and computer worm or computer virus-related claims. When the 2003 California Security Breach and Information Act came into effect, this had a great impact upon cyber exposure and insurance. Companies and organizations conducting business in California now had to provide notifications to any affected residents of a personal data breach by an unauthorized party. As such, first party coverage was introduced to mitigate potential damages on the third-party liability side. But as privacy legislation proliferated,[24] the regulatory and first-party coverage continued to expand.

At first, Cyber risk insurance policies typically did not include both first-party and third-party coverage. It was not until the mid-2000s that these policies evolved in response to cyber threats to include some first-party coverages to protect an organization itself and its potential intellectual property.[25] Updated policies began to cover things like business interruption, cyber extortion, and system restoration costs. "Business interruption is almost like the prodigal son of the cyber insurance market…If you look right back to the 1990s / early 2000s when cyber insurance policies were first developed, there was no meaningful privacy legislation, even in the United States. At that point cyber insurance was all about business interruption. It was developed for the first breed dot-com companies, who were trading online and therefore had big exposure to system downtime."[26]At the same time, some

---

[22] Stephanie K. Jones, *Cyber Insurance: An Evolutionary Coverage*, INS. J. (Dec. 21, 2015), https://www.insurancejournal.com/magazines/mag-features/2015/12/21/391961.htm.

[23] *See id.*

[24] For a US State Privacy Law Map, *see* IAPP, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Map.pdf. Archived editions can also be found here: https://iapp.org/resources/article/state-comparison-table/.

[25] Notably, the intellectual property that was traditionally and is currently protected under Cyber policies is limited to those copyright and trademark infringement claims under a third-party media liability insuring agreement. *But see*, https://www.cloud-protection-plus.com/en.html (describing offering as of March 2020 which provides trade secret coverage under a sublimit).

[26] *See* Bethan Moorcraft, *The Evolution of Cyber Insurance—Where Are We Now?*, (Feb. 6, 2019), https://www.insurancebusinessmag.com/us/news/cyber/the-evolution-of-cyber-insurance--where-are-we-now-124183.aspx (quoting James Burns).

software-related policies also started to evolve, adding sub-limits for HIPAA liability-related software errors.

Today's cyber offerings are generally broken down into three conceptual coverage parts[27]: (1) third-party liability coverages; (2) first-party coverages; and (3) business interruption coverages (which are technically first-party coverages, but of a specific "time element" nature).[28] Each respond to a variety of cyber incidents, spanning from cyber attacks on one's own network, to system failures and other outages, to cyber attacks on a network provider's system. The third-party coverages are typically offered as follows: privacy and security liability, media liability, regulatory coverage, and Payment Card Industry (or "PCI") coverage. Depending upon the types of products and services offered by a potential insured, an additional third-party insuring agreement may also be offered to cover negligence with regard to technology developed or integrated by the insured for a third party. The first-party coverage includes incident response (including call center costs, credit monitoring, and related mitigation costs), cyber extortion, and restoration costs. The business interruption part typically includes coverage for the costs of interruption of business due to a cyber event, whether the event is perpetrated upon the policyholder itself or a business upon which a policyholder depends. This often includes the reputational costs associated with a cyber event. In recent years, another category of first-party coverage has become increasingly common in cyber policies, the purpose of which is to reimburse the insured for financial losses of a quasi-criminal nature, such as when an insured falls victim to social engineering[29] or invoice manipulation. The

[27] That said, the number and arrangement of insuring agreements in any single primary Cyber insurance policy may vary widely. The approach to multiple insuring agreements is non-standard as carriers try to accomplish one or more of the following: 1) limiting the universe of coverage triggers to specific losses (also known as "channeling" exposure); 2) containing deployment of policy limits for certain types of exposure by tying sublimits to certain insuring agreements; 3) providing flexibility to the customer to select and purchase coverage for certain insuring agreements; 4) providing commercial appeal by offering a greater "variety" of coverage agreements; or 5) providing clarity.

[28] For more examples of Cyber policy offerings, *see supra* Table 1.

[29] For a more detailed explanation of Social Engineering as a coverage, *see supra* Table 1. Note that "social engineering" is also understood as a type undesired reconnaissance and access that could be used to cause a loss that would trigger Cyber coverage, like extortion, privacy liability, and business interruption. Part of the challenge with Cyber insurance as a completely accurate reflection of the threat environment is that the Cyber product may conflate concepts like attacker, tactic, technique, procedure, vulnerability, exploit, cause of

coverages may vary by carrier or be labeled differently, but these are the main buckets of insuring agreements that a policyholder may find.

The coverages are a good place to find a common understanding of what the industry considers to be covered or potentially covered cyber loss. For example, third party liability coverages naturally respond to the legal costs and the damages (judgements, fines and penalties, or settlements) that arise from a cyber event. First-party coverages tell us in detail what cyber losses a business may suffer. For instance, an incident response insuring agreement tells us about the costs incurred to engage a host of service providers that are needed to respond when there is a security or privacy incident. These include breach counsel, privacy counsel, credit monitoring services for customers, forensic providers, and public relations firms. The extortion and restoration agreements provide coverage for ransomware payments made to cyber criminals and the costs of a cybersecurity firm to restore one's data (and in some cases, hardware). And finally, the business interruption coverages tell us that companies may undergo loss of income and even loss of contractual or other business opportunities due to a cyber event.

Note that the insuring agreements of a Cyber policy provides a normative view of what constitutes cyber loss, even though Cyber policies typically only extend to financial loss.[30] To achieve a more nuanced picture of what constitutes cyber loss, we could also look to the common exclusionary language in Cyber policies.[31] Although this article will not address common exclusions in detail, it is

---

loss, type of loss, and environment. Social Engineering coverage is one of those cases, where the coverage only contemplates a specific combination of those concepts.

[30] The distinction between "financial loss" and non-financial loss as commonly referred in insurance is such that financial loss is commonly referred to as pure economic loss that would be reflected as loss in a balance sheet only (as compared to the monetization of loss from a non-financial event, such as a bodily injury or property damage event).

[31] This article will not dig deeply into this topic as it is worth an independent study as to what are common exclusions on such policies, why are they there, and what do they mean as far as potential coverage gaps for cyber perils based on these exclusions. The focus is necessarily on the insuring agreements and definitions of the cyber insurance policy, rather than the exclusion as the insuring agreements give the broadest understanding of what is brought into the potential ambit of coverage under a Cyber policy. As a hard and fast rule, there is rarely bodily injury or property damage provided under Cyber policies. Based on this, it is important to note that as it is underwritten and priced, the underwriter of a Cyber policy would assume that the risk transfer for the bodily injury or property damage would fall uninsured to the policyholder or would otherwise be covered by the more specifically appropriate product, including commercial general liability or property policy (assuming clarity on the coverage available for ensuing loss stemming from cyber as a peril or other coverage grants for affirmative Cyber).

worth noting that typically bodily injury and property damage are excluded. Based on this, it is important to note that as it is underwritten and priced, the underwriter of a Cyber policy would assume that the risk transfer for bodily injury or property damage arising out of a cyber incident would fall uninsured to the policyholder or would otherwise be covered by a traditional insurance product, including commercial general liability or property policy, which generally responds to claims of bodily injury and/or property damage (assuming clarity on the coverage available for ensuing loss stemming from cyber-as-a-peril).

III. SILENT CYBER: FROM ABERRATION TO AGGREGATION

The next step is to elucidate the insurance industry concerns surrounding "silent cyber." The insurance industry has been formally discussing the issue of "silent cyber" since 2015, with most crediting the PRA as the initial regulatory catalyst for the movement towards eradicating "silent cyber" in insurance portfolios. In many ways, the silent cyber problem has existed well before the PRA formalized the issue, following a long history of attorneys and brokers offering advice as to where to find cyber coverage under traditional insurance policies.[32] For example, until around 2014,[33] commercial general liability policies rarely included concepts or language specific to cyber risk and even then, they were specifically focused on privacy exposures associated with computer hacking (as opposed to other security and business threats). Conflicts between insurers and policyholders developed over the applicability of coverage as they applied to emerging situations, such as whether

[32] *See* Richard Clarke, *Cyber Liability: Where to Find Cyber Coverage,* INS. J. (Jan. 28, 2013), https://www.insurancejournal.com/magazines/mag-coverstory/2013/01/28/278213.htm.

[33] In 2014, ISO introduced endorsements "addressing the access or disclosure of confidential or personal information":

> • CG 21 06 05 14 (Exclusion—Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability—With Bodily Injury Exception)—excludes coverage, under Coverages A and B, for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information . . . . [This exclusion also includes a limited bodily injury exception.]
>
> • CG 21 07 05 14 (Exclusion—Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability—Limited Bodily Injury Exception Not Included) . . . .

ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INS. J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

coverage existed for damage to data, and whether data was tangible property.[34] Other examples of such disputes include those where policyholders sought coverage under property policies because of power outage events (impacting computerized systems) under a theory of "loss of use or functionality," even where the outage did not amount to actual physical damage.[35] Much of the focus of these disputes focused on

[34] *See, e.g.*, West Bend Mutual Ins.Co. v. Krishna Schaumburg Tan, Inc., 2020 Ill. App. LEXIS 179, at 12 (Ill. Ct. App. Mar. 20, 2020) (holding that under a general liability policy, coverage part b, "publication" encompasses the act of providing plaintiffs fingerprint data to a third party, alleged to be in violation of the Biometric Information Privacy Act (Act) (740 ILCS 14/1 et seq. (West 2014)); Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 803 (8th Cir. 2010) (describing invasion of privacy and deceptive practices allegations from the installation of advertising tracking software on a non-consenting plaintiff, and finding "loss of use" of computer allegations fell within "tangible property" terms of general liability policy); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, at *3 (D. Ariz. Apr. 18, 2000) (describing how a power outage knocked out systems, causing loss of data and loss of software functionality, and the court found there was "property damage" per CGL terms); *see also* Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co., 115 A.3d 458, 460 (Conn. 2015) (describing how personal employment data stored on computer tapes for employees of IBM was lost in transit when the tapes fell out of the back of a van, causing IBM to pursue the transport carrier's CGL insurers, and concluding that IBM's losses were not covered by the personal injury clauses of the CGL policies because there had been no "publication" of the information stored on the tape). *Compare*, Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 97–99 (4th Cir. 2003) (finding that data, information, and instructions are not "tangible property," and that an "impaired property" exclusion precluded coverage for loss of use of tangible property that is not physically damaged), *with* Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141, at *67–72 (N.Y. Sup. Ct. Feb. 24, 2014) (describing how an insured sought coverage under CGL terms for alleged transmission of private information by hackers and finding no coverage).

[35] *See Am. Guarantee*, 2000 WL 726789, at *2 (describing an electrical outage, where an insurer said there was no "physical damage" pursuant to "all risks" policy language, yet finding that "physical damage" is not restricted to physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality); *see also*, National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Company, 2020 U.S. Dist. LEXIS 11411 (U.S.Dist. Ct., Maryland) (holding that loss/corruption of electronic data and software and reduced efficiency of computer systems due to a ransomware event amounted to direct physical damage under BOP policy)*; see also* NMS Servs., Inc. v. Hartford Ins. Co., 62 F. App'x 511, 514 (4th Cir. 2002) (describing property coverage with a computer and media endorsement, and finding that acts of destruction by employees did not preclude coverage). *But see* Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 114 Cal. App. 4th 548, 554–55 (Cal. Ct. App. 2003) (finding no coverage for costs of recovery of data or business interruption because there was no loss of, or damage to, tangible property).

underwriting and drafting intent (and more specifically as to whether there was an aberration from the intended cover). In other words, did the policy wording offer coverage for a cyber loss, even though the insurers did not price the policy to cover this type of risk? In this type of scenario, underwriters did not necessarily contemplate losses caused by cyber threats and, therefore, the definition of loss expanded beyond the intended scope of coverage.

The conversation about unexpected cyber losses began to morph after the PRA performed a cross-industry survey regarding cyber risk in 2015.[36] The initial PRA findings were grim, including the finding that the failure to account for cyber exposure in traditional insurance lines was material and likely to worsen with time.[37] The PRA also found that the industry was hamstrung from taking appropriate corrective action due to a lack of effective cyber exclusions, lack of clear strategy and risk appetite, and an insufficient grasp of aggregation and tail potential of affirmative cyber.[38] As the focus of the PRA findings revolved around potential catastrophic losses (rather than attritional losses), the conversation circles about "silent cyber" broadened from the plaintiff's bar to C-suite of insurance companies.[39]

A secondary catalyst for this broader conversation was the series of cyberattacks in 2017, known as NotPetya,[40] which amounted to more than $10

---

[36] *See* Letter from Chris Moulder, Dir. of Gen. Ins., Bank of England, PRA, (Aug. 10, 2015), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2015/cyber-resilience-questionnaire-for-insurers.pdf?la=en&hash=714C33604FA7A88C1C622C38ABA2F38C8A0ACF9Ff (including questionnaires as to cybersecurity and resilience, cyber insurance and conduct).

[37] *See* Moulder, 2016 Letter, *supra* note 19 at 1.

[38] *See id*. at 1–2.

[39] *See* Consultation Paper CP39/16, *Cyber insurance underwriting risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY (Nov. 2016) at 5, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916 (noting that the responses to its investigation were made by the following roles within insurance firms: Chief Underwriting Officer, Chief Risk Officer, Chief Actuary, Lead Cyber Underwriter, and Head of Exposure Management).

[40] *See 'Petya' Ransomware Outbreak Goes Global*, KREBS ON SECURITY (June 27, 2017), https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/.

billion in losses.[41] As the loss picture of the NotPetya[42] attacks sharpened in 2019,[43] the concerns shifted from attritional losses (usually due to aberrations in coverage) to mountainous aggregation[44] issues (usually due to catastrophic events). Aggregation concerns arise when multiple policies or multiple lines of coverage offered to an insured (either by design or inadvertently) are triggered from a single event, and as such, there is an accumulation of loss across product lines underwritten by any one insurer. "Silent cyber" poses a particular aggregation challenge to insurers because monoline Cyber policies are often the only policies underwritten to cyber risk. As aggregation concerns relate to "silent cyber," the underwriters underestimate the accumulation of cyber risk within a product line or for a specific insured across multiple product lines due to the possibility that traditional policies

---

[41] *See generally* Kenneth Abraham and Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe,* CONN. INS. L. J. (forthcoming 2021) (discussing the prospect of cyber incidents having the potential to simultaneously cause very large losses to numerous firms across the globe, thus resulting in a cyber "catastrophe"); *see The Problem of Silent Cyber Risk Accumulation,* https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation (February 25, 2020). *See also* Mondelez v. Zurich, No. 2018L011008, 2018 WL 4941760 (Ill.Cir.Ct) (subject litigation filed by Mondelez).

The corresponding statement of claim for USD 100 million was filed in October 2018 with the Circuit Court of Cook County, Illinois. The company, Mondelez International Inc. (Mondelez), had purchased an all-risk property insurance policy from Zurich American Insurance Company (Zurich) that included coverage for physical loss or damage to electronic data, programs or software and also physical loss or damage caused by the malicious introduction of a machine code or instruction. In June 2017, Mondelez is alleged to have fallen victim to an attack by the malware program 'NotPetya'. As a result, 1700 servers and 24,000 laptops at Mondelez were permanently damaged and had to be replaced. According to Mondelez, this caused damages of well over USD 100 million for the company. This loss was reported to Zurich by the company. In June 2018, Zurich refused to cover Mondelez, citing the insurance policy's war exclusion clause. To date, it appears that no final decision has been made in this lawsuit.

[42] *See* Tom Johansmeyer, *Could NotPetya's Tail Be Growing?,* at 1 (2019), https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf (referring to a PCS study that NotPetya's economic losses were estimated at $10bn by 2017)

[43] *See* Conan Ward, *Cyber Turned Inside-Out: Three Years After NotPetya,* CARRIER MANAGEMENT (June 17, 2020), *https://www.carriermanagement.com/features/2020/06/17/207958.htm* (estimating $10bn in losses associated with NotPetya, but with estimated $3bn in insurable losses from policies other than cyber dedicated lines).

[44] The term "aggregation" is used synonymously with the term "accumulation" throughout this article.

may unexpectedly respond to cover such losses. A large scale, or geographically boundless cyberattack could impact multiple insureds and multiple policies, both traditional and cyber specific.

IV. PERCEPTION OF CYBER RISK

As a result of its findings, the PRA suggested that insurance carriers begin to better address "silent cyber" in their respective portfolios.[45] The findings were based on a series of meetings and publications among the PRA and a select group of insurance carriers. The PRA issued several letters, Supervisory Statements, and Policy Statements leading up to its conclusion, but the critical points will serve as the basis for this section of the article and the groundwork for the analysis of the semantic structures around the topic of "silent cyber."

First, following a series of surveys to an array of insurers and reinsurers, the PRA again stated that most[46] surveyed insurance firms agreed that several traditional lines of business have considerable exposure to non-affirmative cyber risk.[47] The PRA reported that on certain product lines, however, insurance firms estimated their exposure to non-affirmative[48] cyber risk on certain lines to be anywhere from nothing to full limits. A wide divergence of opinions within the insurance industry as to whether a portfolio is either completely exposed to a catastrophic cyber event or completely immune to the same event suggests that something is amiss. Crudely put, if an entire portfolio is exposed to the same cyber event, the law of large

---

[45] *See* Letter from Anna Sweeney, Director, Insurance Supervision, Bank of England, Prudential Regulation Authority to CEO (Jan. 30, 2019), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results. The letter was a follow up to a Supervisory Statement by the PRA. *See* Supervisory Statement SS4/17, *Cyber insurance underwriting risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY (July 2017), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf?la=en&hash=6F09201D54FFE5D90F3F68C0BF19C368E251AD93.

[46] The PRA reported that it received thirteen responses to the CP. *See* Policy Statement PS15/17, *Cyber insurance underwriting risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY at Section 2.2, page 5 (July 2017), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2017/ps1517.

[47] *See* Sweeney, *supra* note 45 at 1.

[48] The PRA refers to "silent cyber" and "non-affirmative" cyber interchangeably. *See, infra* note 81.

numbers[49] fails, reinsurance mechanisms are stressed (or fail), and the ability of an insurer to pay claims or maintain solvency while paying such claims (or both) is seriously jeopardized. This "all or nothing" viewpoint is potentially a detrimental position for an industry with a core business in quantifying and monetizing risk transfer.

What is the foundation for drastically different viewpoints? Notably, the PRA's proposed explanation of this finding is as follows:

> ...much of the divergence is likely to be reflective of differences in firms' **perception of [cyber] risk**. This suggests that some firms should give **further thought** to the potential for cyber exposure within these specific portfolios.[50]

According to the PRA, the inability of firms to agree on the extent of cyber exposure in their portfolios (again, viewing it as an all-or-nothing proposition) is attributable to differences in "perception of risk"[51] and, as a result, firms should further think about the potential exposure to cyber within such portfolios. The PRA's statement suggests that the source of the gap is some fundamental disagreement about the characteristics or severity of cyber risk itself. The PRA's statement is tough to interpret literally because it suggests that the issue of "silent cyber" stems from the insurance industry's collective lack of appreciation for cyber risk itself. While this could be the root cause, historic media coverage[52] suggests that insurers'

---

[49] *See* IRIMI.com, https://www.irmi.com/term/insurance-definitions/law-of-large-numbers, as follows:

Law of Large Numbers — a statistical axiom that states that the larger the number of exposure units independently exposed to loss, the greater the probability that actual loss experience will equal expected loss experience. In other words, the credibility of data increases with the size of the data pool under consideration.

[50] *See* Sweeney, *supra* note 45 at 1 (emphasis added). This was a finding from Property, Marine Aviation and Transport and Miscellaneous lines. *Id.*

[51] Risk perception is defined as the subjective judgment of the characteristics or severity of a risk. See, generally, Joy Inouye, *Risk Perception: Theories, Strategies, and Next Steps,* CAMPBELL INSTITUTE (2017), https://www.thecampbellinstitute.org/wp-content/uploads/2017/05/Campbell-Institute-Risk-Perception-WP.pdf.

[52] *See, e.g.*, GUY CARPENTER, LOOKING BEYOND THE CLOUDS: A U.S. CYBER INSURANCE INDUSTRY CATASTROPHIC LOSS STUDY 11 (2019) reported as follows: Judy Greenwald, *Catastrophic cyber event could cause up to $23.8B in insured losses,* BUS. INS. (Sept. 5, 2019), https://www.businessinsurance.com/article/20190905/NEWS06/912330500/Catastrophic-

concern about the impact of cyber risk is and has been far-reaching, even prior to and at the time of the PRA's initial investigations. Multiple studies propose that there is consensus among insurance professionals that cyber risk is a serious risk with a high degree of severity and accumulation potential.[53] In its 2015 Global Risk Report, for example, the World Economic Forum identified technological risks, in the form of data fraud, cybersecurity incidents, or infrastructure breakdown, as among the top ten risks facing the global economy.[54] Moreover, cyber risk was identified as the fourth largest risk among surveyed insurers (and first among U.S. and U.K. insurers) in a 2015 report on industry perceptions of risk.[55]

That said, this divergence of opinions as to whether cyber risk has a potential to impact traditional lines of coverage is by some definition the actual problem of "silent cyber." The origin of the problem, however, is less likely due to an insurer's perception of cyber risk *per se* and more likely due to different insurer views as to the ways an insurance portfolio—made up of numerous individual policies—will ultimately respond to cyber risk at the time of a cyber incident. This could derive from a misunderstanding of or an underappreciation as to how a policy's actual

---

cyber-event-could-cause-up-to-%24238B-in-insured-losses-Guy-Carpenter; Amy O'Connor, *Insurers' Worst Fear: Cyber Hurricane or Silent Cyber?*, INS. J. (Mar. 21, 2018), https://www.insurancejournal.com/magazines/mag-cover/2018/05/21/489542.htm; Partner Re, *Cyber Insurance The Markets View* (Sept. 17, 2020) at 2*,* https://partnerre.com/wp-content/uploads/2020/09/Cyber-Insurance-The-Markets-View-2020.pdf.

[53] *See generally* the *Allianz Barometer Reports*, which surveys Allianz customers (global businesses), including global insurers, brokers and industry trade organizations. It also surveys risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty (AGCS) and other Allianz entities. Cyber risk has been in the top 10 business risks in every annual report since 2014 (#8), 2015 (#5), 2016 (#3), 2017 (#3), 2018 (#2), 2019 (#2), 2020 (#1). Reports can be viewed here: ALLIANZ*,* https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

[54] *See* Klaus Schwab, *Global Risks 2015 10th Edition*, WORLD ECONOMIC FORUM (2015), http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

[55] *See PWC and Centre for the Study of Financial Innovation, Insurance Banana Skins 2015: The CSFI Survey of the Risks Facing Insurers* (July 2015) at paragraph 1, http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf.

contractual language will respond to a cyber event, especially where such language does not specifically address cyber events.[56]

The proof—that the issue of "silent cyber" is at base a semantic problem—is in the pudding. Prior to the PRA's widespread publication of its non-affirmative cyber findings (and prior to Lloyd's development and implementation of cyber exclusions), insurers had not begun to approach the problem systematically. While some markets occasionally included cyber exclusions on traditional lines policies to address attritional losses, few carriers had taken an apparent enterprise-wide position as to addressing cyber risk in nontraditional lines of coverage.[57] Moreover, Lloyd's formal response to the PRA's call to action to correct "silent cyber" was a semantic one. In 2019, Lloyd's mandated that all insurers writing on Lloyd's paper clarify all policy language by either excluding cyber or affirming cyber.[58] At the time of the article's publication, this endeavor is underway.[59]

V. SEEKING NORMATIVITY

The PRA's definition of "silent cyber" evolved over the course of its surveys, findings, and publications. Some versions rely on normative concepts of

---

[56] *See* Abraham & Schwarcz *supra* note 41 at 9–29 (describing in detail where coverage for cyber incidents may be "found" in non-Cyber policies). Another potential reason for the differentiation could be that carrier have differing views as to motivations—i.e., as to the likelihood of insureds to seek coverage for cyber losses under traditional lines of coverage. This is a worthwhile topic; however, this article will primarily focus on the semantic differences at play rather than the likelihood of any one or multiple insureds to pursue a type of loss under any given policy.

[57] The first carrier market reported to announce a full-blown conversion of its forms was Allianz in 2018. *See The Problem of Silent Cyber Risk Accumulation* (Feb. 25, 2020), https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation (stating "…Allianz became the first commercial insurer to adopt a more broadscale approach to addressing silent cyber"). However, there is support for the argument that one carrier, FM Global, had attempted to offer cyber coverage more expressly with its property offering in 2016 with its offering, "FM Global Advantage All-Risk Policy." *See The FM Global Advantage All-Risk Policy,* https://www.fmglobal.com/products-and-services/products/the-fm-global-advantage-all-risk-policy. However, this carrier did not participate in the referenced PRA conversations as it is a US-domiciled carrier.

[58] *See* Bulletin from Caroline Dunn, Head of Class of Business, Performance Management at Lloyd's, *Providing clarity for Lloyd's customers on coverage for cyber exposures* (July 4, 2019), https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2019/07/y5258.pdf.

[59] *See id.*

"cyber risk" or "cyber exposure" or "cyber related losses," while others rely on terminology commonly used and defined in Cyber-specific insurance policies. By describing the issue of silent cyber both with normative cybersecurity concepts on the one hand and with Cyber policy concepts on the other, the PRA was touching upon the two main categories of silent cyber loss: ensuing loss and cyber product loss.[60] Both categories are important. A definition Cyber product loss allows insurers to effectively treat situations in which overlapping coverages are inadvertently provided. A definition of ensuing loss is equally important, given that non-Cyber policies will in fact end up being required to pay for losses caused by cyber risk, since insurers are concerned about the potential for aggregated ensuing loss to create solvency concerns.

Put in terms of cause and effect, the "ensuing loss" category of silent cyber loss addresses "cyber" as a peril[61] or as a hazard[62] and refers to losses[63] that flow from such cyber perils or hazard. In other words, as humanity grows increasingly dependent upon computers and digitization, the mere use of a computer or computer-

---

[60] For examples of ensuing loss and product loss, *see* Table B.

[61] *Peril,* BLACK'S LAW DICTIONARY at 524 (2nd Pocket Edition 2001). Black's defines "peril" as follows:

2. *Insurance.* The cause of a loss to a person or property.

Compare with, Black's definition of *hazard:* "The risk or probability of loss or injury esp. a loss or injury covered an insurance policy." *Id.* at 316.

[62] There is an interesting debate over whether cyber is a peril or a hazard. Because it is not germane to my argument, I will not be addressing in detail. Generally, a peril is the occurrence of a bad event and a hazard is a condition that increases the likelihood of a peril to occur. Examples of traditional perils include hurricanes, floods, and fire. Types of traditional hazards include immorality, physical imbalances, and lack of morale. *See generally* Marco Lo Giudice, PhD, *Cyber Risk: from Peril to Product, A New Approach for Managing Silent Cyber Risk* (Mar. 2020), https://resources.kovrr.com/Silent-White-Paper-Final.pdf (stating "Cyber is a multifaceted peril that is both a threat and an opportunity for the insurance industry: an opportunity because of the ever-evolving needs of coverage for businesses of any size, and a threat because of the systemic risk arising from its potential for overlap with other lines of business"). *But see* Ruperto P. Majuca, William Yurcik, Jay P. Kesan, The Evolution of Cyberinsurance, cs.CR (Jan. 2006) at 11 ("The second major problem that insurers need to address in developing cyber insurance coverage is the "moral hazard" problem. The problem is when firms are covered by insurance they may either intentionally cause the loss or take fewer measures to prevent the loss from occurring.").

[63] Generally speaking, "ensuing losses" are losses that follow from an incident that causes direct physical loss or damage.

operated technology will result in losses from otherwise covered perils. Another way to put this is that a computer is somewhere involved in the causal chain of the loss, even if the computer was not the sole cause[64] or the proximate cause[65] of the loss. This type of "silent cyber" is where a loss is caused by or results from computer-related acts or events, but where such cause does not change the nature of the expected loss under any given policy (but may change the magnitude or frequency of such loss). The exposure is typically "silent" due to the structure of all-perils policies or policies that may otherwise embody aging language. An example of ensuing loss is where a hack (cyber incident) exploits a vulnerability in a computerized device so as to cause a fire (a traditionally covered peril), which causes property damage to a building (an ensuing loss).[66] Historically, this type of incident would be covered under a property policy that covers damage to a building caused by fire, a covered peril, regardless of the use or involvement of a computer. Accordingly, there is no apparent mismatch between the policy offering and the intention of the underwriter in terms of type of risk, even though the policy's language may fail to expressly discuss computer-related technologies.

The other category of "silent cyber" relates to Cyber as an insurance product. This version of "silent cyber" is where the losses covered by a non-Cyber policy stemming from a cyber event overlap with losses specifically covered by a Cyber insurance product, against the insurer's intention that traditional policy and Cyber policies "nest" together to cover mutually exclusive sets of losses. In these cases, the cyber-related acts or event results in loss that is a change to the nature or the characteristics of expected loss under a traditional insurance policy. The result is tantamount to the type of coverage one would normally find in the insuring

---

[64] *Sole cause,* BLACK'S LAW DICTIONARY at 89 (2nd Pocket Edition 2001). Black's defines "sole cause" as follows:

The only cause that, from a legal viewpoint, produces an event or injury.

If it comes between a defendant's action and the event or injury at issue, it is treated as a *superseding cause.*

[65] *Proximate cause,* BLACK'S LAW DICTIONARY at 88 (2nd Pocket Edition 2001). Black's defines "proximate cause" as follows:

1. A cause that is legally sufficient to result in liability.
2. A cause that directly produces an event and without which the event would not have occurred. *Id.*

[66] *See* Paul Wagensiel, *Printers Can Be Hacked to Catch Fire,* SCIENTIFIC AMERICAN (Nov. 29, 2011), https://www.scientificamerican.com/article/printers-can-be-hacked-to-catch-fire/ (relaying findings by Columbia University researches that attackers may spread malware causing printers to overheat and catch fire).

agreements[67] of a standalone Cyber policy. Such losses often come as a surprise to the underwriter, are brought under a novel theory of loss (from the perspective of the insurer), and were not factored into the underwriting process when pricing and terms were quoted to the insured. Put another way, such losses are aberrations as to what is underwritten to and ultimately modeled by pricing or CAT actuaries for that specific product line. This type of silent cyber loss has to do with "cyber," not as a normative concept of cyber risk, but as a normative concept of a distinct type of insurance product line (herein "Cyber"). An example of this is where a retailer experiences a cyberattack (such as a data breach) whereby the personal data of many customers is released, including bank account information. The banks, who must now re-issue all affected credit cards to consumers, proceed to sue the retailer-insured to recover the costs of the cards (Cyber product loss). Consequently, the insured alleges that this is a form of damage to tangible property due to their limited usability (novel loss theory).[68]

Earlier iterations of the PRA's definition of "silent cyber" have combined the two views of the term: one, having to do with "cyber" as a peril or a hazard, or in simpler terms, a cause of loss, and the other, having to do with "Cyber" as a type of insurance coverage. In a 2016 advisory, for example, the PRA explained that it was investigating the question of underwriting risks emanating from affirmative[69] Cyber insurance policies, but also "from implicit cyber exposure within 'all-risks'[70] and other liability insurance policies that do not explicitly exclude cyber risk. This latter type of cyber risk is referred to as 'silent' cyber risk…"[71] In this

[67] Meaning, the greatest scope of coverage offered under any Cyber insuring agreement, notwithstanding any exclusions.

[68] This is a novel theory of loss because it involves an allegation that cards are damaged based on "loss of use" versus actual physical damage to the card, particularly because the cards were physically useable after the attack. In other words, users could physically swipe their affected credit cards, albeit not without consequence. *See Target Corp. v. ACE American Ins. Co., et al*, 2021 WL 424468 at *7 (D. Minn. Feb. 8, 2021) (holding that Target could not obtain coverage from its CGL to replace credit cards after a data breach under a "loss of use" theory as the cards diminution in value did not amount to loss of use).

[69] Affirmative Cyber policies are insurance policies that specifically respond to a variety of so-called "cyber incidents," including ransomware attacks, viruses, ddos attacks, but also to computer system failures, supply chain interruptions, and exfiltration of private data (both digital and analogue).

[70] All-risks policies refer to traditional property and casualty policies that respond to all perils unless specifically stated otherwise.

[71] *See* Moulder, *supra* note 19. *See also,* Consultation Paper 39/16, *supra* note 39 at 5.

characterization, the PRA focuses on scenarios where cyber exposure is implicitly covered within all-perils insurance policies. The reason why this would be an area of "silent cyber" is because such all-perils policies would readily have been developed, standardized, and well-established prior to the computerization of society. As such, the policies did not contemplate that the malicious use of a computer could be a peril, simply because computers were not in commercial use at the time the language was initially developed.[72] More appropriately, the cyber aspect was not so much silent as it was absent. Notably, these traditional policies were also first developed prior to the invention of a standalone Cyber policy. So, underwriters could not have possibly considered whether the type of loss would be redundant with an affirmative Cyber insurance product.

Later, in a 2017 Supervisory Statement, the PRA defined cyber insurance underwriting risk as "the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (e.g. cyber attack [sic], infection of an IT system with malicious code) and non-malicious acts (e.g. loss of data, accidental acts or omissions) involving both tangible and intangible assets,"[73] introducing a dichotomy[74] between malicious and non-malicious behaviors that recurs in the recent Lloyd's wording[75] developed to address

---

[72] *See generally* LLOYD'S WORDING REPOSITORY, https://www.lloyds.com/wordings.

[73] Supervisory Statement SS4/17, *Cyber insurance underwriting risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY at 5 (July 2017), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf?la=en&hash=6F09201D54FFE5D90F3F68C0BF19C368E251AD93.

[74] This dichotomy is interesting for a number of reasons but for the purpose of this article, I note that no similar dichotomy between malicious and non-malicious acts appears in standalone affirmative Cyber policies (or to the same extent) as they are offered today. For instance, coverage applies equally if the loss stems from a malicious cyber attack or from an act of negligence or an accidental event (i.e., system failure coverage is a common trigger in an affirmative Cyber policy). So, here is an example of where carriers that are trying for a systematic approach to clarified wording are introducing a concept that is foreign to the Cyber product.

[75] *See generally* LLOYD'S WORDING REPOSITORY, https://www.lloyds.com/wordings. For an example of the introduction of the "malicious" concept into the wording, Lloyd's introduced this language in 2019:

MARINE CYBER EXCLUSION

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

"silent cyber."[76] In other words, a prudential risk—or a non-silent risk, rather—is one that is intentionally underwritten to and priced for, whereas with silent cyber exposures, one of those two elements is absent: underwriting intent as to cyber risk or pricing as to cyber risk.[77] In the same 2017 Supervisory Statement, the PRA simplifies the definition of non-affirmative cyber as: "insurance policies that do not explicitly include or exclude coverage for cyber risk."[78] Given that here the PRA is referring to insurance policies, which are contractual arrangements commemorated in writing, it follows that one of the primary issues of "silent cyber" is an issue of language—specifically, the failure of the underwriter to clearly express: 1) whether cyber perils are covered; and 2) whether that coverage is the same kind of coverage found in an affirmative Cyber insurance product.

One of the major issues with the PRA's earlier definition of "silent cyber" is that it attempts to define cyber underwriting risk in relation to a normative concept of "cyber risk"—a concept that the PRA does not define.[79] As such, in evaluating its

---

1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by,
contributed to by or arising from:
1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or
1.2 the use or operation, **as a means for inflicting harm**, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
LMA5402 (emphasis added). *Id.*

[76] *See* Supervisory Statement SS4/17, *supra* note 73. *But see,* Consultation Paper CP39/16, *Cyber insurance underwriting risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY (Nov. 2016) at 5, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916 (PRA defines cyber underwriting risk is as the set of prudential risks emanating from underwriting insurance contracts that are exposed to losses resulting from a cyber-attack).

[77] *See* Supervisory Statement SS4/17, *supra* note 73.

[78] *See id*. at 5.

[79] There is no known standardized definition of the term "cyber risk." I have come across a variety of definitions of cyber risk. *See, e.g.*, CRO Forum, *The Cyber Risk Challenge and the Role of Insurance,* paragraph 3 (Dec. 2014), *available at* http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/
(defining cyber risk as "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications

portfolio's cyber exposure, the carrier is then left to determine whether "cyber risk" is the same as "cyber underwriting risk" and in turn, whether this equates to "cyber-related losses" or is something else altogether. This potentially raises an issue for insurers trying to understand and comply with the directives of the PRA, and ultimately, to measure their cyber exposure across product lines and perhaps change course to correct their portfolios. If the PRA is going to characterize a type of risk as prudential, there also must be some foundational concept of what that risk is (and what it is not).

In the same Policy Statement[80] referencing a concept of "cyber risk," the PRA also explained that the definition of "silent cyber" should be understood as the equivalent of a concept of "non-affirmative cyber."[81] Here, the PRA departs from a definition of "silent cyber" that is entirely dependent upon a concept of "cyber risk" *per se.* According to the PRA, "silent cyber" and "non-affirmative cyber" can be used interchangeably.[82] The PRA noted that four of the thirteen respondents to its

---

networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments."); Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016), *available at* https://www.bis.org/cpmi/publ/d146.htm (defining cyber risk as "The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation.").

[80] *See* Policy Statement PS15/17, *Cyber Insurance Underwriting Risk,* BANK OF ENGLAND: PRUDENTIAL REGULATION AUTHORITY (July 2017), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2017/ps1517.pdf. Policy Statement SS4/17 is responsive to Consultation Paper (CP) 39/16 'Cyber insurance underwriting risk', including Supervisory Statement (SS) 4/17 'Cyber insurance underwriting risk', which sets out the PRA's final expectations regarding the prudent management of cyber insurance underwriting risk. *Id.* at 1.

[81] Policy Statement PS15/17, *supra* note 80 at 5. *See also*, Supervisory Statement SS4/17, *supra* note 73 at 5-7.

[82] *See* Policy Statement PS15/17, *supra* note 80 at 5. *See*, Supervisory Statement SS4/17, *supra* note 73 at 5 (stating "non-affirmative cyber risk, i.e. insurance policies that do not explicitly include or exclude coverage for cyber risk. This latter type of cyber risk is sometimes referred to as 'silent' cyber risk by insurance professionals.") Other definitions of "silent cyber" exist. For an example, *see* Guidewire's definition in *Silent Cyber Scenario: Opening the Flood Gates* (Oct. 2018), https://success.guidewire.com/rs/140-LHX-683/images/Long_form_final.pdf ("We define "silent cyber" exposure as the potential for

Consultation Paper pointed out that the use of the term 'silent' cyber risk is problematic and may create ambiguity in future arbitration or litigation cases.[83] Moreover, two respondents suggested that the term 'non-affirmative' cyber risk should be used instead whereas one respondent suggested a distinction based on whether cyber-attack is a named peril or not.[84] Finally, one respondent suggested that the distinction between 'silent' and 'affirmative' should be completely removed and instead referred to 'cyber risk exposures.' As a result,

> The PRA's thematic review provided strong evidence of 'silent' cyber risk being a term that is widely understood and used by insurance professionals. However, the PRA agrees that the use of 'non-affirmative' cyber risk may be less ambiguous. We have amended the text…to reflect a distinction between a) affirmative cyber risk (insurance policies that explicitly include coverage for cyber risk); and b) non-affirmative cyber risk (policies that do not explicitly include or exclude coverage for cyber risk).[85]

The PRA's equivocation may seem like an off-hand statement, but it points to one of the PRA's major concerns: aggregation[86]. More specifically, the PRA seeks to identify the potential for "clash" (wherein an insurer can experience excessive

---

cyber risk to trigger losses on policies where coverage is unintentional, unpriced, or both. "Unintentional" coverage means not explicitly excluded or affirmed (with any applicable sublimit)").

[83] Policy Statement PS15/17, *supra* note 80 at 5.

[84] Policy Statement PS15/17, *supra* note 80 at 5.

[85] *Id*. at 5–6.

[86] Clarification of wording alone will not stymie the impact of catastrophic cyber losses to any single insurance firm. However, clarifying the wording and "channeling" the coverages to the appropriate products may serve to gain better or more accurate outputs from cyber models. Insofar as both cyber models and some insurance portfolios fail to distinguish between cyber-as-a-peril and Cyber-as-a-product, outputs may not be credible. For example, when trying to model a cyber event based on limits deployment, the outputs may be overly conservative or overly aggressive. Clarification of wording may lead to a more accurate understanding as to where the potential losses would fall (in terms of product lines and reinsurance treaties) and what the losses would be (roughly, financial loss to Cyber products and property damage to Property products), such that insurers can model with more accuracy and react with appropriate pricing/capital allocation.

covered losses due to one insurable event).[87] In its equivocation of "silent cyber" as "non-affirmative cyber", the PRA's reference point is not only "cyber risk" *per se*, but affirmative Cyber *coverage*, meaning, an actual cyber-specific product offered by the insurance market.

Others who have attempted to define "silent cyber" also embrace the two distinct concepts: normative cyber risk (as a peril) and Cyber as an insurance product. For example, the European Insurance and Occupational Pensions Authority (EIOPA)[88] utilizes a definition of "silent cyber" akin to the PRA's definitions: "Non-affirmative cyber risk refers to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy. The latter type of cyber risk is also referred to as 'silent' cyber risk."[89] Like the PRA, the EIOPA's definition of "silent cyber" both references a concept of cyber risk as well as refers (albeit loosely) to an actual Cyber insurance offering. Unlike the PRA, the EIOPA attempts to define "cyber risk," recognizing that it is a "broadly used term with several definitions."[90] The EIOPA's methodology for this exercise involved asking participants[91] for their enterprise's definition of cyber risk, while providing a cyber risk definition from the

[87] *See* Supervisory Statement SS4/17, *supra* note 73 at 7 (describing minimum standards for insurers to incorporate cyber insurance underwriting risk stress tests that explicitly consider the potential for loss aggregation (eg via the cloud or cross-product exposures) at extreme return periods (up to 1 in 200 years)).

[88] EIOPA is an independent advisory body to the European Commission, the European Parliament and the Council of the European Union. *See, generally,* EIOPA, https://www.eiopa.europa.eu/about/mission-and-tasks_en.

[89] *Cyber Risk for Insurers: Challenges and Opportunities,* EIOPA at 18 (2019), https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf.

[90] *Id.* at 7.

[91] *See id*. at 3. Participants included 41 large (re)insurance groups across 12 European countries representing a market coverage of around 75% of total consolidated assets.

Financial Stability Board (FSB)[92] Cyber Lexicon[93] as an initial reference.[94] The results of the EIOPA's survey varied widely.

> Based on the responses, half of the participating groups seems to be aligned with the FSB definition of cyber risk to some extent. While some groups use an identical definition, others use similar ones with additional specificities, resulting in a narrower definition. Many groups declared that they use the IAIS definition.[95] However, some definitions were substantially different from the FSB Cyber Lexicon. In some cases, the definition of cyber risk was very close

---

[92] *See generally* FINANCIAL STABILITY BOARD*,* https://www.fsb.org. The FSB is an international body that makes recommendations about the global financial system. *Id.*

[93] *See generally Cyber Lexicon*, FINANCIAL STABILITY BOARD (Nov. 12, 2018), https://www.fsb.org/wp-content/uploads/P121118-1.pdf. The FSB developed a cyber lexicon in November 2018, in part, to assess and monitor financial stability risks of cyber risk scenarios. The working group for the Lexicon was comprised of those within and outside of the insurance industry, including formed a working group of experts, chaired by the U.S. Federal Reserve Board. The group members were selected for their expertise in cyber security and cyber resilience regulation and supervision and for their representation of a broad range of FSB member jurisdictions and financial sectors (banks, financial market infrastructures, securities and insurance). The working group included representatives of each of the SSBs, namely, BCBS, CPMI, IAIS and IOSCO. Feedback was provided by International Organization for Standardization (ISO), ISACA (previously known as the Information Systems Audit and Control Association), the SANS Institute and the U.S. National Institute of Standards and Technology (NIST). *Id*. at 3–4.

[94] The *Cyber Lexicon* defines cyber risk as "the combination of the probability of cyber incidents occurring and their impact." *Id.* at 9 (adapted from Committee on Payments and Market Infrastructures-International Organization of Securities Commissions, International Association of Insurance Supervisors (CPMI-IOSCO, ISACA) Fundamentals and ISACA Full Glossary).

[95]According to IAIS, the definition of cyber risks is "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information − be it related to individuals, groups, or governments." *Draft Application Paper on Supervision of Insurer Cybersecurity*, IAIS (2018) *available at* https://www.iaisweb.org/file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity.

> to the FSB definition of a cyber incident[96], **where groups define cyber risks as an ex-post event which implies harmful outcomes**. One group defined cyber risks as the **risk of non-compliance with regulatory and legal requirements due to inadequate cyber protection**. Finally, **a few groups do not have a specific definition for cyber risks at all, although they declared to be working on establishing a clear definition.**..[97]

In summary, the EIOPA concludes that "Overall, it seems that the insurance sector is not fully aligned yet when it comes to conceptually defining cyber risks."[98] EIOPA goes on to say that, "Having a clear, comprehensive and common set of definitions on cyber risks would enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could facilitate the development of sound solutions to cybersecurity challenges."[99]

The EIOPA's conclusion that having a clear and common set of definitions would foster a more productive dialogue regarding cybersecurity challenges, including quantification methods for "silent cyber," rings true. Its straightforward observation aligns with the PRA's findings regarding disparate opinions as to the amount and severity of cyber risk within traditional lines of coverage. As discussed, this divergence in view likely stems from a lack of a collective semantic framework. What the EIOPA, the PRA, and the FSB overlook, however, is the idea that an established semantic framework already exists and is fully accessible to insurers. The sector has already built a strong framework based upon a series of normative constructs and definitions that comes close to a fully formed concept of "cyber risk" viz-a-viz its current standalone Cyber product offerings.

---

[96] The *Cyber Lexicon* defines cyber incident as a cyber event that: "(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not." *See, Cyber Lexicon*, *supra* note 93 at 9.

The FSB defines cyber event as: "Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring." See (adapted from NIST's definition of "Event")

[97] *See, Cyber Risk for Insurers, supra* note 89 at 7 (emphasis added).

[98] *Id.* at 8.

[99] *Id*.

VI. CYBER INSURANCE AS THE SEMANTIC PARADIGM FOR SILENT CYBER

What if, instead of relying upon definitions derived from outside the insurance industry to address "silent cyber," the insurance industry drew upon its own resources as a normative guide for cyber risk? A good starting place is to look at what a standalone Cyber risk policy covers and does not cover. Even though a market-standard monoline Cyber policy will typically only provide coverage for financial loss (and does not typically extend to bodily injury and property damage), insurance carriers can still refer to the insuring agreements of such a standalone policy to formulate a comprehensive idea as to what "cyber risk" means, both to the insurance industry and to its policyholders.

Since its earliest iterations, the cyber policy offering has evolved to stay fit for purpose. The coverage will continue to evolve over time as offerings expand and contract in response to the threat environment as well, the insurance marketplace, and the performance of affirmative Cyber portfolios.[100] However, there are two main reasons to rely upon cyber concepts that are already formulated in an insurance coverage policy. One is that the Cyber insurance policy is developed from a set of norms that the industry already accepts, some of which was directly in reaction to the threat environment experienced by actual companies, so it is a good place from which to establish common dialogue.

A second reason is that the industry's preoccupation with "silent cyber" is due in large part to the potential "clash" risk involved with having accumulative and redundant cyber coverages available to the same client or subject to the same cyber event, unbeknownst to the underwriters. Namely, of the two theories of "silent cyber" loss, the Cyber product loss is the more pressing aspect of the silent cyber problem. By its very definition, ensuing loss from a cyber event is likely contemplated by the underwriter and priced for accordingly. And because the cyber event is one event among others on the causal chain, as opposed to being the single event on the causal chain, ensuing loss has an anchor to a time and place type peril (e.g., fire), which helps to anchor the loss in a predictable pricing manner. On the other hand, Cyber risk as a form of product loss is where insurers can start to see the pronounced effects of accumulation across a portfolio. Because Cyber as a product loss refers specifically to *covered* losses under affirmative cyber policies, where

---

[100] *See* John Hewitt Jones, *AIG Introduces Ransomware Co-Insurance and Sub-Limits at 1.1 Cyber Renewals* (Jan. 7, 2021), https://insuranceinsider.com/articles/137600/aig-introduces-ransomware-co-insurance-and-sub-limits-at-11-cyber-renewals.

traditional policies respond to the cyber perils in the same type of way as Cyber policies, there is a real potential for an insurer to have significant limits exposed to a cyber event at significantly reduced pricing. Accordingly, if Cyber product loss accumulation is the more prominent concern of "silent cyber," correcting traditional policy language to eliminate (or at least price for) redundant Cyber coverage becomes the first priority[101] of the "silent cyber" solution. To accomplish this objective, an enterprise must be well-versed in the mechanics and semantics of a typical standalone Cyber offering.

To some, the following analysis may seem to presuppose that affirmative Cyber coverage is an accurate reflection of the real cybersecurity landscape. Certainly, there is an overlap as to the realities of cyber, as a peril, and "Cyber," as an insurance product as demonstrated further in the history of the cyber product section of this article. Regardless, while it may be the case that an insurance policy is a kind of representation of the threat or peril that it purports to cover, it uses abstractions to describe both the coverage triggers and the losses.[102] Accordingly, it less critical to the silent cyber solution that policy language accurately reflect the actual threat environment or encompass all that can be imagined as "cyber risk," than it is for the insurance policy to accurately reflect the intentional and *insurable* (whether potential or actual) Cyber risk. By "insurable" Cyber risk, I am referring to the causes of loss and the types of loss to be covered, as contemplated by the underwriter.

As such, the appropriate definition of cyber risk for "silent cyber" is simply the type of risk that insurers of affirmative Cyber are generally willing to cover at a given point in time. Of course, there is no one single standard for a standalone Cyber coverage offering now or in the past, and there continue to be changes in policy offerings across various firms, along with nuances of certain offerings. However, there are coverage norms from which the insurance industry can gain a better understanding of the risk landscape as it seeks to correct the problem of "silent cyber." In other words, what we are looking to do with "silent cyber" is align portfolios within insurance companies and across the insurance industry. To realize this goal, a common language and framework for understanding must be accessed

---

[101] A secondary component of the "silent cyber" solution is the capability to accurately map and quantify the areas of Cyber product losses, regardless of the original intent of the underwriter at the time of binding. Quantifying this accumulation exposure can be done more meaningfully if insurers map cyber exposures to the general categories of insurable Cyber losses throughout their portfolios.

[102] KENNETH S. WOLLNER, HOW TO DRAFT AND INTERPRET INSURANCE POLICIES (1999) at 80 (explaining how abstractions are useful in succinctly drawing together a series of concrete ideas into a single concept and in anticipating unforeseen circumstances).

from within so that the industry can retrofit its aging architecture of insurance terminology to confront this emerging risk.

VII. CONCLUSION

Many organizations and government bodies are widely concerned about the risks associated with cybersecurity. The media attention alone does not allow the public to ignore cyber threats, albeit much of the media attention is dedicated to individual attacks against individuals and disparate companies, and less of it is focused on cybersecurity events that would lead to widespread, catastrophic, cumulative loss for insurers. Insurers, are in the business of underwriting risk, including cyber risk. Pricing for such risk is done based upon modeling losses and various other factors, with most of the premium associated with attritional losses expected for any individual insured. Correlated cyber loss, has become a more pressing concern for insurers.[103]

Since the PRA's work on silent cyber since 2015, there has been increased awareness of silent cyber exposures, and fears of underpricing for it within an insurer's portfolio. Most stakeholders seem to agree that cyber risk is a risk that should be measured, priced, underwritten, and otherwise treated appropriately. So, how do we then reconcile the acute variations in understanding cyber exposures simply as differences in perception of risk? Instead, insurers must admit that this there is an emerging consensus around the perceived severity of cyber risk. They must also recognize that the central issue of "silent cyber" is first and foremost a problem of semantics. When insurers and governing agencies have looked for a common language regarding cyber, they have looked outward, instead of looking inward. This has led to confusion and discord which in hindsight was largely avoidable had the industry and its regulators used the nomenclature at its disposal.

Carriers' first step to addressing "silent cyber" has been to review and potentially alter policy wording with regard to cyber risk. Curiously, most of the characterization has been dedicated to insurers making efforts as to "clarifying intent."[104] The suggestion is that the intent the insurance company seeks to clarify is

---

[103] Amy O'Connor, *Insurers' Worst Fear: Cyber Hurricane or Silent Cyber?* INS. J. (Mar. 21, 2018), https://www.insurancejournal.com/magazines/mag-cover/2018/05/21/489542.htm.

[104] *See Silent Cyber: What It is and How You Can Cover Cyber Perils*, MARSH (Aug. 2020) https://www.marsh.com/uk/insights/research/silent-cyber-how-you-can-cover-

"subjective" intent.[105] The characterization is a strange one considering insurance contracts: 1) consist of a series of logical syllogisms[106]; and 2) are (for the most part) standardized. As such, legal interpretation of contracts (especially ones that fit this linguistic structure) depend almost entirely on the plain meaning of the text with the assumption that there is in fact an objective meaning to be communicated and understood. In such an interpretive undertaking, questions of intent on the part of the drafters or ratifiers of the document are rare and reserved for coverage litigation.

Why then would insurers ask themselves what was intended by the language set forth before cyber risk existed? While the question of intent cannot altogether be avoided when it comes to clarifying what Cyber loss will ultimately be covered by any given policy, the PRA was being generous. Most insurers did not intend for Cyber product loss to fall within traditional policies because cyber risk, cyber warfare, the use and promulgation of the computer, and mounting issues of privacy facing humanity did not exist[107] at the time those policies were first written or, if

---

perils.html ("Insurers are taking steps to address this issue, some required by regulators, to clarify their coverage intent regarding cyber.").

[105] Notably, the EIOPA promotes a mutuality in this undertaking: https://www.eiopa.europa.eu/sites/default/files/publications/cyber-underwriting-strategy-february-2020_0.pdf ("A mutual understanding of contractual definitions, conditions and terms, for both, policyholders and insurance undertakings. Clear and transparent cyber coverages are crucial from a consumer protection perspective. It is the role of industry and consumers associations to provide this clarity and align expectations on cyber insurance coverages to avoid the potential for coverage disputes and costly litigation. The European Commission and EU institutions (including EIOPA), on the other side, could promote and act as an accelerator of this process towards greater transparency and improved mutual understanding.")

[106] WOLLNER *supra* at 140 ("normalized drafting represents an attempt to bring the certainty of symbolic logic to the drafting process.").

E.g.,

If THIS, then THAT.

THIS means abc.

THAT means xyz.

If abc, then xyz.

[107] Arguably, they did exist but were not relevant to the underwriting of commercial insurance. For instance, in 1982, the CIA tricked the Soviet Union into acquiring ICS software with a built-in flaw. The software was programmed to malfunction, resulting in one of the world's largest non-nuclear explosions. *Owning the Battlefield,* CYBEREASON INTELLIGENCE GROUP, at 4 (2017) *https://hi.cybereason.com/hubfs/Content%20PDFs/Owning%20the%20Battlefield-Fighting%20the%20Growing%20Trend%20of%20Destructive%20Cyber%20Attacks.pdf.*

they did exist, insurers failed to anticipate that they would impact traditional products[108] with any sort of accuracy. The pressing concern is not what insurers "intended" back then but more so consensus within insurance organizations today on base concepts such as what is cyber risk, what are cyber perils, and what constitutes physical loss versus non-physical loss. Only then can insurers decide where those risk should be covered and how they should be priced.

If insurers would recognize the futility in arguing over whether they should have seen the problem of silent cyber coming, and if they would cease their public posturing over the "original" intent of the policy language, perhaps they could then turn their attention to retrofitting the wording to the realities of the current threat environment, giving this problem some *further thought* as the PRA had suggested. I propose that insurers (and deciding courts) acquire a deeper understanding of the plain meaning of the wording contained in Cyber insurance forms, take those concepts, and apply them to traditional wording. The best frame of reference for analyzing whether there is Cyber coverage lurking in a traditional policy (and therefore more broadly within a product line) is the coverage afforded by a standalone Cyber policy. Not only will this reveal the plain meaning of critical definitions which govern both cyber as a peril and Cyber as a coverage, but this understanding will be derived from the collective expectation of coverage from the insurance consumer point of view. In other words, if one wants to know if a non-cyber policy[109] offers Cyber coverage, one must first read and understand what an affirmative Cyber policy offers. From this vantage point, insurers can begin to assess and measure the extent of "silent cyber" within their portfolios.

The question of how much the insurance industry knew about cyber risk before the advent of the standalone Cyber policy would make for an interesting discussion, but it is largely irrelevant to the scope and severity of the present cyber threat environment in which the industry finds itself. Therefore, when insurers profess to be "clarifying" our intent, it would be more honest to simply acknowledge that they are examining whether they need to charge more now to compensate for the fact that they had unwittingly offered coverage *gratis* for one of the most complex insurance risks that exists today.

[108] *See* Abraham & Schwarcz *supra* note 41 at 9–29 (describing in detail where coverage for cyber incidents may be "found" in non-Cyber policies).

[109] I am using the term Non-Cyber Policy to mean any policy that was not expressly designed to cover cyber risk.

VIII. TABLE 1

Insuring Agreements	**First or Third Party**	**What it covers**	**Examples**
Privacy Breach Liability (together or separate with Security Breach Liability)	3rd party (responds to a Claim made)	Defense costs Loss (judgment, settlement)	Retailer is sued by customers after its computer system is hacked for failure to adequately protect their data. OR A hospital is sued by a patient for negligence with respect to privacy because a paper file with the patient's health information was stolen by the hospital's disgruntled employee.
Regulatory Liability	3rd party (responds to a Claim made)	Defense costs Fines and penalties	The ICO brings a regulatory investigation against a hotel that suffered a data breach due to a computer virus and exposed customer information. The ICO assesses a fine of $2m against the hotel under the GDPR.
PCI Liability	3rd party (responds to a Claim made)	Defense costs PCI Payments	Restaurant has a data breach exposing credit card data of thousands of customers. The bank that the restaurant uses to handle credit card transactions sues the restaurant to recover some of their losses from the merchant that had the breach under their contract (called a PCI assessment).
Incident Response	1st party (responds to a Security Incident or a Privacy Incident)	Mitigation costs (costs to mitigate the damages to the party that is suing the insured)	Retailer discovers that its computer system is hacked and personal and financial information of its customers is stolen. It seeks coverage for a privacy counsel, a forensic to see where the breach came from, costs to notify affected customers, setting up and

		e.g., privacy counsel, forensic analysts, costs to notify of the breach, call center operations, credit monitoring costs	operating a call center for customers, and credit monitoring for customers.
Cyber Extortion	1st party (responds to a ransomware threat)	Ransomware payments	A company gets a notification on a work computer that all the data in the system has been encrypted and if the company wants its data back, they will need to pay the attackers $25,000. The company negotiates with the hacker and agrees to pay a ransomware payment of $15,000 to release in the information.
Restoration	1st party (responds to a security incident or a system failure)	Payments to vendors who will do any of the following: Determine whether data or software can be restored; replace or restore data or software	A company who experienced a ransomware strain is unable to pay the ransom and they lose access to their data. The company decides to hire vendors to restore their critical data.
Business Interruption (also contingent business interruption; also	1st party (responds to a security incident or a system failure)	Payments of the Loss of gross profit sustained by the company due to the slowdown or	A retailer is attacked by a computer virus and its payment processing systems go down. They are offline for 7 days and lose $40,000 in gross profit.

reputational harm)		interruption of business when a company is attacked.	
Social Engineering	1st party (responds to a fraudulent transfer of funds based on a security incident)	Payment of the actual transferred payment to the bad actor	A cyber hacker breaches a law firm's computer system. He is has the capability to send an email from the company's system, pretending he is the CEO. He asks an admin to reroute a payment for advertising services to a new location. The payment is routed to him under false pretences in the amount of $4,000.

IX. TABLE 2

Traditional Product	**Ensuing Loss**	**Cyber Product Loss**
Professional Liability	A publicly traded enterprise experiences a large data breach due to a malicious computer attack. The news of the breach is disclosed publicly, the stock drops, and shareholders file a securities class action against the enterprise, alleging misrepresentations and seeking recovery of financial losses from the drop in stock. The enterprise makes a	A law firm is representing an individual plaintiff in a medical malpractice suit, whom in its professional representation has a duty to keep privilege. During the litigation, a malware is introduced to the law firm environment and the plaintiff's PHI is exfiltrated publicly. The client sues the law firm for malpractice, including negligence in maintaining the confidentiality of her data. She seeks damages, including the costs of credit fraud monitoring and emotional distress. The law firm makes a claim under its Lawyers E&O policy. ***Cause of Loss:*** *cyber* ***Loss:*** *In addition to Ensuing Loss, the CPL loss is an overlap with data breach insuring agreements (1st and 3rd party) under cyber policies.* ***See Privacy Breach*** *and* ***Incident Response*** *above.*

	claim under its D&O policy. ***Cause of Loss:*** *cyber* ***Loss Sustained:*** *financial loss covered under D&O policy*	***Change in Loss Characteristic:*** *The Insurer is being asked to pay for consumer's financial loss in having their private data exposed, not just the financial loss from the attorney's malpractice.*
Casualty	A self-driving car is hacked and as a result, an accident occurs injuring two passengers in the car. The passengers sue the manufacturer of the car, which makes various claims under casualty products. ***Cause of Loss:*** *cyber* ***Loss Sustained:*** *bodily injury covered under general liability /auto/products liability*	Retailer experiences a cyberattack whereby many customers' personal data is released, including bank information. Banks must re-issue all affected credit cards to consumers. Bank sues the retailer-insured to recover the costs of the cards, which it alleges is damage to tangible property due to their limited usability (customers cannot use without risk of fraud). Retailers submit claim to GL policy under a theory of damage to tangible property. ***Cause of Loss:*** *cyber* ***Loss Sustained:*** *Overlap with credit card issuance costs found under data breach and PCI insuring agreements on cyber policies.* ***See Incident Response*** *and* ***PCI*** *above.* ***Change in Loss Characteristic:*** *The Insurer is being asked to pay for credit cards that were not actually physically damaged.*
Property	Pirates hack into a vessel's computerized navigation system, causing it to stop. The pirates onboard and steal	Company was attacked by malware during a routine software update its computer systems leaving certain computerized devices "bricked." The company's business is inoperable for 7 days. Company seeks recovery of its business interruption loss

	various merchandise. The vessel owner makes a claim under a marine product. ***Cause of Loss:*** *cyber* ***Loss Sustained:*** *theft of tangible property*	given the alleged property damage to its computers. ***Cause of Loss:*** *cyber* ***Loss Sustained:*** *In addition to Ensuing Loss, there is an overlap with insuring agreements on cyber policies due to a Bricking Incident. See* ***Business Interruption*** *above.* ***Change in Loss Characteristic:*** *The devices that are "bricked" are not physically damaged. They can still be used for a purpose, even their intended purpose, if they are commercially restored.*

BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY: INSURANCE APPLICATIONS, LEGAL DEVELOPMENTS, AND CYBERSECURITY CONSIDERATIONS

Ken Goldstein[1]

*"*Forecasts suggest that global blockchain technology revenues will experience massive growth in the coming years, with the market expected to climb to over 39 billion U.S. dollars in size by 2025."[2]

ABSTRACT

Blockchain technology is experiencing breakout growth globally. Companies from diverse industry sectors, including insurance, are tapping into its decentralized distributed ledger capability in order to efficiently and transparently transact business, track anything of value, and operate in a more secure environment. While blockchain is being creatively implemented, however, there are also important legal (including legislative) and cybersecurity considerations to account for as a part of the decision-making process.

This paper will start by providing an overview of blockchain technology, including the ability to use it as a decentralized distributed ledger. It will then pivot to a variety of blockchain applications either disrupting or supporting the insurance industry. Thereafter, it will explore blockchain-related legal issues along with Connecticut-based legislative developments in the insurance capital of the world. Lastly, the paper will reflect upon cybersecurity strengths, weaknesses, and best practices associated with blockchain.

---

[1] Ken Goldstein is a former global Cyber Security Product Manager at legacy Chubb Group of Insurance Companies. He is currently a Clinical Instructor of Risk Management and Insurance at the Barney School of Business, University of Hartford, and teaches innovative InsurTech and Cybersecurity curriculum, the former in collaboration with UConn School of Business. Professor Goldstein earned his J.D. at Western New England University School of Law and B.A. at Binghamton University. Professor Goldstein would like to thank Mateo Ramirez-Webster, rising senior at the University of Hartford's Barney School of Business, for his helpful support and insight regarding blockchain legislative developments.

[2] Shanhong Liu, *Blockchain technology market size worldwide 2018-2025*, STATISTA (June 9, 2020), https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/.

I. INTRODUCTION

Blockchain technology has become a critical priority for global organizations.[3] In fact, in a recent Gartner press release, it is suggested that business value associated with blockchain will "surge to exceed $3.1 trillion by 2030."[4] Not surprisingly, companies are looking to dynamically integrate blockchain technology into diverse segments of insurance, including its overall ecosystem.[5] While blockchain test-use cases are rapidly developing, there are also legal, Connecticut-based legislative, and cybersecurity factors to account for as a part of the decision-making process.[6]

This paper explores blockchain and the chance to innovatively implement distributed ledger technology within the insurance industry. It also reinforces various issues of importance while using blockchain relating to the law and preventing unauthorized access to private and proprietary information.

We will start by defining blockchain and highlighting its various purposes. This foundational understanding will allow us to better appreciate the ability to use blockchain as a decentralized distributed ledger.

---

[3] Mike Walker, *Top Blockchain Trends for 2020 And Beyond,* FORBES (Feb. 27, 2020, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2020/02/27/top-blockchain-trends-for-2020-and-beyond/#71aaeebc3774 (noting fifty three percent of Deloitte survey respondents suggested as much).

[4] *Gartner Predicts 90% of Current Enterprise Blockchain Platform Implementations Will Require Replacement by 2021*, GARTNER (June 3, 2019), https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

[5] Sam Daley, *Nine Companies Using Blockchain to Revolutionize Insurance,* BUILT IN (May 9, 2021), https://builtin.com/blockchain/blockchain-insurance-companies.

[6] Christopher Owen, *6 Cybersecurity Trends Worth Looking at in 2020: Blockchain Is on the List*, THE DAILY HOLDL (Mar. 8, 2020), https://dailyhodl.com/2020/03/08/6-cybersecurity-trends-worth-looking-at-in-2020-blockchain-is-on-the-list/; *Legislature Looks at Blockchain Technology, Lacking Master Plan*, CONN. BY NUMBERS (Apr. 25, 2019), https://ctbythenumbers.news/ctnews/legislature-looks-at-blockchain-technology-lacking-master-plan; Stuart D. Levi, Alexander C. Drylewski, Giyoung Song & Thania Charmani, *Emerging Discovery Issues in Blockchain Litigation*, LAW.COM (Apr. 3, 2019, 7:00 AM), https://www.law.com/legaltechnews/2019/04/03/emerging-discovery-issues-in-blockchain-litigation/; John McKinlay, Duncan Pithouse, John McGonagle & Jessica Sanders, *Blockchain: Background, Challenges and Legal Issues*, DLA PIPER (Feb. 2, 2018), https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/.

Next, we will look at blockchain and distributed ledger technology within the insurance environment, including its application to life, health and property & casualty business. We will also evaluate the potential for blockchain and distributed ledger technology to disrupt and/or support the overall insurance ecosystem. This will establish various paths that might be considered by startups and legacy insurers while proactively utilizing blockchain and distributed ledger technology.

Thereafter, we will analyze diverse legal concepts associated with blockchain, including contract formation and enforcement, governance framework issues, and the potential for mistakes or intentional errors to impact an agreement. This will highlight and reinforce the need to have experienced blockchain counsel as a part of the development and implementation process.

Lastly, we will explore strengths and weaknesses associated with blockchain and cybersecurity. This will provide an opportunity to consider best practices that organizations and individuals might consider regarding the protection of blockchain keys and collaborating with third-party service providers.

II. BLOCKCHAIN OVERVIEW

In order to appreciate blockchain applications to the insurance industry and corresponding legal, Connecticut-based legislative, and cybersecurity considerations, it is helpful to start with blockchain's background and purposes. It was originally established to timestamp digital documents to ensure information integrity.[7] While blockchain struggled to obtain widespread use, in 2009, Satoshi Nakamoto utilized blockchain to create Bitcoin, a now popular digital

[7] Brian O'Connell, *What Is Blockchain Technology and How Does It Work?*, THESTREET (Nov. 25, 2019, 11:59 AM), https://www.thestreet.com/technology/what-is-blockchain-15179703.

cryptocurrency.[8] Since that time, blockchain is used to provide decentralized distributed ledger capabilities to anyone (anywhere) with an internet connection.[9]

A decentralized distributed ledger, also referred to as a peer-to-peer network, amasses information permanently across multiple personal computers as opposed to a single, central system.[10] Decentralized distributed ledger technology ("DDLT") is capable of being programmed to keep a record of, and track changes to, anything of value over a period of time (e.g., medical records).[11] Recording and tracking information in this fashion creates overall trust in the data and reinforces a transparent chain of information.[12] It simultaneously removes the need for

---

[8] Avi Mizrahi, *Who is Satoshi Nakamoto? An Introduction to Bitcoin's Mysterious Founder*, BITCOIN.COM (Mar. 8, 2020), https://news.bitcoin.com/satoshi-nakamoto-founder-of-bitcoin/; Rakesh Sharma, *Three People Who Were Supposedly Bitcoin Founder Satoshi Nakamoto*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/tech/three-people-who-were-supposedly-bitcoin-founder-satoshi-nakamoto/.

[9] Andrew Meola, *Distributed Ledger Technology & the Blockchain Explained*, BUS. INSIDER (Jan. 16, 2020, 11:08AM), https://www.businessinsider.com/distributed-ledger-technology-blockchain (noting that you should "[t]hink of blockchain and distributed ledger in the same way you might think of Kleenex and facial tissues" because "[t]he former is a type of the latter . . . ."); Nitish Singh, *15+ Practical Blockchain Use. Cases in 2021*, 101 BLOCKCHAINS (Jan. 28, 2020), https://101blockchains.com/practical-blockchain-use-cases/ ("With blockchain, everything can be accessed from anywhere.").

[10] *Chapter 1: Blockchain Explained: The Ultimate Peer-to-Peer Network*, SINGLE GRAIN, https://www.singlegrain.com/blockchain/blockchain-explained/ (last visited Feb. 25, 2021).

[11] Christina Majaski, *Distributed Ledgers*, INVESTOPEDIA (May 12, 2020), https://www.investopedia.com/terms/d/distributed-ledgers.asp;
Lucas Mostazo, *What is BLOCKCHAIN? The best explanation of blockchain technology*, YOUTUBE (Jan. 14, 2018), https://www.youtube.com/watch?v=3xGLc-zz9cA.

[12] *How Distributed Ledger Technology Can Eliminate Bank Data Breaches*, NASDAQ (Apr. 8, 2020, 1:31 PM), https://www.nasdaq.com/articles/how-distributed-ledger-technology-can-eliminate-bank-data-breaches-2020-04-08 ("Decentralized ID will change the structure of trust in data . . . ."); *What is the Blockchain?*, BITCOIN NEWS, https://thebitcoinnews.com/what-is-the-blockchain/ (last visited June 21, 2021) (reinforcing that the technology is distinguished by, among other things, transparency).

intermediaries and other third parties while allowing users to interact directly with others and their data in real-time.[13]

In addition, blockchain has a direct correlation to rapidly developing applications for different sectors of business, including the insurance industry.[14] In fact, as discussed later in this paper, blockchain and DDLT are being creatively deployed in vast segments of life, health, and property & casualty business.[15] It is also fundamentally reshaping the make-up of the traditional insurance ecosystem, including the underwriting and sales process, the management of claims, and in certain instances, the need for a traditional insurance carrier partnership altogether.[16]

From a mechanical perspective, DDLT embodies a physical chain approach, albeit one made of data as opposed to tangible links.[17] Every piece of the chain, referred to as a block, is added and owned by an authorized user.[18] Once a particular

---

[13] *Blockchain: Legal Implications, Questions, Opportunities, and Risks,* DELOITTE LEGAL, (Mar. 2018), https://www2.deloitte.com/global/en/pages/legal/articles/2018-legal-blockchain.html.

[14] Paramita (Guha) Ghosh, *Blockchain Trends in 2020*, DATAVERSITY (Mar. 17, 2020), https://www.dataversity.net/blockchain-trends-in-2020/ ("The most visible change in business processes due to blockchain may be observable in the insurance sector in 2020."); Ramesh Darbha, *Blockchain: The P&C insurance industry's potential game changer*, CAPGEMINI, (July 23, 2018), https://www.capgemini.com/2018/07/blockchain-the-pc-insurance-industrys-potential-game-changer/; Annap Derebail, *Three areas in the insurance industry to use blockchain*, IBM (Mar. 13, 2018), https://www.ibm.com/blogs/blockchain/2018/03/three-areas-in-the-insurance-industry-to-use-blockchain/; Bernard Marr, *Blockchain Implications Every Insurance Company Needs to Consider Now*, FORBES (Oct. 31, 2017, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2017/10/31/blockchain-implications-every-insurance-company-needs-to-consider-now/#3742513c7026.

[15] Daley, *supra* note 5; *Blockchain applications in insurance,* DELOITTE, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf (last visited June 21, 2021).

[16] Ghosh, *supra* note 14.

[17] Mostazo, *supra* note 11.

[18] Rick Martin, *The Complete Guide to Blockchain for Insurance Companies*, IGNITE (Nov. 30, 2018), https://igniteoutsourcing.com/blockchain/blockchain-and-insurance-industry/.

block is added, unless it is the first in a sequence (referred to as the Genesis block),[19] it is permanently attached to the other blocks.[20] Stated differently, each block is hashed (hashes uniquely identify a block and all of its contents in an encrypted fashion) to the blocks before it and are simultaneously encrypted with a security key based on the blocks before it.[21] A central benefit of this approach is that the overall sequence (or blockchain) is much more difficult to obtain unauthorized access to by an outsider.[22] In fact, in order to tinker with a blockchain, a hacker would need to tamper with all of the blocks on a chain, redo the authorization associated with the network, and then take control of more than fifty percent (50%) of the peer-to-peer network.[23]

In terms of the change and approval process associated with blockchain, if you need to alter information recorded in a particular block, the change is stored in a new block.[24] For example, showing X changed to Y at a particular date and time.[25] Importantly, however, blocks will not be added to a chain unless a cryptographic puzzle is solved.[26] After the puzzle is unraveled (by miners on the peer-to-peer network), it is automatically shared with all of the other computers on the network for verification and approval.[27] This process is referred to as Proof-of-Work, and once accomplished, a block is added to an overall chain.[28]

---

[19] Amanda Allen, *What Is Genesis Block In A Blockchain*, JUMPSTART BLOCKCHAIN (Aug. 26, 2018), https://www.jumpstartblockchain.com/article/what-is-genesis-block-in-a-blockchain/.

[20] International Data Corporation, *What Is Blockchain?,* (2019), https://uk.idc.com/resource/RESOURCES/ATTACHMENTS/IDC-blockchain-infographic.pdf.

[21] Martin, *supra* note 18; Simply Explained, *How does a blockchain work - Simply Explained*, YOUTUBE (Nov. 13, 2017), https://www.youtube.com/watch?v=SSo_EIwHSd4.

[22] Martin, *supra* note 18.

[23] Mohammed Zubair, *Blockchain: Internet 3.0*, PRIMITIVE LOGIC (May 2018), https://www.primitivelogic.com/insights/blockchain-internet-3-0/ ("[t]o successfully tamper with the blockchain, you would need to tamper with all the blocks in it, redo the proof of work for all the blocks, and take control of more than 50 percent of the P2P network.").

[24] Centre for International Governance Innovation, *supra* note 11, at 01:07–01:15.

[25] *Id.* at 01:17.

[26] Simplilearn, *Blockchain in 7 Minutes*, YOUTUBE, at 04:48–04:54 (Feb. 27, 2019), https://www.youtube.com/watch?v=yubzJw0uiE4.

[27] *Id.* at 04:41–04:48.

[28] *Id.* at 05:02–05:07.

Since blockchain is used as a decentralized technology, and not limited to a single network, there are various ways to implement it.[29] These include public, private, or hybrid versions of blockchain.[30] For example, with a public blockchain, each user has the ability to review and access the network's information.[31] On the other hand, with a private blockchain, only select users have the ability to review and access information.[32] Not surprisingly, with a hybrid (public/private) blockchain, public users have more limited ability to review and access information while the private participants can review and access everything.[33]

From a transactional perspective, participants on a blockchain environment have two keys, one public, the other private.[34] A public key is equivalent to a known email address where everyone is aware of the information associated with it.[35] However, a private key permits the user to maintain confidentiality with regard to the information.[36] A good overall comparison would be an unshared password associated with the same email account.[37]

Consider the following transaction example to reinforce how keys work within the blockchain environment:

> Jane Doe, a buyer of a product, uses her private key to send a cryptocurrency payment to a seller, John Doe. Jane's use of her private key generates a hashing algorithm. This also permits Jane to virtually sign and account for the transaction and indicate it came from Jane to John. In order to protect Jane's private key information, however, the transaction is transmitted across the network using her public key. John then receives and decrypts the

---

[29] Lucas Mearian, *What is Blockchain? The Complete Guide,* COMPUTERWORLD (Jan. 30, 2019, 11:13 AM), https://www.shirebiz.net.au/nrsite/wp-content/uploads/2020/09/Block-Chain-Technology-Explained.pdf (noting that blockchain allows data to be stored on thousands of servers).

[30] Mostazo, *supra* note 11, at 04:34–04:53.

[31] *Id.* at 04:30–04:40.

[32] *Id.* at 04:40–04:58.

[33] *Id.*

[34] Leon Di, *Why Do I Need a Public and Private Key on the Blockchain?*, WETRUST (Jan. 29, 2017), https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76.

[35] Simplilearn, *supra* note 26, at 03:30–03:37.

[36] *Id.* at 03:42–04:04.

[37] *Id.* at 03:36–03:46.

> transaction using his own private key. Thereafter, a miner validates the transaction by solving a complex math problem. Once the problem is solved, the transaction is shared with other computers on the network (Proof-of-Work), the entire network verifies it, and a block is added to the blockchain. Jane's and John's digital wallets are then updated.[38]

III. BLOCKCHAIN AND DDLT APPLICATIONS TO INSURANCE

With a better appreciation for blockchain's background and capabilities in mind, we are now in a position to explore different blockchain and DDLT applications to insurance. Not surprisingly, as technology has changed rapidly over the past decade, there has been an opportunity to re-assess various issues adversely impacting the insurance industry.[39] These issues range from inefficient underwriting, sales, and claims practices to the potential for human transactional errors, fraudulent submissions by policyholders, and unauthorized access to private and proprietary information.[40] Overall, while certain DDLT applications are being used as disruptive wedges to the insurance industry, there are many others that can be viewed as supportive attempts to reshape the existing landscape.[41]

---

[38] *Id.* at. 03:47–05:19.

[39] Sritanshu Sinha, *Insurance Industry Eyes Blockchain as Top Firms Begin Tests*, COINTELEGRAPH (Dec. 24, 2019), https://cointelegraph.com/news/insurance-industry-eyes-blockchain-as-top-firms-begin-tests ("Blockchain technology is not a silver bullet, but rather a powerful new tool to drive data integrity, interoperability and traceability.").

[40] Daley, *supra* note 5; Martin, *supra* note 18; Paul Rogers, *How Blockchain is disrupting the insurance industry*, INTELLIGENTCIO (Dec. 20, 2019), https://www.intelligentcio.com/africa/2019/12/20/how-blockchain-is-disrupting-the-insurance-industry/ ("Currently, insurers struggle with inefficient exchange of information, complex liability assessments when it comes to reinsurance, fragmented data sources, the use of a middle-man and a manual driven claims review and process environment."); Charlie Wood, *AXA XL partners with insurtech Slice, Microsoft on cyber solution*, REINSURANCE NEWS (Dec. 13, 2019), https://www.reinsurancene.ws/axa-xl-partners-with-insurtech-slice-microsoft-on-cyber-solution/ (noting the goal of improving cyber resilience).

[41] Sinha, *supra* note 39 (second-largest health insurance company in the U.S. plans to leverage blockchain to secure medical data of members); Raj Shroff, *Blockchain in Insurance: Use Cases and Implementations*, MEDIUM (Aug. 21, 2019), https://medium.com/swlh/blockchain-in-insurance-use-cases-and-implementations-a42a00ebcd91. *Cf.* Russ Banham, *How Blockchain Is Disrupting 3 Industries*, RUSS

From a segmentation perspective, the insurance industry is best understood within three core pillars, life, health, and property & casualty business.[42] Thinking about the traditional insurance model, regardless of segmentation, individuals and organizations offer to be evaluated (underwritten) and pay premium in exchange for insurance policy protection from a third-party provider.[43] As a part of the process, insurance providers quote and accept business from desired insurance applicants, and if a covered event ensues, they adjust the matter and indemnify (or pay) the applicable individual or organization for his/her/their loss(es) above a retention (or deductible).[44]

With blockchain in mind, DDLT has the ability to make the transactional process associated with underwriting and sales more efficient and simplified.[45] For example, consider a life insurance transaction that permits an underwriter's ability to quickly unlock required medical information before issuing a quote to a customer.[46] As an alternative, how about accessing automated medical records in order to timely consider a health applicant's request for coverage.[47] Or finally, what about evaluating a vehicle's history in order to promptly respond to a request for auto insurance.[48] In each of these instances, there is the ability to utilize DDLT to obtain required information and engage in a much quicker turnaround time.

BANHAM (Mar. 27, 2019), https://www.russbanham.com/2019/03/27/how-blockchain-is-disrupting-3-industries/; *8 Blockchain Startups Disrupting The Insurance Industry* STARTUS INSIGHTS, https://www.startus-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-insurance-industry/ (last visited June 22, 2021).

[42] Brian Beers, *A Brief Overview of the Insurance Sector*, INVESTOPEDIA, https://www.investopedia.com/ask/answers/051915/how-does-insurance-sector-work.asp (Apr. 16, 2021).

[43] *Id.*

[44] *Id.*

[45] Shay Alon, *3 insurance underwriting predictions for 2020 and beyond*, ACCENTURE (Jan. 7, 2020), https://insuranceblog.accenture.com/3-insurance-underwriting-predictions-for-2020-and-beyond (blockchain and DDLT will be used to unlock underwriting efficiencies); Andrea Tinianow, *Insurance Interrupted: How Blockchain Innovation is Transforming the Insurance Industry*, FORBES (Jan. 9, 2019, 9:30 AM), https://www.forbes.com/sites/andreatinianow/2019/01/09/insurance-interrupted-how-blockchain-innovation-is-transforming-the-insurance-industry/#65be04813ec6.

[46] Martin, *supra* note 18.

[47] *Id.*

[48] KASKO2GO, https://kasko2go.com (last visited June 22, 2021).

Next, let us think about these same transactions within the context of claims. For starters, life insurance beneficiaries can be identified and paid in a transparent fashion using DDLT.[49] Further, health insurers can easily access treatment records from third-party providers in order to quickly pay policyholders for their medical visits.[50] Lastly, within the context of automobile insurance, once an insurable event occurs, DDLT can be used to upload photos and then external information can be utilized to verify an accident before reimbursement takes place.[51] Each of these incidents reinforces the open nature of blockchain and the swiftness associated with claim reimbursement payments.

In addition to business segmentation, it is equally important to appreciate blockchain's impact upon the insurance industry's ecosystem. There are certainly startups taking advantage of blockchain and DDLT to create an independent value proposition for competitive purposes.[52] At the same time, newer companies are actively partnering with insurance industry insiders in order to innovatively adapt blockchain and DDLT for the benefit of incumbents and their customers.[53] Beyond that, there are global leaders that are utilizing blockchain and DDLT in order to creatively solve for additional gaps in the industry.[54]

Beginning with a disruptive startup, Lemonade, an InsurTech unicorn headquartered in New York, utilizes artificial intelligence (AI) and DDLT to

---

[49] Steven Ehrlich, *MetLife Plans to Disrupt $2.7 Trillion Life Insurance Industry Using Ethereum Blockchain*, FORBES (June 19, 2019), https://www.forbes.com/sites/stevenehrlich/2019/06/19/metlife-plans-to-disrupt-2-7-trillion-life-insurance-industry-using-ethereum-blockchain/#5d3781dc2770 (MetLife is utilizing blockchain to add transparency and efficiency to the claims process); Martin, *supra* note 18.

[50] Leah Rosenbaum, *Anthem Will Use Blockchain To Secure Medical Data For Its 40 Million Members In Three Years*, FORBES (Dec. 12, 2019), https://www.forbes.com/sites/leahrosenbaum/2019/12/12/anthem-says-its-40-million-members-will-be-using-blockchain-to-secure-patient-data-in-three-years/?sh=435e59a06837 (Anthem will eventually use blockchain to process insurance claims and pay benefits faster); Shroff, *supra* note 41; Martin, *supra* note 18.

[51] KASKO2GO, *supra* note 48.

[52] Banham, *supra* note 41.

[53] Daley, *supra* note 5.

[54] *ABOUT* B3I, https://b3i.tech/home.html (last visited Feb. 5, 2021); Sian Barton, *InsurTech Futures: AXA Launches Automatic Compensation For Late Flights Product*, INSURANCEAGE (Sept. 20, 2017), https://www.insuranceage.co.uk/technology/3144031/insurtech-futures-axa-launches-automatic-compensation-for-late-flights-product.

competitively offer renters and homeowners insurance.[55] Thinking back to the peer-to-peer network component of blockchain generally, Lemonade offers peer-to-peer insurance (P2PI) to its customers via smart contracts and an innovative app and platform.[56] Customers can interface with a chatbot (instead of a human agent or broker) as a part of the insurance placement process in order to pool insurance premiums with other similarly situated customers.[57] Thereafter, Lemonade takes a fee, purchases reinsurance to protect the pool from catastrophic claims, and offers any returned premium to a customer's desired charitable organization.[58] By building a platform in this fashion, and utilizing smart contracts and AI, they reinforce: a simplified underwriting and sales process, efficiency, and very competitive premiums.[59] On the back-end of the transaction, if necessary, artificial intelligence is often used to pay out claims rapidly (e.g., three seconds).[60] As a part of the claims' adjustment process, however, Lemonade has also built market-leading fraud prevention and detection to avoid moral hazards.[61]

In addition to Lemonade, Kasko2Go, located in Switzerland, was the first to market with a fully blockchain-based automotive insurance solution.[62] Kasko assigns every vehicle with a unique identifier (link in an overall blockchain), and after an accident occurs, the policyholder uploads photos of the incident and the system uses public sources to verify the nature and extent of the event.[63] Key benefits associated with this type of platform are that claims are paid quickly, fraud is detected and prevented, and savings are ultimately passed on to customers.[64]

Turning to active support of the insurance industry, Guardtime is a global company with expertise in blockchain and cybersecurity.[65] They partnered with

---

[55] Sam Daley, *31 Blockchain Companies Paving The Way For The Future*, BUILT IN, (May 3, 2021), https://builtin.com/blockchain/blockchain-companies-roundup.

[56] *FAQ*, LEMONADE, https://www.lemonade.com/faq (last visited June. 25, 2021).

[57] *Id.;* LEMONADE, https://www.lemonade.com/?f=1 (last visited June 26, 2021).

[58] *FAQ*, *supra* note 56.

[59] *Id.*

[60] *Id.*; *CLAIMS,* LEMONADE, https://www.lemonade.com/claims (last visited June 26, 2021).

[61] *Id.*

[62] Emilia Picco, *Blockchain in Insurance Use Case #1: Kasko2go*, DISRUPTOR DAILY (May 17, 2019), https://www.disruptordaily.com/blockchain-insurance-use-case-kasko2go/.

[63] *Id.*

[64] *Id.*

[65] GUARDTIME, https://guardtime.com/ (last visited June 26, 2021).

Maersk to provide a blockchain-based maritime insurance platform.[66] The platform's benefits include the management of risk, the use of smart contracts, and most importantly, establishing an immutable chain-of-shipping for tracking purposes.[67] This helps marine insurers get comfortable providing insurance, and at the same time, it actively supports thousands of vessels pursuing maritime coverage.[68]

Another example of industry collaboration concerns Etherisc, a Zug-Switzerland-based insurance platform.[69] In July 2019, they launched a crop insurance product based upon a weather index in partnership with an international brokerage firm (Aon), an independent charitable organization (Oxfam), and an insurance company (Sanasa).[70] The product, referred to generally as parametric insurance, is actively supported with blockchain and DDLT.[71]

Lastly, insurance incumbents are appreciating the importance of blockchain, including DDLT abilities. For example, global insurance leader AXA, via its subsidiary Fizzy, piloted a market-leading flight delay insurance tool based upon blockchain.[72] The platform, which ensured that delayed flights beyond two hours were compensated, covered 80% of all worldwide flights.[73] Unfortunately, AXA concluded that the market was not sufficiently mature to support the ongoing business offering.[74]

Aside from Fizzy, The Blockchain Insurance Industry Initiative (B3i) reflects an ongoing alliance among global insurers to assess blockchain and DDLT applicability to the insurance industry.[75] Their first successful venture related to

---

[66] Daley, *supra* note 5.

[67] *Id.*

[68] *Id.*

[69] ETHERISC, https://etherisc.com/ (last visited June 26, 2021).

[70] *Etherisc, Aon and Oxfam in Sri Lanka on a Mission: to Expand Inclusive Insurance in Sri Lanka*, ETHERISC (Nov. 29, 2018), https://blog.etherisc.com/etherisc-aon-and-oxfam-in-sri-lanka-on-a-mission-to-expand-inclusive-insurance-in-sri-lanka-696b51c98d9b.

[71] *Id.*

[72] *AXA Goes Blockchain with Fizzy*, AXA (Sept. 13, 2017), https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy.

[73] Daley, *supra* note 5.

[74] Elliot Hill, *AXA Drops Ethereum-Based Flight Insurance Platform*, COIN RIVET (Nov. 10, 2019), https://coinrivet.com/axa-drops-ethereum-based-flight-insurance-platform/.

[75] *ABOUT B3i*, B3I SERVICES, https://b3i.tech/home.html (last visited June 26, 2021).

property reinsurance contracts, all of which were fully executed on a secure blockchain.[76] To date, thirty (30) contracts have been completed on B3i's platform.[77]

IV. LEGAL AND CONNECTICUT–BASED LEGISLATIVE DEVELOPMENTS

With a better understanding of blockchain and DDLT applications to insurance, let us move next to legal (including Connecticut-specific legislative) developments. In order to do so, as a refresher, smart contracts ensure that parties are able to transfer something of value without the need of an intermediary.[78] Mechanically, within the insurance context, this might include an insurance policy that is written as a coded, decentralized smart contract.[79] Such a contract establishes that a policyholder would pay a specific insurance premium in exchange for insurance policy protection.[80] Overall, this type of transaction raises several potential legal issues to consider, and as a result, obtaining legal advice from an experienced blockchain attorney is advisable.[81]

First, it is questionable whether a smart contract's terms and conditions can be sufficiently captured with code in order to ensure proper contract formation.[82] Stated differently, a smart contract might not be sufficiently broad to capture the true intent of the parties to a particular agreement.[83] One potential solution might be to combine blockchain's coding capabilities with the natural language contained in a traditional, written contract.[84] In fact, the traditional contract can be stored off the

---

[76] Daley, *supra* note 5.

[77] *Major Re/Insurers and Brokers Complete Complex Placements on B3i's Blockchain Platform*, B3i (Feb. 12, 2020), https://b3i.tech/news-reader/major-re-insurers-and-brokers-complete-complex-placements-on-b3is-blockchain-platform.html.

[78] Nigel Gopie, *What are Smart Contracts on Blockchain?*, IBM: BLOCKCHAIN PULSE (July 2, 2018), https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/.

[79] *Id.*

[80] Beers, *supra* note 42.

[81] McKinlay, *supra* note 6; Security Token Academy, *Legal and Regulatory Issues Relating to Smart Contracts and Blockchain*, YOUTUBE, at 2:05 (Sept. 5, 2018), https://www.youtube.com/watch?v=O4CkxYRs3e4.

[82] Bird & Bird, *Blockchain and the Legal Issues*, YOUTUBE, at 3:04-3:25 (Feb. 14, 2019), https://www.youtube.com/watch?v=t7TCrZ76BWs.

[83] *Id.*

[84] *Id.* at 04:09

blockchain but properly linked with a hash secure value to reinforce confidence that the final version is the one being relied upon by the parties.[85] This type of approach adds an additional advantage associated with blockchain's digital timestamp capabilities.[86]

Second, assuming successful contract formation, there are also questions about jurisdiction and applicable law.[87] With multiple nodes across the blockchain platform, there are potentially different places to enforce liability under a smart contract with distinct legal expectations.[88] That raises additional issues for the parties and courts to grapple with while overseeing legal proceedings.

Lastly, the parties to a smart contract will need to appreciate how the specific governance framework might work in advance of a dispute. For example, in the private blockchain context, there is likely to be a software development agreement between the developer and client.[89] Beyond that, terms of use might be instructive for the parties, including for user/developer and user/user arrangements.[90]

With regard to Connecticut-specific legislative developments,[91] Connecticut continues to be in its infancy stages with blockchain exploration.[92] Not

---

[85] Simply Explained, *supra* note 21, at 03:57.

[86] O'Connell, *supra* note 7.

[87] Security Token Academy, *supra* note 81, at 00:23.

[88] *Id.* at 02:13-02:20.

[89] Bird & Bird, *supra* note 82, at 02:11-02:15.

[90] *Id.* at 02:28-02:32.

[91] Heather Morton, *Blockchain 2019 Legislation*, NAT'L CONF. OF STATE LEGISLATURES (July 23, 2019), https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx (noting that beyond Connecticut, as of mid-year 2019, there were at least twenty-seven additional states that introduced legislation relating to blockchain and a large percentage of the resolutions were enacted and adopted).

[92] *How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact Its Adoption*, BUS. INSIDER (Jan. 27, 2021), https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global (noting that "the federal government has not exercised its constitutional preemptive power to regulate blockchain to the exclusion of states [as it generally does with financial regulation], thereby leaving individual states free to introduce their own rules and regulations"); *Cf.* Brandi Vincent, *Advancing Blockchain Act Calls for Federally-Led Deep-Dive Into the Nascent Tech*, NEXTGOV (May 29, 2020), https://www.nextgov.com/emerging-tech/2020/05/advancing-blockchain-act-calls-federally-led-deep-dive-nascent-tech/165775/ (suggesting recently introduced legislation to potentially mandate an exhaustive federal government-led examination of blockchain in the U.S. and abroad).

surprisingly, the first step in assessing blockchain fit is often forming a taskforce to research potential applicability.[93] In Connecticut, SB443 was unanimously passed in 2018 to do so and it was signed into law on June 6, 2018.[94] The law ensured that a dedicated group was established to evaluate how Connecticut could be a leader in blockchain technology.[95] It charged the group with four areas of potential exploration, including:

> (1) The identification of growth areas associated with blockchain technology;
> (2) The ability to assess Connecticut's industry sectors for potential blockchain applicability;
> (3) Reviewing industry and academic needs for furthering blockchain knowledge across business sectors; and
> (4) Making blockchain legislative recommendations to promote an innovative environment that supports economic growth.[96]

Approximately nine months after Connecticut's initial blockchain group was formed, they shared four (4) different proposed bills for consideration. First, HB7310 related to the authorization of smart contract usage in commerce across the state.[97] Second, HB7309 concerned allowing notaries to perform electronic and remote notarial acts.[98] Third, SB1032 proposed engaging in a pilot program in connection with the administration of a Connecticut department function.[99] Fourth, and finally, SB1033 suggested that non-compete agreements be prohibited in connection with the blockchain technology industry.[100] Overall, while each of the

---

[93] Christopher Adcock, *An Update on State Smart Contract Legislation*, HUNTON ANDREWS KURTH (Apr. 15, 2020), https://www.blockchainlegalresource.com/2020/04/an-update-on-state-smart-contract-legislation/.

[94] *Connecticut Blockchain Working Group Being Formed by Governor (SB 443)*, BITCOIN EXCH. GUIDE (June 10, 2018), https://bitcoinexchangeguide.com/connecticut-blockchain-working-group-being-formed-by-governor-sb-443/.

[95] *Id.*

[96] *Id.*

[97] Emily Denaro, *Blockchain Legislation Testimony Delivered at CT State Capitol by Chateaux's Nick Kammerman,* CHATEAUX (last visited June 26, 2021), https://chatsoft.com/blockchain-connecticut-testimony/.

[98] *Id.*

[99] *Id.*

[100] *Id.*

proposed bills was discussed at a public hearing, and referred to joint committee for further consideration, they have not been adopted by Connecticut as a matter of law.[101]

V. CYBERSECURITY CONSIDERATIONS

Notwithstanding the status of Connecticut's legislative posture concerning blockchain, it can certainly be used to better prevent data security breaches.[102] In fact, while a centralized system stores information in one place and draws the interest of hackers, blockchain's decentralized model makes it more difficult for cyber criminals to successfully attack.[103] Beyond the decentralized make-up, encryption can be used to ensure that data is not accessible to external parties.[104] Furthermore, biometrics can be incorporated to ensure that access is based upon fingerprint or retina scanning technology.[105] While centralized systems need to be concerned with the possibility of a denial of service attack, integrating blockchain to an organization's security posture can lessen that possibility – since there is no ongoing centralized attack point to repeatedly go after.[106] Lastly, while IoT devices are often manufactured and sold with limited consideration for security, smart contracts can be used to manage IoT activities and keep the devices more properly secure.[107]

---

[101] H.B. 7310, 2019 Gen. Assemb., Reg. Sess. (Conn. 2019); H.B. 7309, 2019 Gen. Assemb., Reg Sess. (Conn. 2019); S.B. 1032, 2019 Gen. Assemb., Reg. Sess. (Conn. 2019); S.B. 1033, 2019 Gen. Assemb., Reg. Sess. (Conn. 2019).

[102] Andrew Arnold, *4 Promising Use Cases of Blockchain in Cybersecurity*, FORBES (Jan. 30, 2019), https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/#1ddbd9ca3ac3.

[103] Sam Mire, *What Are the Benefits of Blockchain In Cybersecurity? 6 Experts Share Their Insights*, DISRUPTOR DAILY (May 5, 2019), https://www.disruptordaily.com/benefits-of-blockchain-cyber-security/.

[104] Kirill Yusov, *Use of Blockchain in Cybersecurity – the 2020 Perspective*, JELVIX, https://jelvix.com/blog/blockchain-cybersecurity-predictions (last visited June 26, 2021).

[105] Sam Daley, *Wallets, Hospitals and the Chinese Military: 19 Examples Of Blockchain Cybersecurity at Work*, BUILT IN (Apr. 6, 2020), https://builtin.com/blockchain/blockchain-cybersecurity-uses.

[106] John Ocampos, *Contribution of Blockchain to Cybersecurity*, BLOCKCHAIN LAND (Mar. 23, 2020), https://theblockchainland.com/2020/03/23/contribution-blockchain-cybersecurity/.

[107] *Id.*

While there are certainly many strengths associated with blockchain, there are also potential weaknesses to keep in mind. These weaknesses are often outside of the direct context of blockchain and include human and third-party elements. For example, there is the potential for hackers to target and actively pursue blockchain keys directly from users.[108] These might be stored on lesser-protected personal computers, workstations, and even mobile devices.[109] Relatedly, companies often partner with third-party service providers in order to run their operations. These types of partners can expose transactions due to inconsistent coding, weak credentials, and poor security and privacy best practices.[110]

For certain, the human element and third-party vendor relations raise several aspects to think about while managing a viable blockchain posture. In order to overcome theft of keys, personal and organizational systems should be maintained with appropriate antivirus and malware scanning protection and encryption should be independently contemplated.[111] Lastly, it is important to partner with experienced vendors that take their security and privacy postures seriously and are open to being vetted as a part of the collaborative process.[112] This might include considering contract management to address the potential for indemnification via contract.[113]

VI. SUMMARY AND CONCLUSIONS

Blockchain and DDLT are being innovatively implemented in various sectors of insurance, including the industry's overall ecosystem. While test-use cases are rapidly developing, ongoing consideration should be given to legal, Connecticut-based legislative, and cybersecurity dynamics.

---

[108] *Exploring the Security Weaknesses of the Blockchain*, TECHBULLION (Sept. 25, 2018), https://techbullion.com/exploring-the-security-weaknesses-of-the-blockchain/.

[109] *Id.*

[110] *Id.*

[111] Rick Martin, *5 Blockchain Security Risks and How to Reduce Them*, IGNITE (Nov. 29, 2018), https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/.

[112] Teresa Meek, *Outsourcing Cybersecurity: When And How To Bring In Contractors*, FORBES (May 27, 2017), https://www.forbes.com/sites/eycybersecurity/2017/03/27/outsourcing-cybersecurity-when-and-how-to-bring-in-contractors/#412bb0e26ca1.

[113] Matt Schwartz, *Using Contracts to Curb Cyberrisks*, RISK MGMT. (May 1, 2017), http://www.rmmagazine.com/2017/05/01/using-contracts-to-curb-cyberrisks/.

This paper initially explored the definition of blockchain and highlighted its origins and diverse purposes, including the ability to maximize distributed ledger technology. It also assessed blockchain and DDLT within the context of insurance, including its potential applications to life, health, and property & casualty business. Beyond that, the paper shared examples of how blockchain and DDLT are being used to disrupt and/or support the insurance ecosystem. Lastly, it addressed diverse issues of importance while using blockchain relating to the law, CT-based legislative initiatives, and preventing unauthorized access to private and proprietary information.

WHEN IS A CYBER INCIDENT LIKELY TO BE LITIGATED AND HOW MUCH WILL IT COST? AN EMPIRICAL STUDY

JAY P. KESAN*
LINFENG ZHANG**

ABSTRACT

Numerous cyber incidents have shown that there are substantial legal risks associated with these events. However, empirical analysis of the legal aspects of cyber risk is largely missing in the existing literature. Based on a dataset of historical cyber incidents and cyber-related litigation cases, we provide one of the earliest quantitative studies on the likelihood of cyber incidents being litigated and the cost of settling a cyber-related case. Using regression models, we showed that some company and incident characteristics play an important role in determining the litigation probability and settlement costs for which our models propose a useful explanation. Our findings show that the lack of Article III standing is commonplace in cyber-related cases, and that solely relying on the common law system makes it difficult for victims of malicious data breaches to sue and receive legal remedies. In addition, we demonstrate that our findings have valuable implications for enterprise risk management in terms of how the legal risk associated with different types of cyber risk should be properly addressed.

TABLE OF CONTENTS

* College of Law, University of Illinois at Urbana-Champaign. Email: kesan@illinois.edu

** Department of Mathematics, University of Illinois at Urbana-Champaign. Email: lzhang18@illinois.edu

We would like to thank Daniel Schwarcz and the other participants at the Cyber Insurance Conference, jointly organized by the University of Connecticut and the University of Minnesota, for their insightful comments and suggestions.

I. INTRODUCTION

Organizations in both the private and public sectors face new challenges with the emergence of cyber risk, which are not limited to investing in security and implementing those measures. Because cyber risk cannot be eliminated,[1] almost inevitably, an organization will have to deal with the outcomes of a cyber incident at some certain point. A cyber incident can typically lead to various types of losses, and legal cost is one of the most prevalent losses.[2] In addition, lawsuits are costly, and because many cyber insurance policies provide coverage for legal expenses,[3] oftentimes insurers and policyholders will need to share these costs. NetDiligence[4] provided an analysis on historical insurance claims and showed that within the five-year period from 2015 to 2019, for small and medium enterprises, the average cost of legal defense was $61,000 and the average cost of settlement was $134,000. For large companies, the average defense cost was $1.4 million, and the average settlement cost was $2.6 million.[5] Those costs constitute a significant proportion of the total costs of an incident. Therefore, it is

---

[1] *See* Ranjan Pal & Pan Hui, *The Impact of Secure OSs on Internet Security* What Cyber-Insurers Need to Know (2012), https://arxiv.org/abs/1202.0885.

[2] Jay P. Kesan & Linfeng Zhang, *Analysis of Cyber Incident Categories Based on Losses,* 11 ACM TRANSACTIONS ON MGMT. INFO. (2020).

[3] *See*, Sasha Romanosky, Lillian Ablon, Andreas Kuehan & Therese Jones, *Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 6 (2019).

[4] NETDILIGENCE, CYBER CLAIMS STUDY 2020 REPORT 10 (2020), https://netdiligence.com/cyber-claims-study-2020-report.

[5] *Id.*

certainly of interest to companies and their insurers to understand what types of cyber incidents are likely to be litigated and how much they are likely to cost.

However, not all cyber incidents will result in lawsuits, and it is not clear what factors are driving the litigation of cyber incidents. That is, when is a cyber incident likely to be litigated? The answer to this question has many applications. For example, Romanosky, Hoffman, and Acquisti found that incidents which affect personal financial information (PFI) have a particularly high probability of resulting in federal lawsuits, and thus, we may expect that companies which hold a large amount of PFI will bear a higher legal risk than those that do not.[6] This information can be useful by those companies to prioritize the protection of customers' PFI to avoid high legal risk. It can also be used by insurers for a more accurate assessment of clients' risk exposures, thus pricing cyber insurance products more fairly. Romanosky, Hoffman, and Acquisti also identified several other factors, which will be discussed in Section 2.1.[7]

In this study, with a similar goal of shedding some light on this question, we try to identify more key factors that affect the probability of a cyber incident being litigated with an expanded scope. In terms of the definition of cyber risk, we follow the one given by Cebula and Young, which states that cyber risks are "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.*"[8] Therefore, we consider a variety of cyber incidents, including privacy violations, malicious data breaches, and non-data-related incidents that only affect the functionality of information systems, as distributed denial-of-service events.

For the first part of this study, we examined a collection of historical cyber incidents. Some of the incidents are litigated, and the rest of them are not. By regressing a set of explanatory variables against the odds of litigation in logistic regression models, we find that many factors (including the incident type, loss of personal sensitive information (*PSI*), number of breached records, company size, and company type) play significant roles in determining the probability of litigation, and some of them are more influential than the others. We also find that there are many significant

---

[6] Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, J. EMPIRICAL L. STUD. 3 (2013).

[7] *Id.*

[8] James J. Cebula, Mary E. Popeck & Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks Version 2*, SOFTWARE ENG'G INST. 1, 16 (2014).

interaction effects between those explanatory variables. They reveal that the characteristics of a cyber incident may have different impacts on companies of different sizes and types. For example, the number of breached records in a malicious data breach event will increase the litigation probability, but the amount of the increase is different between small and large companies.[9]

For the second part, we examined the dismissal rate and settlement costs of litigation arising from cyber incidents. Our findings show that many cases associated with privacy violations and malicious data breaches are dismissed because of a lack of Article III standing. Moreover, we have identified a set of explanatory variables that have a significant impact on the cost of settlement, including the type of incident, the number of records affected in privacy violations and malicious data breaches, the company type, and the type of legal action (*i.e.*, class action or individual). There are also some pairwise interaction effects that are worth mentioning.

Our contribution to the literature is threefold. First, in terms of identifying a set of significant explanatory variables, we provide a cross-validation to those variables that have been studied previously by other scholars and offer the results from a formal statistical test of those variables that have been hypothesized, but not tested before. Our findings offer additional, specific insights into the question, "when is a cyber incident likely to be litigated?" Second, we are not aware of any previous empirical studies that have discussed the interaction effects of those explanatory variables. This discovery justifies the adoption of predictive models that allow for interaction effects, and thus can be especially useful for insurers and insurtech companies to improve their existing models. Third, this is the first study to provide a quantitative model of the settlement costs of cyber-related litigation cases. The model offers some useful insights into the legal risk of cyber incidents, and how it should be properly taken into account.

The overall organization of this Article is as follows. In Part 2, we provide an extensive analysis of the litigation probability of cyber incidents based on a dataset of historical cyber incidents and their associated lawsuits. In Part 3, we take a closer look at the outcomes of litigated cyber incidents in terms of their dismissal rate and then propose a linear model that explains the settlement costs of cyber-related lawsuits. Finally, we offer a discussion of the limitations of this study in Part 4 and conclude our findings in Part 5.

---

[9] *See infra* Section 2.5.3.

II. CYBER LITIGATION PROBABILITY

A. HYPOTHESIZED FACTORS RELATING TO CYBER LITIGATION IN LITERATURE

Some studies have already tested or hypothesized several factors that are important in determining whether or not a cyber incident will develop into a lawsuit. In Romanosky, Hoffman, and Acquisti, factors considered include:

- the type of information that is breached, including social security numbers, medical records, financial records, and credit card information;
- whether the breach is caused by improper disclosure of information or by hacking,
- the number of breached accounts;
- whether or not there is any presence of actual harm;
- whether or not any credit monitoring services are provided after the breach.[10]

In this study, because we use a different data set, we believe it is worthwhile to revisit those variables in our study. However, because of the difference in the datasets used, some information is not available or compatible with the data we have, including information on the presence of actual harm and credit monitoring services provided after data breaches.[11]

---

[10] Romanosky et al., *supra* note 5, at 9–10.

[11] *Id.* at 16. For litigated cases, evidence of actual harms is found in the complaints, but for cases that are not litigated, information about actual harms is collected from news articles. For a particular case that is not litigated, if no financial loss is mentioned in relevant news articles, then it is considered to have no actual harm. However, we hesitate to take the same approach because it is difficult to guarantee the accuracy and consistency of data collected from different sources using different methods. Therefore, for this study we simply disregard this factor, and will possibly perform another study to address this issue, if there is better data in the future.

In addition, inspired by Brickley, Lu, and Wedig,[12] we study how the size of an organization affects the probability of it being a target in a lawsuit. Brickley, Lu, and Wedig is not particularly about cyber incidents, but it observes that when there is a rise in tort liability litigation, deep-pocketed nursing homes are more likely to shield their assets by selling them to judgment-proof buyers (such as small chains and independent owners, especially those who are not insured) because they are less attractive to plaintiffs, and exposed to smaller tort liability. In this study, we are mostly interested in finding out whether large companies are more likely to be the targets of lawsuits after cyber incidents.[13]

Moreover, as mentioned in Hooker and Pill , there are four common types of cybersecurity litigation, including shareholder derivative actions, securities fraud class actions, customer class actions and federal regulatory actions.[14] The first two types both relate to losses in stock value and unhappy shareholders.[15] In a shareholder derivative action, shareholders claim that the company failed to take adequate measures to safeguard against cyber incidents and bring suits against executives or board members. In a securities fraud action, shareholders contend that the company has misrepresented its preparedness against cyber attacks. Given these lawsuits concern shareholders' interest, we hope to investigate if there is empirical evidence for the hypothesis that public companies are more likely to be sued after cyber incidents.

To summarize, the variables that we will investigate in this study include:

- Incident characteristics
  - the type of breached information,
  - the type of cyber incidents,
- Company characteristics
  - the number of affected records in a data breach,
  - the size of the affected organization,

---

[12] James A. Brickley, Susan F. Lu & Gerard J. Wedig, *Malpractice Laws and Incentives to Shield Assets: Evidence from Nursing Homes*, 14 J. EMPIRICAL LEGAL STUD. 301, 319 (2017).

[13] *Id*. at 306–307.

[14] Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FL. BAR J. 30, 31–32 (2016).

[15] Id.

- whether or not the affected organization is a publicly traded company.

If we look at these variables at a higher level, they can be put into two categories. One category includes the intrinsic characteristics, such as size and type, of the company that gets hit by a cyber incident. The other category contains descriptions of characteristics of the incident, including the type of incident, the type of impacted data, and the size of the impacted data. We will see later that companies with different intrinsic characteristics, and that experience different types of cyber incidents, will have different probabilities of getting involved in lawsuits.

Another variable corresponds to the violation of data-related and/or privacy laws and regulations, such as the Fair Credit Reporting Act (FCRA) and the Fair Debt Collection Practices Act (FDCPA), and we want to study how such a violation would affect the probability of litigation. In most cases, if an organization is found to be violating some specific law/regulation, the corresponding enforcer would bring charges against the organization. For example, in *Federal Trade Commission v. Equifax, Inc.*, the Federal Trade Commission charged Equifax, Inc. for the violation of the FTC Act and the Gramm-Leach-Bliley Act in a well-known massive data breach in 2017 that affected the personal information of over 147 million Americans.[16] Although this variable seems promising in predicting lawsuits, we cannot study the influence of this variable on litigation probability because virtually all the litigated cases in our sample involve the violation of some specific laws or regulations.

Thus far, we have provided a list of explanatory variables for predicting lawsuits that follow cyber incidents. In addition, we include variables to control for year and industry fixed effects. A detailed account on each of the variables will be provided in the following section about the dataset that we use for this study. Then, using those variables, we will present a collection of logistic regressions, which aim to help identify significant factors that can impact the probability of litigation, and we will focus on analyzing the effect of each variable.

[16] *In re* Equifax, Inc., 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

B. DATA AND SUMMARY STATISTICS

For this study, we acquired a dataset of historical cyber incidents from Advisen Ltd.,[17] which is a data collector specializing in data for the insurance industry.[18] The dataset that we received has its latest update in late 2018, and thus there is no information on the incidents that occurred in the past two years.[19] The data is extensive and contains over 100,000 records, which is sufficient for the purpose of this research. Each of the observations has the information on a cyber incident that occurred in the past, along with information on the affected organization, the nature and impact of the incident, and most importantly, information about the lawsuit that followed, if any.

Of course, not all observations and variables are relevant, and thus, we first subset this dataset according to the scope of this study. We first limit our focus to incidents and lawsuits that took place in the US, for reasons including:

- The legal environment in different countries may not be comparable. In the United States, there are cybersecurity and privacy laws and regulations that may not have similar counterparts in other places of the world. Therefore, to control for the legal environment, we need to treat different countries separately.
- The data set we have is imbalanced. It has more than 87% of the incidents from the U.S., and the remaining cases are spread out across over 160 countries and regions. Note that there are significantly more cases in the U.S. mainly because the data collector is based in the U.S., and information about cyber incidents from U.S. sources is more accessible. Therefore, this disproportionate number of U.S. cases is only a result of selection bias.

In addition, the earliest incident in this dataset can be traced back to 1903, which is hardly relevant to how cyber cases are perceived and

---

[17] *Cyber Loss Data*, ADVISEN, https://www.advisenltd.com/data/cyber-loss-data [hereinafter *Cyber Loss Data]* (last visited Apr. 20, 2021).

[18] ADVISEN, https://www.advisenltd.com (last visited Apr. 20, 2021).

[19] *2018 Data Set Name*, ADVISEN (Apr. 11, 2021), https://www.advisenltd.com/data/cyber-loss-data.

regulated nowadays. To create a more relevant sample, we focus only on those incidents that occurred in and after 2000.

One additional data processing procedure we have to perform is grouping observations that are related--in the sense that for a single incident, there might be multiple records. In that case, some of the records solely concern the nature of the incident, such as the number of affected accounts in a data breach, whereas the other records have information about further actions that are found, such as lawsuits arising from that cyber incident. This can be done with the common identifier shared by related observations. For this reason, the number of observations corresponding to individual cyber incidents that is left in our data is substantially smaller than the original dataset size. In addition, many observations do not have a known number of breached records, which is a variable of interest to this study. Some of those missing values cannot be safely imputed, and thus those observations are removed from the sample. This point will be elaborated when discussing the variable for the number of breached records. These filtering criteria result in 24,896 observations in total. Next, we will provide detailed descriptions about those explanatory variables as well as the response variable.

1. Litigated or Not? – LITIGATED

The response variable in this study is whether or not there is a lawsuit associated with a cyber incident. All documented court cases are provided with docket numbers in the original dataset, and that helps us identify which of the incidents are litigated. Because docket numbers are publicly accessible, it is reasonable to assume that those incidents without corresponding docket numbers did not result in lawsuits. Therefore, we create a binary variable named *LITIGATED* based on the column of docket numbers. For those incidents with known docket numbers, *LITIGATED* takes the value of 1 and for those no associated with docket numbers, *LITIGATED* takes the value of 0.

Among all 24,896 observations, there are 21,094 litigated cases, and the remaining 3,802 incidents are not associated with known lawsuits. The data is moderately imbalanced with a litigated-to-not-litigated ratio of approximately five to one. Note that this ratio does not represent the actual probability of cyber incidents being litigated. There are more cases being litigated in our dataset than not. This is most likely because litigated incidents have more publicity, thus causing a sampling bias that favors incidents with known lawsuits. In addition, it is almost impossible to get a reliable estimate

on the probability of litigation because it depends on the premise that we can know the total number of all cyber incidents in a given time period. Due to the large volume of unreported incidents,[20] that information is unlikely to be observable. Therefore, instead of obtaining an accurate estimation of the probability of litigation, this study focuses on identifying factors that have significant impacts on that probability and building a relatively reliable classifier that has better performance than baseline models--such as a dummy classifier that always predicts the majority class.

2. Loss of Personal Sensitive Information – PSI

The first explanatory variable we will investigate is whether or not there is personal sensitive information, including personally identifiable information, personal financial information, and personal health information, involved in a cyber incident. Romanosky, Hoffman, and Acquisti found that the breach of either medical records or financial information will increase the probability of an incident being litigated at the federal level, and thus in this study, we would expect to see similar findings.[21] In the original dataset, more detailed information is given on the type of assets damaged in an incident, such as various types of sensitive personal information (*PSI*), corporate information, and several types of physical assets. We are mostly interested in the comparison between incidents with and without *PSI* involved, and thus create a binary variable named *PSI*, which takes the value of either 0, which represents that there is no *PSI* affected, or 1, for the involvement of *PSI*.

In the sample, 24,008 observations involve the breach of personal sensitive information, and the remaining 888 do not. To get a heuristic impression on the relationship between *PSI* and the probability of an incident being litigated, we create Table 1, which is a two-way table that shows the number of observations in each combined class based on *PSI* and *LITIGATED*. Because *PSI* and *LITIGATED* each have two sub-classes, there are four combined classes in total. We also provide the percentages calculated based on the total number of observations in each *PSI* class. For example, when *PSI* = 0, (*i.e.*, there is no personal sensitive information

---

[20] *See Cyber Security: Underpinning the Digital Economy*, INST. DIRS. 19 (Mar. 2016),

https://www.iod.com/Portals/0/Badges/PDF's/News%20and%20Campaigns/Infrastructure/Cyber%20security%20underpinning%20the%20digital%20economy.pdf?ver=2016-04-14-101230-913.

[21] Romanosky et al., *supra* note 6, at 12, 17.

involved) 9.1% of the incidents have resulted in lawsuits, and the remaining 90.9% have not. Because of the potential sampling bias, these percentages are shifted, and the true litigation probability of incidents that affect *PSI* may not be as high as ninety percent. But relatively speaking, from this table, we observe that when *PSI* is involved, the probability of litigation is likely to be much higher compared to the scenario in which no *PSI* is affected. This justifies the inclusion of *PSI* as an insightful explanatory variable.

For the reason that more than ninety-six percent (24,008/24,896) of the observations in this sample have personal sensitive information involved, the proportion of litigated cases in the entire sample (21,094/24,896 = 84.7%), as we saw earlier, is close to the proportion of litigated cases in the *PSI=1* class (87.5%). Despite such a large imbalance, there are sufficient numbers of observations in both classes, and thus they can still be effectively compared, and the impact on estimating the effects of *PSI* is minimal.

		LITIGATED=0	*LITIGATED=1*	*TOTAL*
PSI=0	Percentage	90.9%	9.1%	100.0%
	Count	807	81	888
PSI=1	Percentage	12.5%	87.5%	100.0%
	Count	2995	21013	24008

Table 1: Two-way table of *PSI* and *LITIGATED*. Percentages are calculated based on the total number of observations in each *PSI* class.

3. Type of Cyber Incidents – ITYPE

Because this study concerns not only the leak of data, but also other types of cyber incidents--malicious data breaches caused by hacking,[22] we also include one more category for those incidents that are not related to the breach of confidential information, such as cyber system malfunctioning caused by IT implementation errors. The type of incident is represented by a variable named *ITYPE* with three possible values, including **PV**, **DB** and **ND**, to represent privacy violations caused by organizations improperly disclosing or collecting confidential information (**PV**), malicious data breaches caused by organizations being hacked by attackers (**DB**), and incidents that are not data breaches (**ND**). These three categories of cyber

[22] *Id.* at 12–13.

incidents are mutually exclusive in this study. This information is inferred from the sixteen types of cyber incident in the original dataset, and they are put into three broader categories in line with the method proposed in Kesan and Zhang.[23]

Similarly as before, we report a two-way table of *ITYPE* and *LITIGATED*, as shown in Table 2. From this table, we can see that this variable suffers from the same issue as *PSI* and has imbalanced classes. Observations in the **PV** class account for over 80% (20,133/24,896) of the sample, and most of them (98.8%) lead to litigation. Likewise, given an adequate number of observations in each class, the impact on coefficient estimation and the analysis on the effect of each class should be small, but it makes it problematic to use this sample for training predictive models.

		LITIGATION=0	LITIGATION=1	TOTAL
ND	Percentage	87.3%	12.7%	100.0%
	Count	2365	344	2709
DB	Percentage	57.9%	42.1%	100.0%
	Count	1189	865	2054
PV	Percentage	1.2%	98.8%	100.0%
	Count	248	19885	20133

Table 2: Two-way table of *ITYPE* and *LITIGATED*. Percentages are calculated based on the total number of observations in each *ITYPE* class.

4. Number of Breached Accounts – BSIZE

Romanosky, Hoffman, and Acquisti found that the number of records breached in a cyber incident increases the possibility of the incident being federally litigated.[24] In this study, the same variable, denoted by *BSIZE* is included in our models. Since we use a different dataset than Romanosky et al., our findings provide a cross-validation of their results. This is the only variable in our sample that has a significant missing rate. We took a careful approach to impute or remove those missing values, which is described in detail in Appendix C.

Because the number of breached records only matters for data breaches and privacy violations, we will focus on how that number affects

[23] Kesan & Zhang, *supra* note 2, at 13–16.

[24] *See* Romanosky et al., *supra* note 6, at 9–17; see also Appendix A.

the probability of litigation in an incident that belongs to either of those two classes. Table 3 provides the summary statistics of *BSIZE* on a log scale,[25] and we can see that it distributes differently in **PV** class and **DB** class. For data breach events, usually the number of impacted records is much higher than that in a privacy violation event if we compare their means and quantiles. This is because most of the privacy violation incidents in our sample are those caused by companies disclosing or collecting the information of only a few individuals, such as hospitals sending health records to wrong recipients, but in malicious data breach events, attackers usually have the intent to unlawfully acquire a large amount of data for a large enough financial gain.

[25] Because many of the values are 0, before taking the logarithm, all values are shifted by 1. For example, if there is only one record affected, the number on a log scale is log(1 + 1) = 0.69, instead of 0.

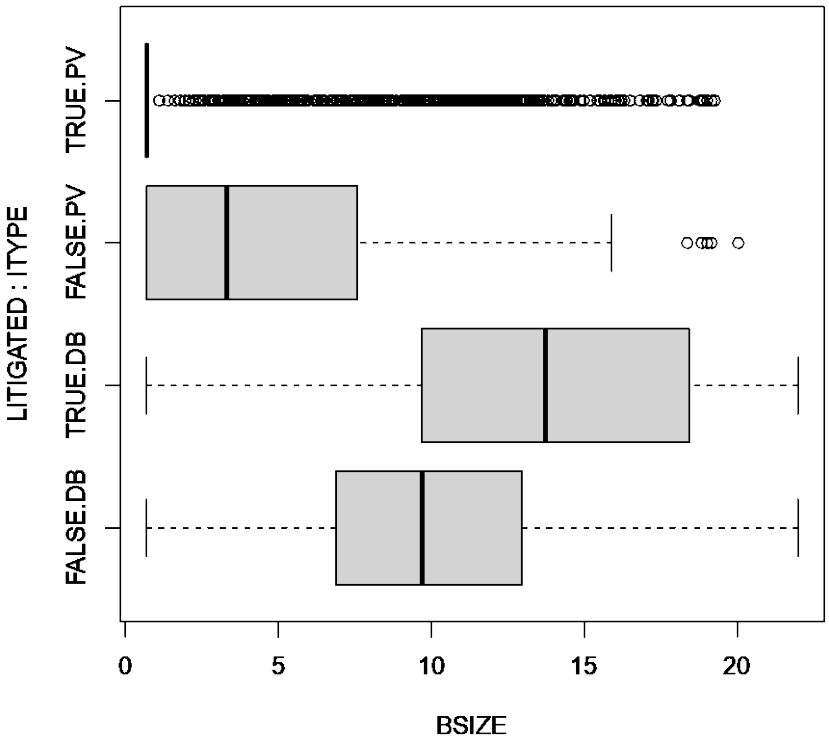


Figure 1：Box plot of *BSIZE* plotted against *LITIGATED* and *ITYPE*.

The distribution of *BSIZE* in different classes of cyber incidents and its relationship with litigation rate is visualized in Figure 1. This box plot shows that in litigated privacy violation incidents, most of the breach sizes are extremely small, thus causing many breaches that are moderately large to lie outside the rightmost whisker. For privacy violation incidents that are not litigated, the distribution of their breach sizes is less skewed, with only a few large cases lying outside the rightmost whisker. In contrast, the distribution of breach size in malicious data breach events is more balanced.

	Summary Statistics of *BSIZE*					
	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
PV	0.69	0.69	0.69	1.88	0.69	20.03
DB	0.69	7.26	11.24	11.25	15.32	21.98
PV&DB	0.69	0.69	0.69	2.75	1.39	21.98

Table 3：Summary statistics of *BSIZE* on a log scale of observations in **PV** (privacy violation), **DB** (data breach), and combined (privacy violation and data breach) classes.

5. Size of Company – CSIZE

For the definition of a large company large, we refer to the table compiled by the U.S. Small Business Administration,[26] which determines whether or not a company is counted as a small business based on its industry and annual revenue or number of employees. However, we do not strictly follow this definition for reasons including the following:

- The purpose of this table is to specify which companies are eligible for participating in government contracting programs that are reserved for small businesses. In addition, the standard of small businesses changes over time and is a complicated issue.[27] From time to time, the legislative definition of small businesses changes depending on macroeconomics and other variables that are important to determine who should be eligible for small business compensation. Those considerations have little to do with the questions we are trying to investigate in this paper.
- For some industries, the size of a business is defined by its annual revenue, whereas for others, the size of a business is defined by its number of employees.[28] Given

[26] U.S. Small Business Administration, Table of Small Business Size Standards Matched to North American Industry Classification System Codes (Aug. 19, 2019), https://www.sba.gov/sites/default/files/2019-08/SBA%20Table%20of%20Size%20Standards_Effective%20Aug%2019%2C%202019_Rev.pdf.

[27] *Id.* at 1.

[28] *See generally id.*

> that in our data set, although there is a column of annual revenues and a column for numbers of employees, they both have a considerable number of missing values, and this missingness does not always occur simultaneously in those columns. For example, we may only have information on the number of employees of a specific company but not its annual revenues. Given the industry the company operates in, whether it is considered small, however, is determined by its annual revenue. In that case, if we strictly follow the definition given by SBA, we cannot determine whether that company is small or not. The consequence is that the missingness issue is worsened.

Therefore, we only use the SBA standard as a rough guideline. The definition of small businesses in most industries is a company that generates at most $41.5 million in annual revenue, or some amount lower than that.[29] For example, in the broadcasting industry, a radio networked company is considered small if its annual revenue is less than $35 million, whereas for a radio station, it is considered small if its annual revenue is less than $41.5 million.[30] All required amounts for being small are below $41.5 million. Therefore, we use this amount as a threshold, and create a variable named *CSIZE* for company size. Companies that generate less than $41.5 million in revenue are regarded as small, and those that generate revenues more than that are not considered as small businesses. For companies with unknown revenues, the variable *CSIZE* takes the value of **`Unknown`**.

The three classes, **`Small`**, **`Large`**, and **`Unknown`**, have relatively balanced sizes, and the numbers of observations are 10,383, 8,677, and 5,836, respectively. Table 4 shows that small companies have an overall probability of litigation of 86.5%, which is slightly higher than that of large companies, which is 82.6%.

---

[29] *See generally id.*
[30] *Id.* at 30.

		LITIGATED=0	*LITIGATED*=1	TOTAL
Small	Percentage	13.5%	86.5%	100.0%
	Count	1401	8982	10383
Large	Percentage	17.4%	82.6%	100.0%
	Count	1511	7166	8677
Unknown	Percentage	15.3%	84.7%	100.0%
	Count	890	4946	5836

Table 4: Two-way table of *CSIZE* and *LITIGATED*. Percentages are calculated based on the total number of observations in each *CSIZE* class.

6. Publicly Traded or Not? – PUB

Public companies might be the target of lawsuits for damages incurred by cyber incidents on shareholder value. For example, in *Eugenio v. Berberian et al.*, the plaintiff, who is a shareholder of Laboratory Corporation of America Holdings (LabCorp), initiated a shareholder derivative lawsuit against the board of directors and certain executive officers of the company.[31] The plaintiff alleged that the management of LabCorp failed to take adequate measures against cyber threats, thus leading to data breaches.[32] Therefore, we see that public companies are likely to have a larger legal exposure, because more stakeholders are involved if there is a cyber incident.

To study the effect of being publicly traded, we utilize the information on company type from the original dataset. In the dataset, there are eight types of organizations.[33] Since we are only interested in testing whether public companies are more likely to experience cyber-related lawsuits, we combine some of the types to create only two groups of companies, including public and nonpublic, and we introduce a variable named *PUB*, which takes the value of 0 for non-public companies, and 1 for publicly traded companies.

[31] Complaint at 1-2, Eugenio v. Berberian, No. 2020-0305-PAF, 2020 WL 2095561 (Del. Ch., Apr. 28, 2020).

[32] *Id.* at 7–8.

[33] *See infra* Appendix B.

One concern about introducing this explanatory variable is that there might be a positive association between a company being public (*PUB*) and a company being large (*CSIZE*). We can visualize this association using a two-way table between *CSIZE* and *PUB*, as shown in Table 5. We see that a large number of small companies are nonpublic (9,193), while the majority of large companies are public (5,474), and this suggests that there is a positive association between company size and whether or not it is public. We will later discuss the approach that we take to distinguish the effect of company size and the effect of company type by including interaction terms in some of the regression models.

	PUB=0	*PUB*=1
Small	9193	1190
Large	3203	5474
Unknown	4094	1742

Table 5：Two-way table of *CSIZE* and *PUB*, where the values are numbers of observations in individual classes defined by *CSIZE* and *PUB*.

Similarly, we report a two-way table of *PUB* and *LITIGATED*, from which we can see that nonpublic companies overall have a slightly higher probability (85.5%) of litigation than public companies (83.3%), which coincides with what we found for small companies and large companies, given the positive association between company size and company type.

		LITIGATED=0	*LITIGATED*=1	TOTAL
PUB=0	Percentage	14.5%	85.5%	100.0%
	Count	2395	14095	16490
PUB=1	Percentage	16.7%	83.3%	100.0%
	Count	1407	6999	8406

Table 6：Two-way table of *PUB* and *LITIGATED*. Percentages are calculated based on the total number of observations in each *PUB* class.

7. Interaction Effects

As previously pointed out, there is a positive association between company size and company type (see Table 5), that is, most of the small

companies are nonpublic and most of the large companies are public. So, is it still worthwhile to include both variables in the model? To answer this question, we need to look at the two minority classes in which those two classes are not well aligned. Specifically, in terms of the probability of litigation, how does a small nonpublic company differ from a small public company, and how does a large nonpublic company differ from a large public company? Insights into these questions can be obtained by including the interaction term of *PUB* and *CSIZE*. The existence of such an interaction effect is hinted at by Table 7, where the percentages are the proportions of incidents litigated in individual classes, *i.e.*, the number of litigated incidents divided by the number of all incidents in each class. Note that they do not represent the true or approximated probability of litigation because as mentioned before, there is a sampling bias that causes the litigated incidents to outnumber those that are not litigated. Nevertheless, we can still compare those numbers on a relative basis. This table shows that for small companies, being publicly traded reduces the likelihood of cyber incidents being litigated, whereas for large companies, that likelihood is higher among the public ones. This suggests that the size of a company may change the effect of being public and its influence on the probability of litigation.

	CSIZE		
	Small	**Large**	**Unknown**
PUB=0	86.8%	82.0%	85.3%
PUB=1	84.4%	82.9%	83.5%

Table 7：Interaction table of *PUB* and *CSIZE*, where the percentages represent the proportion of incidents litigated in each class.

It is reasonable to hypothesize that there might be other interaction effects between different pairs of variables, and therefore, we will include all pairwise interaction effects in the model, as described in the following section.

8. Litigation Rate in Different Industries

In this study, the industry variable is controlled for as a fixed effect, because compared to the status of being a public or private company and the size of a company, it is reasonable to assume that the particular industry that a company operates in is unlikely to change since the inception of the company. It is, however, interesting to learn which industries are more likely

to face litigation after cyber incidents. For example, for the underwriting and pricing of cyber insurance, the specific industry of an insurance applicant or policyholder is typically a factor that insurers would take into consideration, as suggested in Romanosky, Ablon, *et al.*.[34] Therefore, here we provide a somewhat qualitative description.

By calculating the litigation rates of all industries, which are defined by 2-digit SIC codes, we get Figure 2. The rates are simply the percentage of cyber incidents that were litigated in the corresponding industry. For example, in the Services industry, 88.5% of the cyber incidents in our sample are litigated. Error bars are also provided, of which the ends are the 5% and 95% quantiles if the litigation rate is assumed to follow a Beta distribution. A wide error bar means there are few data points in that industry, for example, the Mining industry. Despite some wide error bars in certain industries, we can still make some comparisons. Figure 2 shows that the deviation in litigation rates among different industries is considerably large, with the highest one being 88.5% and the lowest one being 39.5%. Among all industries, Services and Finance, Insurance, Real Estate industries are the two that have the highest litigation rate for cyber incidents. This result should not be surprising because companies in the Service industry, such as healthcare providers and educational institutions, and those in the Finance, Insurance and Real Estate industry, such as banks and credit agencies, typically hold a large amount of confidential information related to their customers. Therefore, they are commonly the target of cyber intruders and the chance that those companies mishandle that data is also high. Later, we will see that privacy violation incidents have an especially high probability of being litigated, and therefore, those industries that have a high risk of getting involved in privacy violations naturally have a high litigation probability.[35] In contrast, those industries that have a much smaller volume of privacy-related data, such as Agriculture, generally have lower litigation rates. The relationship between industry (*IND*) and privacy violation, as a value of *ITYPE*, is also depicted in Figure 2, and we can easily observe that the litigation probability of an industry is highly aligned with the probability of a company in that industry having privacy violations.

---

[34] Sasha Romanosky, Lilian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 12 (2019).

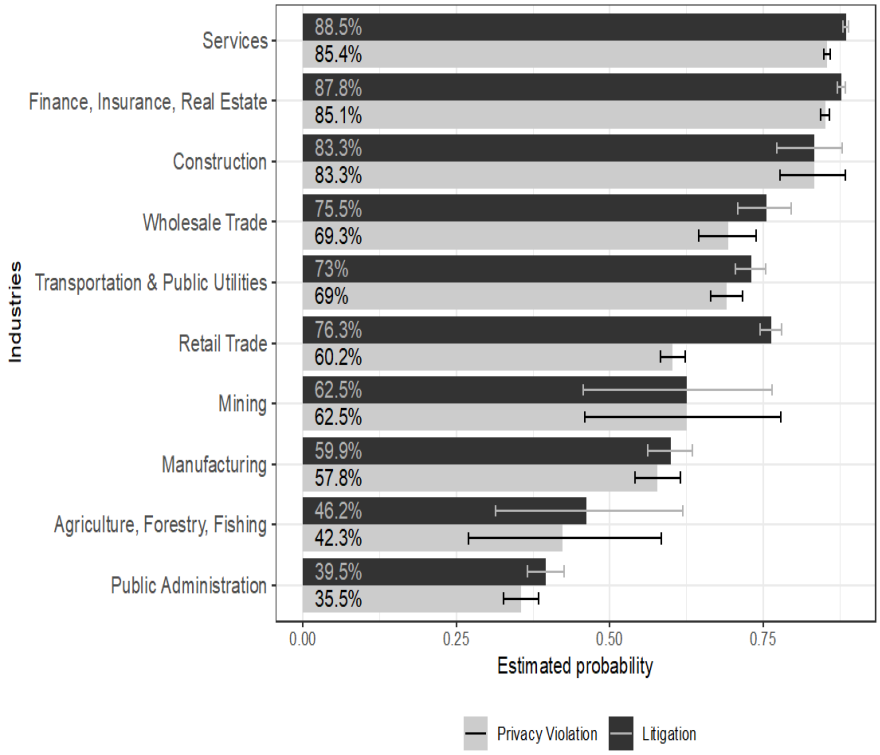


Figure 2：Litigation rates and rates of privacy violations in different industries

For this reason, we believe that the difference between industries in terms of litigation probability is rooted in the divergence of the characteristics of cyber incidents that different industries experience, and therefore, we primarily focus on the type of incident as an explanatory variable of litigation probability, which indirectly explains why some industries have higher litigation rates than others.

9. Effect of Data Breach Notification Laws

Beyond the previously mentioned variables, we have attempted to investigate whether data breach notification laws have an impact on the probability of litigation of cyber incidents. Since 2002, the year in which California enacted the first data breach notification law in the U.S.---which

requires organizations to notify authorities and customers whose confidential information is affected by data breach events---all U.S. states have enacted similar laws. We are also interested in studying how data breach notification laws affect the likelihood of a case being litigated. The effect does not necessarily have to be the direct consequence of violating those laws. It could also be the case that because of the notification laws, companies are obligated to disclose any incidents that involve customers' data, thus resulting in a greater publicity of those incidents, and then lawsuits are more likely to follow.

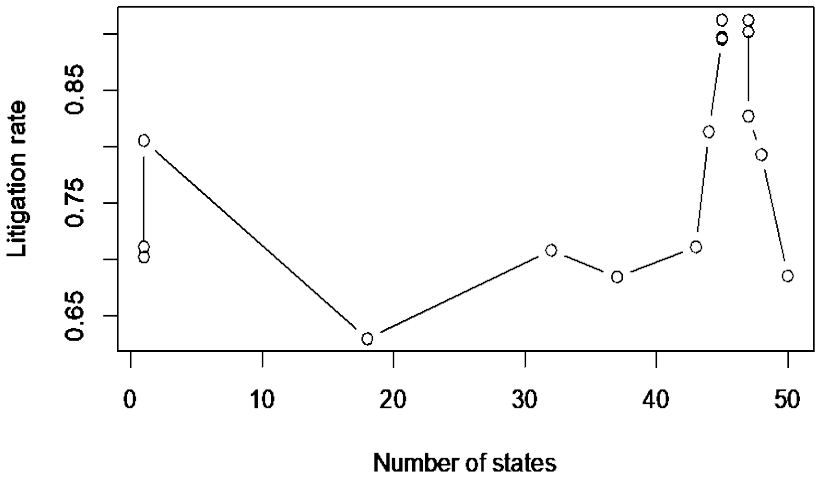


Figure 3：Litigation rate against the number of states with enacted data breach notification laws.

Because there is no such law at the federal level, to test this effect, we collected information on the year in which the data breach notification law was enacted in each state.[36] In addition, the scope of application of those laws are not uniformly the same. In some states, the law is applicable to all entities, whereas in other states, the law can only be applied to entities that

[36] *Data Breach Notification Law by State*, ITGOVERNANCE, https://www.itgovernanceusa.com/data-breach-notification-laws (last visited May 26, 2021).

conduct businesses in those states.[37] The notification requirements also differ by state. For example, North Dakota requires entities to notify customers if a data breach involves their date of birth or mother's maiden name, because such information is commonly used for security questions and password recovery.[38] However, there is no such requirement in most other states.[39] Given the diversity in state data breach notification laws, it is difficult to determine a company's legal exposure created by all notification laws in the U.S. in a given year. For this study, we use the number of states that have notification laws in a certain year as a proxy of the overall legal exposure of all companies in that year. That is, as more and more states have enacted their own data breach notification laws, a company is more likely to be subject to the compliance requirements specified in one or more state notification laws. We want to study whether such an increase in legal exposure will increase the probability of litigation following an incident. However, given that the data of the number of states with enacted notification laws is a time series in nature, we will not incorporate this variable in our panel data analysis. Therefore, we create Figure 3, which plots the litigation rate[40] in a year against the number of states with enacted data breach notification laws in that year, and the litigation rate in the same year.

This figure shows that there is no obvious relationship between notification laws and litigation rate. But we believe this is not conclusive and it is unlikely to obtain meaningful results by simply applying statistical methods to the data we have because there is no straightforward connection between the observations and any specific notification laws. Certainly, more thorough legal studies can be conducted on how each individual state law affects companies in different states in the U.S.

a. *Base Model and Full Model*

To quantify the effects of explanatory variables as discussed in the previous section, we construct two logistic regressions as follows:

---

[37] *See generally id.*

[38] *See* N.D. CENT. CODE ANN. § 51-30-01 (West 2021) (defining "Personal information"); N.D. CENT. CODE ANN. § 51-30-03 (West 2021) (requiring the disclosure of any data leaks to the owner of the personal information).

[39] *See generally* ITGOVERNANCE, *supra* note 36.

[40] The litigation rate is calculated as follows: the number of litigated cases divided by the number of all incidents in a certain year.

- Base model:

$$\log\left(\frac{P(LITIGATED)}{1-P(LITIGATED)}\right) = \beta_0 + \beta_1 PSI + \beta_2 ITYPE + \beta_3 CSIZE + \beta_4 PUB + \beta_5 BSIZE + \gamma_1 IND + \gamma_2 YEAR + \epsilon$$

- Full model:

$$\log\left(\frac{P(LITIGATED)}{1-P(LITIGATED)}\right) = \beta_0 + \beta_1 PSI + \beta_2 ITYPE + \beta_3 CSIZE + \beta_4 PUB + \beta 5 BSIZE + \beta_6 PSI * ITYPE + \beta_7 PSI * CSIZE + \beta_8 PSI * PUB + \beta_9 PSI * BSIZE + \beta_{10} ITYPE * CSIZE + \beta_{11} ITYPE * PUB + \beta_{12} ITYPE * BSIZE + \beta_{13} CSIZE * PUB + \beta_{14} CSIZE * BSIZE + \beta_{15} PUB * BSIZE + \gamma_1 IND + \gamma_2 YEAR + \epsilon$$

In these regressions, the asterisk operator $*$ denotes the interaction effects between two variables. In terms of coefficients, β_0 is the intercept. $\{\beta_i\}_{i=1,2,\ldots,5}$ denote the coefficients of main effects of *PSI*, *ITYPE*, *CSIZE*, *PUB* and *BSIZE*, and $\{\beta_i\}_{i=6,7,\ldots,15}$ are the coefficients of pairwise interaction terms.

As a standard practice, we control for the industry fixed effect (*IND*) and the year fixed effect (*YEAR*) in both models, so that incidents that occurred in the same year and the same industry are compared. For the classification of industries, we use the 2-digit Standard Industry Classification (SIC) codes.[41]

In both models, we need to specify the reference level for categorical variables with more than two levels, which are *ITYPE* and *CSIZE*.[42] For

[41] *Standard Industrial Classification (SIC) Manual*, OCCUPATIONAL SAFETY & HEALTH ADMIN., https://www.osha.gov/data/sic-manual (last visited Apr. 20, 2021).

[42] The fixed effects *IND* and *YEAR* are also categorical, but since they are controlled for, and because we do not intend to compare between the different levels of them, the choice of reference level of those two variables does not matter and does not affect the estimation of the coefficients of explanatory variables, except the intercept. In our model, we arbitrarily choose the Agriculture, Forestry and Fishing industry (SIC code: 01-09) as the reference level of *IND* and 2018 as the reference level of *YEAR*.

ITYPE, we make the **`PV`** class the reference level, because as we saw from the two-way table of *ITYPE* and *LITIGATED*, privacy violation incidents seem to have an extraordinarily high likelihood of litigation compared to the other two classes and we hope to quantify such differences. For *CISZE*, we make **`Small`** the reference level, so that we can compare between small companies and large companies. The **`Unknown`** class is not informative, and therefore, we will not make any inference about it. For binary variables that can only be either 0 or 1, the reference level is naturally 0.

The only difference between the base model and the full model is that the full model includes all pairwise interaction terms, and thus, we are able to compare those two models and test whether or not any of the interaction effects are significant. In the following section, an adjusted model will be introduced based on the full model for an improved fit.

b. *Results*

Table 8 shows the estimate and standard error of each coefficient from the three models.

	Base		**Full**		**Adjusted**	
(Intercept)	1.458	*	12.472		2.816	**
	(0.794)		(211.201)		(0.862)	
PSI=1	0.451	**	-9.255		0.378	.
	(0.141)		(211.199)		(0.224)	
*ITYPE***ND**	-6.267	***	-16.925		-7.174	***
	(0.100)		(211.199)		(0.185)	
*ITYPE***DB**	-4.992	***	-15.093		-6.523	***
	(0.117)		(211.199)		(0.208)	
*CSIZE***Large**	0.287	***	-2.562	***	-2.548	***
	(0.086)		(0.443)		(0.439)	
*CSIZE***Unknown**	0.027		-1.031	*	-1.037	*
	(0.095)		(0.434)		(0.434)	
PUB=1	0.261	**	2.560	***	2.502	***
	(0.080)		(0.425)		(0.421)	
BSIZE	0.011		-0.290	***	-0.219	***

	Base	Full		Adjusted	
	(0.009)	(0.064)		(0.017)	
PSI=1:*ITYPE***ND**	-	9.784		-	
	-	(211.199)		-	
PSI=1:*ITYPE***DB**	-	8.519		-	
	-	(211.199)		-	
PSI=1:*CSIZE***Large**	-	1.713	***	1.689	***
	-	(0.392)		(0.389)	
PSI=1:*CSIZE***Unknown**	-	0.582		0.589	
	-	(0.383)		(0.381)	
PSI=1:*PUB=1*	-	-1.894	***	-1.826	***
	-	(0.361)		(0.355)	
PSI=1:*BSIZE*	-	0.071		-	
	-	(0.062)		-	
*ITYPE***ND**:*CSIZE***Large**	-	1.355	***	1.374	***
	-	(0.258)		(0.259)	
*ITYPE***DB**:*CSIZE***Large**	-	1.253	***	1.236	***
	-	(0.243)		(0.242)	
*ITYPE***ND**:*CSIZE***Unknown**	-	0.641	*	0.649	*
	-	(0.275)		(0.276)	
*ITYPE***DB**:*CSIZE***Unknown**	-	0.411		0.418	
	-	(0.286)		(0.286)	
*ITYPE***ND**:*PUB=1*	-	-0.765	**	-0.770	***
	-	(0.233)		(0.234)	
*ITYPE***DB**:*PUB=1*	-	-0.823	***	-0.809	***
	-	(0.242)		(0.241)	
*ITYPE***DB**:*BSIZE*	-	0.239	***	0.235	***
	-	(0.018)		(0.017)	
*CSIZE***Large**:*PUB=1*	-	-0.247		-0.255	
	-	(0.214)		(0.214)	
*CSIZE***Unknown**:*PUB=1*	-	-0.558	*	-0.571	*
	-	(0.256)		(0.256)	

	Base	**Full**		**Adjusted**	
*CSIZE***Large**:*BSIZE*	-	0.045	*	0.047	*
	-	(0.022)		(0.022)	
*CSIZE***Unknown**:*BSIZE*	-	0.057	*	0.056	*
	-	(0.026)		(0.026)	
PUB=1:*BSIZE*	-	0.043	*	0.042	*
	-	(0.020)		(0.020)	
YEAR controls	Y	Y		Y	
Industry controls	Y	Y		Y	
Number of Observations	24896	24896		24896	
Degrees of Freedom	24861	24843		24846	
Pseudo R^2	0.671	0.686		0.686	
AIC	7075.8	6785.3		6783.9	

Values in parentheses are standard errors of their corresponding estimates.

Significance codes: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, . $p < 0.1$

Table 8： Logistic regression results of three models for litigation probability

Details on the base model and the full model have already been given. The comparison between those two models suggests that many of the interaction effects do exist, and the full model fits the data better than the base model if their qualities are measured by the Akaike Information Criterion (AIC).

However, there are also some issues with the full model. If we look at the main effects of *PSI* and *ITYPE,* as well as their interaction effect, we can find that their coefficients are associated with large standard errors (211.119), which indicates that not enough data points can be used to estimate those effects. In addition, we observe that very little to no interaction effect is found between *PSI* and *BSIZE*. That is, with all other conditions fixed, whether or not there is an impact on personal sensitive information does not change how the number of breached records affects the probability of litigation.

Based on those observations, we removed those two interaction terms, including $PSI * ITYPE$ and $PSI * BSIZE$, from the full model and created the adjusted model with most of the main effects and interaction

effects being statistically significant at the 0.05 level, except the main effect of *PSI*. But because some interaction effects associated with *PSI* are very significant, such as the interaction between *PSI* and *PUB*, *PSI* should not be removed from the model. The adjusted model's performance is close to the full model, with a slight improvement in terms of the AIC value.

For each of the three models, we report its pseudo R^2, or equivalently McFadden's R^2, as defined in McFadden.[43] It is calculated as 1 − (residual deviance)/(null deviance), and intuitively it means how much the deviance of a null model (intercept only) is reduced by introducing additional explanatory variables into the model. Therefore, a higher pseudo R^2 means a better fit. However, as we saw before, the act of privacy violation and the involvement of personal sensitive information are strong indicators of litigation, at least according to the distribution of litigated cases in our sample, and they represent the majority of the observations. Therefore, a pseudo R^2 as high as 0.686 does not mean that the model can have a high explanatory power for incidents that are not privacy violations or have no impact on personal sensitive information.

Overall, the full model and the adjusted model have similar performances, but because the adjusted model does not have the same estimation issue as we saw in the full model, as a result, it is more interpretable. Therefore, the following discussions will be derived based on the adjusted model.

c. *Discussions*

Because of the existence of interaction effects, the effect of each variable cannot be interpreted in an isolated manner. As aforementioned, there are two categories of variables, including incident characteristics and company characteristics, and thus one way of understanding those interaction effects is to answer the following question: what is the difference between the probabilities of litigation when a specific type of cyber incident impacts different types of companies? For example, does the involvement of personal sensitive information have different effects on small companies and large companies, in terms of the probability of litigation?

For the reason that the probability of litigation cannot be accurately measured due to selection bias, the direct effect of an explanatory variable on the litigation probability also cannot be precisely described. That is, no unbiased and satisfying answer can be provided to questions like: "what is

---

[43] Daniel McFadden, *Conditional Logit Analysis of Qualitative Choice Behavior*, *in* FRONTIERS IN ECONOMETRICS 105 (Zarembka ed., 1973).

the litigation probability of an incident that does not affect personal sensitive information?" and "how much increase/decrease in that probability will there be if the incident actually affects personal sensitive information?" Therefore, we will evaluate the model results straightforwardly based mainly on the estimated variable coefficients. Intuitively, they represent the relative change in log odds (O) introduced by the effect, which is defined as

$$\mathbf{O} = \log\left(\frac{P(LITIGATED)}{1 - P(LITIGATED)}\right)$$

$$\text{Odds change} = \mathbf{O}_{\text{Effect}} - \mathbf{O}_{\text{Baseline}}$$

$\mathbf{O}_{\text{Baseline}}$ is the baseline log odds of litigation, measured when all explanatory variables take their reference levels (*i.e.* on condition that a privacy violation event hits a small nonpublic company and results in no loss of personal sensitive information). Additionally, the log of number of breached accounts *BSIZE* is set to be 2.45, which is the sample mean, for the baseline condition. $\mathbf{O}_{\text{Effect}}$ is the logaddsratio after additional effects are added to the baseline.

The conversion between probability and odds ratio can be done as follows. With our sample data, the baseline log odds ratio is estimated to be 2.31, which corresponds to a litigation probability of ninety-one percent. This high probability is largely attributed to privacy violation being set as the reference level of *ITYPE*, and as suggested by Table 2, this type of incident has a high litigation rate. The change in odds tells us the direction and magnitude of an effect relative to that probability and avoids directly using the biased estimate of the litigation probability on the baseline condition. Note that because of the nonlinear relationship between probability and odds ratio, a decrease in odds results in a larger reduction in probability than the increase in probability caused by an increase in odds of the same amount. The exact decrease or increase in probability depends on the baseline.

d. *Effect of PSI*

To focus on the effects of personal sensitive information on various types of organizations, we arrange the results in Table 8, and put the information relevant to *PSI* into Table 9.[44]

[44] The aggregate effect is the sum of all relevant mean effects and interaction effects. For example, to get the total effect of PSI on large public companies, we

	PSI	*ITYPE*	*CSIZE*	*PUB*	*BSIZE*	Effect (Odds change)
Small & Nonpublic	0	-	**Small**	0	-	0.000
	1	-	**Small**	0	-	0.378
Large &Nonpublic	0	-	**Large**	0	-	-2.433
	1	-	**Large**	0	-	-0.366
Small & Public	0	-	**Small**	1	-	2.605
	1	-	**Small**	1	-	1.157
Large & Public	0	-	**Large**	1	-	-0.083
	1	-	**Large**	1	-	0.158

NOTE: TYPE and *BSIZE* columns are left empty because there is no significant interaction effect between *PSI* and either *ITYPE* or *BSIZE*, and thus those two variables have no impact on the effect of *PSI*.

Table 9: Effects of *PSI* on different types of organizations.

The result suggests that *PSI* is associated with two other variables, including *CSIZE* and *PUB* through interaction terms (as we discussed, the interaction terms with *ITYPE* and *BSIZE* are removed from the full model for low significance). The first row of Table 9 represents the baseline, thus having an odds change of 0. When everything else is held constant, we observe that the loss of personal sensitive information causes the baseline odds to increase by 0.378. This corresponds to a small litigation probability increase, given that the baseline probability is high. This comparison is shown in the left pane of Figure 4, when *PUB* takes the value of FALSE (equivalent to 0). For large nonpublic companies, the increase in litigation probability caused by loss of personal sensitive information is much more substantial. When there is no loss of personal sensitive information, the

need the main effects of *CSIZE***Large** (-2.548), *PUB=1* (2.502) and *PSI=1* (0.378), and all three pairwise interaction effects, including *PSI=1:CSIZE***Large** (1.689), *PSI=1:PUB=1* (-1.826), and *CSIZE***Large**:*PUB=1* (-0.255). In addition, because *PUB* and *CSIZE* also have interaction effects with *BSIZE*, *i.e.*, *PUB=1:BSIZE* (0.042) and *CSIZE***Large**:*BSIZE* (0.047), and the baseline value of *BSIZE* is 2.45, for large public companies, there will be an additional effect of size 2.45 × (0.042 + 0.047) = 0.218 from those interactions. All those numbers in parentheses can be directly found in Table 8, and their sum (the total effect calculated under the given condition) is listed in the last row in Table 9. All other rows in Table 9 are obtained in the same way.

litigation probability is much lower than the baseline (see the red bar on the left in the right panel of Figure 4), suggesting that for nonpublic companies, the small ones are much more likely to be hit by lawsuits after a cyber incident without loss of personal sensitive information, compared to the large ones. However, once the loss of personal sensitive information is present, the litigation probability immediately returns back to the baseline level. Provided the 91% baseline litigation probability, loss of personal sensitive information almost doubles the litigation probability for large nonpublic companies.

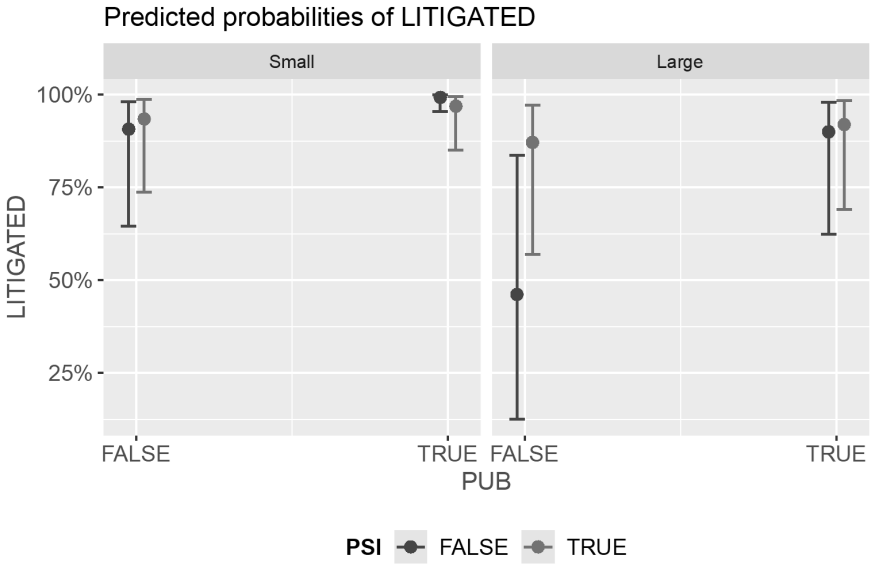


Figure 4: Visualization of the effect of *PSI* on companies with different characteristics, compared to the baseline probability (leftmost bar).

For small public companies, with or without the loss of personal sensitive information, the litigation probability is higher than the baseline. Because of the nonlinear relationship between the odds ratio and litigation probability, an increase in odds ratio by 2.605 or 1.157 under the situation without or with loss of sensitive personal information, respectively, yields a marginal increase in litigation probability. This increase is more noticeable if the baseline is low. For large public companies, litigation probabilities are very close to the baseline. Therefore, we see that, except for small public

companies, the impact of loss of personal sensitive information on litigation probability is overall small.

e. *Effect of ITYPE and BSIZE*

Other than the loss of personal sensitive information, regarding the characteristics of a cyber incident, we are also interested in the type of the incident, *i.e.*, *ITYPE*, and the number of affected records, *i.e.*, *BSIZE*, if it is a data breach or privacy violation event. Because the adjusted model in Table 8 shows that there is an interaction effect between those two variables, we will discuss them jointly and show how they affect companies with different characteristics. Similarly as before, we consider small nonpublic, large nonpublic, small public, and large public companies.

We create Table 10 in the same way as Table 9, but because of the interaction effect between *ITYPE* and *BSIZE*, the table needs to be expanded for different sizes of affected records. *BSIZE* is a continuous variable, and to highlight the contrast between small breaches and large breaches, we consider two specific values of *BSIZE*. First, 2.45, which is the mean for *BSIZE* and corresponds to a small breach with a number of records of $e^{2.45} \approx 12$, and then 10, which represents a large breach that affects $e^{10} \approx 22{,}026$ records. Correspondingly, those effects are visualized in Figure 5a and 5b.

For all companies, the distinction between privacy violation incident and the other two types of incidents is significant. That is, the probability of a privacy violation incident being litigated is much higher than the litigation probability for the other two types of incidents.

The litigation probability is especially low for cyber incidents that cause no loss of information, and the reason might be that in this category of incidents, there is usually little to no impact on third parties. For example, in typical distributed denial-of-service attacks, in most cases the damage is contained within the victim company and rarely affects the confidentiality of customers' information. Data breaches caused by malicious attacks have a slightly higher litigation probability compared to non-data related cyber incidents, such as DDoS attacks and ransomware attacks. However, privacy violations have a significantly higher probability of being litigated compared to malicious data breaches. This result is possibly because malicious data breaches are caused by attackers, whose actions are out of the company's control. Generally, the plaintiff has the burden of proof to show that the company has the duty of protecting customers' data but has then failed to take adequate security measures to do so. Obtaining evidence to establish the breach of such a duty may be much more difficult than finding statutory

violations caused by a company's own negligent or willful acts, which are commonly the basis for bringing a privacy violation related lawsuit.

This suggests that the common law system may not be sufficient for providing legal remedies for malicious data breaches, and that there should be statutes directed at establishing the duty to secure data so that the barrier for litigating data breach events may be lowered by making it easier for individuals impacted by data breaches to seek relief in court.

In addition, as suggested by Table 3, malicious data breaches generally impact a much larger number of records than privacy violations, and thus lawsuits derived from data breaches are often in the form of class actions; whereas privacy violation events are less widespread and lead to the prevalent individual actions. Specifically, the number of class actions derived from malicious data breaches is 481[45], which presents 55.6% (481/865) of all litigated data breach cases; whereas for privacy violations, the number of class actions is 3,115[46], which is only 15.6% (3,115/19,885) of the total number of privacy lawsuits. It is also possible that the complexity of class actions might discourage potential lawsuits from being brought up after data breach events, as suggested by Kesan and Hayes.[47]

For the effect of breach size on different types of incidents, as is to be expected, we find that breach size has no effect on non-data related cyber incidents. For privacy violation events, however, there is a negative relationship between breach size and litigation probability. This is counterintuitive, and the reason might be that there are a large number of litigated privacy violation cases which affect only one record (see Table 3 and Figure 1), thus making the estimation of the litigation rate highly sensitive to those large breaches that are not litigated. However, based on the sample we have, it is difficult to find an explanation for why some large privacy violations are not litigated, other than the possibility that those large privacy violations are settled prior to litigation. For malicious data breach events, there is a small positive relationship between breach size and litigation probability for all companies with different characteristics. Overall, the breach size does not seem to play an important role in litigation probability. Although it is found to have a significant main effect and interaction effects with other variables, increasing *BSIZE* from 2.45 (12

---

[45] *Cyber Loss Data, supra* note 17.

[46] *Id.*

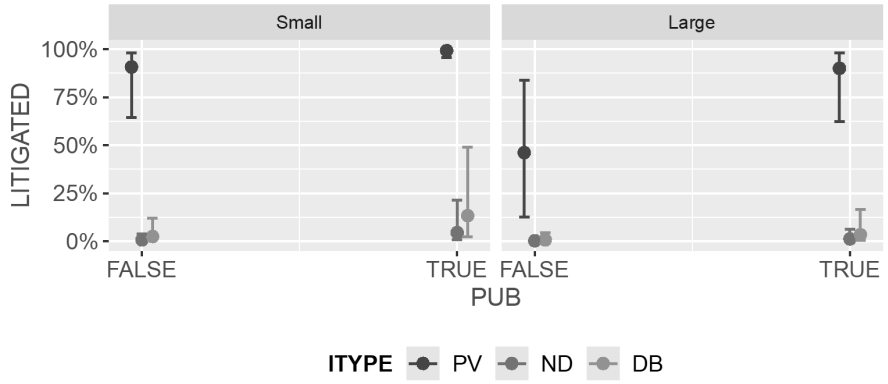
[47] Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries,* 2019 U. ILL. L. REV. 295 (2019).

records) to 10 (22,026 records) has a very limited impact on the litigation probability of all types of incidents and all types of companies.

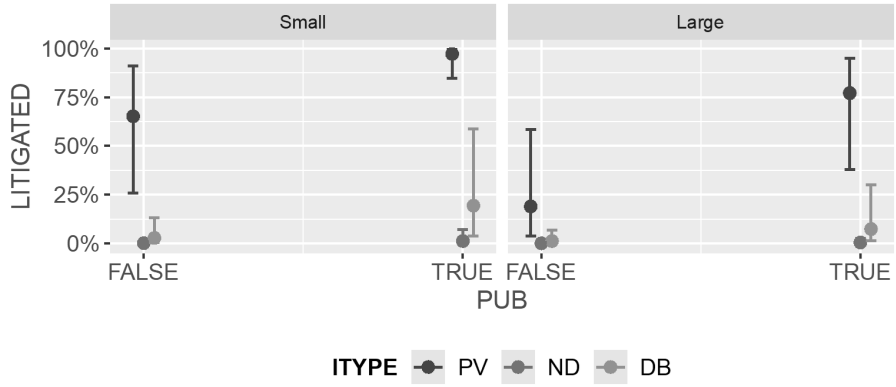
	PSI	*ITYPE*	*CSIZE*	*PUB*	*BSIZE*	Effect (Odds change)
Small & Nonpublic	-	**PV**	**Small**	0	2.45	0.000
	-	**ND**	**Small**	0	2.45	-7.174
	-	**DB**	**Small**	0	2.45	-6.523
	-	**PV**	**Small**	0	10	-1.651
	-	**ND**	**Small**	0	10	-8.825
	-	**DB**	**Small**	0	10	-6.398
Large & Nonpublic	-	**PV**	**Large**	0	2.45	-2.548
	-	**ND**	**Large**	0	2.45	-8.348
	-	**DB**	**Large**	0	2.45	-7.835
	-	**PV**	**Large**	0	10	-3.847
	-	**ND**	**Large**	0	10	-9.647
	-	**DB**	**Large**	0	10	-7.358
Small & Public	-	**PV**	**Small**	1	2.45	2.502
	-	**ND**	**Small**	1	2.45	-5.442
	-	**DB**	**Small**	1	2.45	-4.829
	-	**PV**	**Small**	1	10	0.851
	-	**ND**	**Small**	1	10	-6.774
	-	**DB**	**Small**	1	10	-4.385
Large & Public	-	**PV**	**Large**	1	2.45	-0.301
	-	**ND**	**Large**	1	2.45	-6.871
	-	**DB**	**Large**	1	2.45	-6.397
	-	**PV**	**Large**	1	10	-1.026
	-	**ND**	**Large**	1	10	-7.851
	-	**DB**	**Large**	1	10	-5.600

NOTE: *PSI* column is left empty because there is no significant interaction effect between *PSI* and either *ITYPE* or *BSIZE*, and thus *PSI* has no impact on the effects of *ITYPE* and *BSIZE*.

Table 10: Effects of *ITYPE* and *BSIZE* on companies with different characteristics.



(a) *BSIZE* = 2.45



(b) *BSIZE* = 10

Figure 5: Visualization of the effect of *ITYPE* and *BSIZE* on companies with different characteristics.

f. *Effect of CSIZE and PUB*

Combining the results about how incident characteristics affect companies with different characteristics, we can also get some useful insights into how the size and type of a company affect its cyber incident litigation probability.

In terms of the company size, surprisingly, we observe that the small ones are overall more likely to face lawsuits after cyber incidents compared to large companies of the same company type (*i.e.*, either among all public companies or among all nonpublic companies). This disproves the hypothesis that large companies have a higher probability of being sued after cyber incidents because of their deeper pockets. However, if public companies and nonpublic companies of the same size are compared, we observe that public companies face a substantially higher legal risk from all types of cyber incidents. Those two findings, taken together, suggest that small public companies face the highest legal risk in cyber incidents.

Overall, the effects of *CSIZE* and *PUB* are quite considerable, especially when they are compared with the effects of *PSI* and *BSIZE*. This is a strong signal that the legal risk faced by different companies should be evaluated differently.

III. CYBER LITIGATION OUTCOMES

Given that a cyber incident is litigated, what would be the consequence and the impact on the defendant company? Will it be dismissed or resolved? If a resolution is reached, how much does the resolution cost in terms of award or settlement? To find the answers to those questions, we further analyzed the outcomes of cyber litigation.

A. DISMISSAL RATE OF LITIGATED CYBER CASES

Previously, we briefly touched on the issue that in lawsuits brought by individuals, who suffer from privacy violations or breaches of confidential information, against organizations that are allegedly liable for such incidents, the plaintiffs would typically have a difficult time demonstrating that they have experienced concrete harms arising from the incident. This makes those lawsuits likely to be dismissed for lacking Article III standing.

To see the proportion of litigated cases that are dismissed, we have created a subset of the previous sample to include only litigated cases that have reached a resolution. That is, based on the coded status of the cases, we only consider those that are dismissed with or without prejudice, settled between the parties, or awarded a judgment after trial. Note that because the population of interest is now all the litigated cases, and it is reasonable to assume that most of those cases are well documented, this new sample does

not have the same sampling bias issue caused by unreported incidents, as we saw in the previous analysis.

This sample of dismissed, settled, and tried cases contains 16,773 observations, of which 8,636 cases were either settled or went to trial, and the remaining 8,137 were dismissed.[48] Therefore, the overall dismissal rate is as high as 48.5%. From Table 11, we can easily observe that this high likelihood of dismissal is mainly attributed to privacy violations and malicious data breaches. This could be evidence of a lack of standing from a statistical perspective. To further strengthen this evidence, in the short description attached to each incident, we performed a keyword/key phrase search for words and short phrases, such as *standing* and *substantial/concrete/actual harm/damage*, which are indicators of the standing issue, and found that there are at least 2,223 litigation cases dismissed for this reason. The number could in fact be larger because in some case descriptions, the reason for dismissal is not explicitly stated. This finding suggests that, although privacy violations have a high litigation rate, in a considerably large number of those relevant lawsuits, the plaintiffs are unable to satisfy the requirements for Article III standing, such as demonstrating actual harm or a concrete injury.

		Not Dismissed	Dismissed
PV	Percentage	50.8%	49.2%
	Count	8161	7915
ND	Percentage	85.6%	14.4%
	Count	190	32
DB	Percentage	60.0%	40.0%
	Count	285	190

Table 11: Dismissal rate of cases relating to different types of cyber incidents

Moreover, since we are examining cyber cases conditioned on whether they are litigated, we can associate additional legal information with those cases. Specifically, we will take a look at whether a lawsuit is a class action or an individual action, and how that affects the dismissal rate, as well as the cost of settlement or award in the following section, if the lawsuit is not dismissed. Class actions are popular in cyber litigation cases since mass

[48] *Cyber Loss Data, supra* note 17.

data breaches or mass privacy violations occur quite frequently, such as the 2017 Equifax data breach[49] and the Facebook biometric privacy class action initiated in 2020.[50] Similarly as before, Table 12 shows the dismissal rate of class actions and individual actions. We observe that class actions have a higher dismissal rate than individual actions, possibly because the certification of class actions is subject to strict requirements under Federal Rule of Civil Procedure 23,[51] and we observe that some of the certifications are denied. For example, in Weitzner v. Cynosure, Inc., the plaintiff filed a complaint against the defendant for the alleged violation of the Telephone Consumer Protection Act of 1991 (TCPA) by sending unsolicited advertisements via facsimile.[52] The certification of a nationwide class action was denied by the court for not satisfying the commonality, typicality, predominance, and superiority requirements of Rule 23.[53]

		Not Dismissed	Dismissed
Class	Percentage	40.1%	59.9%
	Count	942	1409
Individual	Percentage	53.3%	46.7%
	Count	7694	6728

Table 12: Dismissal rate of different legal actions

Overall, we observe that a large number of lawsuits following cyber incidents are dismissed. The most prevalent cause of such dismissals is the lack of substantial interest in the incidents that cause data loss, including privacy violations and malicious data breaches. In addition, class actions are more likely to be dismissed than individual actions because of the difficulty in meeting the class action requirements.

[49] *In re* Equifax, Inc., 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

[50] *In re* Facebook Biometric Info. Priv. Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

[51] FED. R. CIV. P. 23.

[52] Weitzner v. Cynosure, Inc., No. MICV2005-01778, 2012 WL 11953976, *1 (Mass. Super. Ct. 2012).

[53] *Id.* at *4–5.

B. COST OF SETTLEMENT OR AWARD

Provided that a case is settled or goes to trial at some cost, we conduct a further quantitative analysis on the factors that affect the size of the settlement or the award. In the existing literature concerning the cost of cyber incidents, many studies use indirect measures as proxies for the severity of an incident. For example, two periodicals[54] used the dataset of data breaches from the Privacy Rights Clearinghouse[55] to study the statistical properties of cyber losses in terms of the number of records breached. However, when the monetary cost of a cyber incident is of concern, the cost is unlikely to be exactly proportional to the number of breached records. This is especially so for legal settlements, which are the result of negotiations between multiple parties with different interests. There are few studies that address the monetary loss of cyber incidents. Romanosky examined a dataset of historical cyber incidents from the same provider from which we acquired our dataset.[56] The focus of Romanosky's study is on the total loss, and the author finds that the company size and the number of breached records play a significant role in determining the size of the total loss.[57] Eling and Wirfs extracted cyber-related losses from the SAS OpRisk Global data and used heavy-tailed distributions and factor models to fit the frequency and severity of those losses.[58]

However, we are not aware of any existing study that focuses on the legal costs of cyber incidents as we see from NetDiligence,[59] legal costs are a key component in the total cost of a cyber incident and worth in-depth exploration. Therefore, the goal of this section is to provide some insights into this topic.

---

[54] Martin Eling & Nicola Loperfido, *Data Breaches: Goodness of Fit, Pricing, and Risk Measurement*, 75 INS.: MATHEMATICS & ECONS. 126 (2017); Maochao Xu, Kristin M. Schweitzer, Raymond M. Bateman & Shouhani Xu, *Modeling and Predicting Cyber Hacking Breaches*, 13 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 2856 (2018).

[55] Data Breaches, PRIV. RTS. CLEARINGHOUSE, https://privacyrights.org/data-breaches (last visited Apr. 18, 2021).

[56] Sasha Romanosky, *Examining the Costs and Causes Cyber Incidents*, 2 J. CYBERSECURITY 121, 121 (2016).

[57] *Id.*

[58] Christian Biener, Martin Eling & Jan Hendrik Wirfs, *Insurability of Cyber Risk: An Empirical Analysis*, 40 GENEVA PAPERS 131, 135 (2015).

[59] NETDILIGENCE, *supra* note 4, at 2.

1. Data and Summary Statistics

The sample we used for modeling the cost of settlement or award is a subset of the sample we used in Section 2. This subset only contains cases that are settled or that go to trial and result in positive settlement costs or payouts as awards to plaintiffs.[60] Keeping all variables from that sample, we additionally introduced the variable of action type, denoted by *ACTION*, *i.e.*, class action or individual action, as described when previously discussing the dismissal rate. Moreover, we include the variable for settlement or award cost, denoted by *COST*, which is used as the response variable in this section. Because the distribution of those costs is highly skewed to the right, *COST* is normalized to be on the natural log scale.

Table 13 provides summary statistics for all variables that we will use to model the cost of settlement or award. In total, there are 1,393 settlement or award costs recorded in our sample, which is large enough to provide us with some meaningful insights. There is a large variation in those costs, with the lowest settlement being only $1[61] and the highest judgment exceeding $710 million[62]. Most costs concentrate near the lower end of the spectrum, with 50% of them being no more than $200,000, whereas the average cost is inflated by some extraordinarily large settlements. The log transformation brings the median (12.2) and the mean (11.9) close to each other, thus increasing the normality of the data.

[60] Missing values were removed.

[61] This is real. *See* Consent Judgment, Boring v. Google, Inc., No. 2:08-cv-00694-CB (W.D. Pa. Dec. 1, 2010).

[62] Order Granting Facebook, Inc.'s Application for Default Judgment against Defendant Sanford Wallace, Facebook, Inc. v. Wallace, No. C 09-798 JF (N.D. Cal., Oct. 29, 2009).

	Summary Statistics					
Continuous Variables	**Min.**	**1st Qu.**	**Median**	**Mean**	**3rd Qu.**	**Max.**
EXP(*COST*)	1	9000	200000	4788386	1739000	710738200
COST	0	9.1	12.2	11.9	14.4	20.4
BSIZE	0	0.7	3.7	5.2	9.2	21.2
Categorical Variables			**Levels**			
PSI			0/FALSE			1/TRUE
(count)			35			1358
PUB			0/FALSE			1/TRUE
(count)			991			402
ACTION			**Class**			**Individual**
(count)			438			955
ITYPE		**PV**		**ND**		**DB**
(count)		1029		139		225
CSIZE		**Small**		**Large**		**Unknown**
(count)		590		473		330
Number of Observations						1393

Table 13: Summary statistics of variables used for modeling costs of settlements and awards

2. Models and Comparisons

We take a similar approach as the one described in Section 2.3 to build the base model and the full model. The full model contains all pairwise interaction terms, whereas the base model does not. For both models, we control for the industry and year fixed effects. The difference is that since the response in this case is numerical, we simply use linear regression models instead.

- Base model:

$$COST = \beta_0 + \beta_1 PSI + \beta_2 ITYPE + \beta_3 CSIZE + \beta_4 PUB + \beta_5 BSIZE + \beta_6 ACTION + \gamma_1 IND + \gamma_2 YEAR + \epsilon$$

- Full model:

$$COST = \beta_0 + \beta_1 PSI + \beta_2 ITYPE + \beta_3 CSIZE + \beta_4 PUB + \beta 5 BSIZE + \beta 6 ACTION + \beta_7 PSI * ITYPE + \beta_8 PSI * CSIZE + \beta_9 PSI * PUB + \beta_{10} PSI * BSIZE + \beta_{11} PSI * ACTION + \beta_{12} ITYPE * CSIZE + \beta_{13} ITYPE * PUB + \beta_{14} ITYPE * BSIZE + \beta_{15} ITYPE * ACTION + \beta_{16} CSIZE * PUB + \beta_{17} CSIZE * BSIZE + \beta_{18} CSIZE * ACTION + \beta_{19} PUB * BSIZE + \beta_{20} PUB * ACTION + \beta_{21} BSIZE * ACTION + \gamma_1 IND + \gamma_2 YEAR + \epsilon$$

In addition, similarly as before, an adjusted model is introduced based on the full model with insignificant effects removed. The results of these three models are presented as follows.

3. Results and discussions

	Base		**Full**		**Adjusted**	
(Intercept)	9.381	***	12.202	***	9.226	***
	(2.610)		(3.629)		(2.542)	
PSI=1	-0.501		-2.746		-	
	(0.424)		(2.589)		-	
*ITYPE***ND**	3.060	***	0.058		3.794	***
	(0.243)		(2.257)		(0.349)	
*ITYPE***DB**	0.262		-0.618		1.816	***
	(0.207)		(2.465)		(0.431)	
PUB=1	0.577	***	-0.538		0.639	***
	(0.168)		(1.256)		(0.168)	
*CSIZE***Large**	0.347	*	2.414	*	0.594	
	(0.167)		(1.223)		(0.385)	
*CSIZE***Unknown**	-0.032		-1.926		-1.246	*
	(0.160)		(1.574)		(0.522)	
BSIZE	0.264	***	0.197		0.248	***
	(0.017)		(0.264)		(0.034)	

	Base		Full		Adjusted	
*ACTION***Individual**	-1.627	***	-1.913		-2.367	***
	(0.160)		(1.310)		(0.325)	
PSI=1:*ITYPE***ND**	-		2.609		-	
	-		(2.003)		-	
PSI=1:*ITYPE***DB**	-		1.970		-	
	-		(2.406)		-	
PSI=1:*PUB=1*	-		2.123		-	
	-		(1.187)	.	-	
PSI=1:*CSIZE***Large**	-		-1.890		-	
	-		(1.156)		-	
PSI=1:*CSIZE***Unknown**	-		0.671		-	
	-		(1.484)		-	
PSI=1:*BSIZE*	-		0.039		-	
	-		(0.263)		-	
PSI=1:*ACTION***Individual**	-		-0.486		-	
	-		(1.274)		-	
*ITYPE***ND**:*PUB=1*	-		0.598		-	
	-		(0.603)		-	
*ITYPE***DB**:*PUB=1*	-		-0.131		-	
	-		(0.474)		-	
*ITYPE***ND**:*CSIZE***Large**	-		-1.139		-1.116	*
	-		(0.637)	.	(0.509)	
*ITYPE***DB**:*CSIZE***Large**	-		-0.957	*	-0.853	.
	-		(0.487)		(0.455)	
*ITYPE***ND**:*CSIZE***Unknown**	-		-0.530		-0.755	
	-		(0.609)		(0.579)	
*ITYPE***DB**:*CSIZE***Unknown**	-		-1.015		-0.930	
	-		(0.697)		(0.683)	
*ITYPE***DB**:*BSIZE*	-		-0.074		-0.113	**
	-		(0.044)	.	(0.039)	
*ITYPE***ND**:*ACTION***Individual**	-		0.982		-	
	-		(0.842)		-	
*ITYPE***DB**:*ACTION***Individual**	-		0.279		-	
	-		(0.498)		-	
PUB=1:*CSIZE***Large**	-		-0.611		-	

	Base	Full		Adjusted	
	-	(0.387)		-	
PUB=1:*CSIZE***Unknown**	-	-0.103		-	
	-	(0.506)		-	
PUB=1:*BSIZE*	-	-0.045		-	
	-	(0.041)		-	
PUB=1:*ACTION***Individual**	-	-0.585		-	
	-	(0.378)		-	
*CSIZE***Large**:*BSIZE*	-	-0.008		-0.044	
	-	(0.043)		(0.037)	
*CSIZE***Unknown**:*BSIZE*	-	0.107	*	0.108	*
	-	(0.052)		(0.051)	
*CSIZE***Large**:*ACTION***Individual**	-	0.557		0.463	
	-	(0.406)		(0.345)	
*CSIZE***Unknown**:*ACTION***Individual**	-	1.347	**	1.315	**
	-	(0.491)		(0.483)	
BSIZE:*ACTION***Individual**	-	0.083	*	0.073	*
	-	(0.038)		(0.030)	
YEAR controls	Y	Y		Y	
Industry controls	Y	Y		Y	
Number of Observations	1393	1393		1393	
Degrees of Freedom	1358	1333		1349	
R^2	0.478	0.506		0.498	
AIC	6290.2	6264.3		6252.8	

Values in parentheses are standard errors of their corresponding estimates.
Significance codes: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, . $p < 0.1$

Table 14: Regression results of three models for cost of settlement or award

Table 14 presents the estimated coefficients for the explanatory variables in all three models. By comparing the base model and the full model, we see that the full model achieves a better goodness-of-fit since it has a lower AIC value and a higher R^2. However, the interaction effects in the full model overall have low significance. To improve the model, we observe that *PSI* shows no significance in the base model and almost all interaction effects associated with this variable in the full model turn out to be insignificant. Therefore, to create the adjusted model, we removed *PSI* and all of its interaction effects. In addition, we identified those interaction effects that are insignificant in the full model, including *ITYPE*PUB*,

*ITYPE*ACTION*, *PUB*CSIZE*, *PUB*BSIZE*, and *PUB*ACTION*, and excluded them in the adjusted model. After those adjustments, the adjusted model attains a lower AIC value and an R^2 value comparable to that of the full model. Most importantly, the adjusted model is able to identify a set of significant explanatory variables. Therefore, the following discussion will be based on the results from the adjusted model.

Note that the baseline condition in this adjusted model is the following scenario: a small non-public company experiences a privacy violation incident, which affects around 190 ($\approx e^{5.2}$) records, and the company then settles a class action at the cost of approximately $10,000 ($\approx e^{9.226}$). Here, 5.2 is the mean of *BSIZE* and 9.226 is the intercept of the model. The effects of all the explanatory variables are compared to this baseline.

In terms of the incident characteristics, we first observe that whether there is a loss of personal sensitive information does not affect the settlement cost, but the type of incident does change the cost drastically. If the incident in the baseline condition is a malicious data breach incident instead of a privacy violation, the cost would increase by a factor of 6 ($\approx e^{1.816}$), where 1.816 is the coefficient of *ITYPE* when it takes the value of **DB**. For non-data-related incidents, the rate of increase could be as high as 44 ($\approx e^{3.794}$). Combining this result with what we have found about how incident type affects litigation probability, we have an interesting finding, which suggests that although privacy violations are highly likely to be litigated, there is a great chance that those cases would be dismissed or settled at a relatively low cost. In contrast, non-data-related incidents like DDoS are rarely litigated, but when they are, they can be extremely costly to settle. Malicious data breaches are in the middle ground, where the litigation probability is higher than non-data-related incidents, and their associated cost is higher than privacy violations.

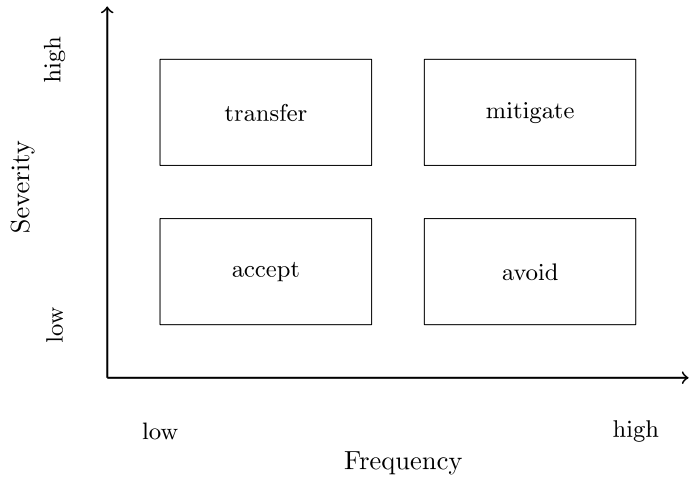


Figure 6: Risk Management Matrix

In the business environment, a commonly used guideline for enterprise risk management is the risk management matrix, as shown in Figure 6.[63] It shows the best strategies for treating risks that have different frequency-severity profiles. Based on our findings regarding the litigation probability and settlement cost of different types of cyber incidents, if we place them in this matrix, the legal risk of privacy violation would likely to be in the high-frequency-low-severity box, and in that case, risk avoidance would be the best option for managing such a risk. For non-data-related incidents, since they are rarely litigated, but carry high settlement costs, the most suitable treatment is transferring the risk to third parties, such as insurers. For malicious data breaches, depending on the company's risk appetite, either acceptance or mitigation could be the best strategy. Therefore, the results we obtain here provide valuable insights into how the legal risk of different types of cyber incidents should be treated by businesses, and how cyber insurance products should be designed to meet the most urgent needs.

In addition, the number of breached records in privacy violations and malicious data breaches also have a significant impact on the settlement cost. Compared to the baseline scenario, if the number of affected records in the privacy violation incident is increased by a factor of 2.7 ($\approx e$), the settlement cost would increase by a factor of 1.28 ($\approx e^{0.248}$). Therefore, we see that the

[63] Yi-Gean Chen & Jao-Nan Cheng, *Application of IPA on Business Risk Management for Preschools: Risk Identification and Ranking*, 22 ACAD. INT'L LEADERSHIP J. (2018); Mark Bridgers, *Applying Risk Mitigation Techniques*, NUCA BUS. J., Summer 2018, at 12.

increase in cost is not proportional to the increase in number of affected records, and the former is slower than the latter. Note that this rate of increase in cost is conditioned on that the incident is a privacy violation. Beyond that, there is also a significant interaction effect of *ITYPE* and *BSIZE*. That tells us when the incident is a malicious data breach event, there is a reduction of 0.113 in the size of the effect of *BSIZE*. Specifically, if the number of affected records in a malicious data breach is still increased by a factor of 2.7 ($\approx e$), the increase in settlement cost would only increase by a factor of 1.14 ($\approx e^{0.248-0.113}$). This finding suggests that for data breach events, when the legal costs are a concern, the number of breached records may not be a good proxy for the severity of the incident. Regarding the effect of company characteristics on settlement cost, we observe that company size shows no or little statistical significance. That is, large companies do not necessarily bear higher settlement costs than smaller companies do. However, the status of being publicly traded or not is deterministic. Compared to the non-public company described in the baseline scenario, we observe that the settlement cost would be 1.9 ($\approx e^{0.639}$) times higher if it is a public company. Associated with our findings in Section 2, this suggests that given the same size, public companies in general face a higher litigation probability than non-public companies, and the cases can be more costly to settle.

Lastly, we compare between individual actions and class actions, and it should be to no one's surprise that class actions are more expensive to settle. When all other conditions are fixed, class actions cost about 10 ($\approx e^{2.367}$) times the settlement amount compared to individual actions. However, as previously mentioned, class actions are more likely to be dismissed than individual actions for not meeting the certification requirements, and therefore, this can be considered as another instance of where the legal risk has a low frequency but a high impact, and companies should treat this risk accordingly. Despite the fact that individual actions are less costly, they slightly enlarge the effect of *BSIZE* by 0.073 because of the interaction effect of *BSIZE* and *ACTION*. That means the cost of individual actions is more sensitive to the size of the breach compared to the cost of class actions.

IV. LIMITATIONS

In this study, we examined the likelihood and cost of cyber litigation. There are several limitations in this study that can potentially be addressed in the future.

The first major limitation is that there is the sampling bias as discussed in Section 2.2, which cannot be mitigated at this moment until a more representative dataset is built. The existing data collection procedure favors incidents that are reported and known to the public. In many cases, the publicity results from court documents, thus causing an imbalanced sample with an overwhelming number of litigated incidents. This inflates the estimated litigation probability, which prevents us from getting reliable estimates on litigation probabilities.

Second, although we have information on why an incident is litigated, we do not have information on why an incident is not litigated, and that may depend on the unspoken considerations of the affected parties involved in the incident. Because of that, it is difficult to explain some of our findings, such as the negative relationship between breach size and litigation probability for privacy violation events caused by some incidents that affect a large number of records, but which are not litigated. A related but slightly different issue is that the statistical analysis we conduct does not provide insights into the root causes of certain effects, such as the higher legal risk exposure that small companies face. Similarly, although the hypothesized effect that public companies have a higher litigation probability is tested positive, a more thorough investigation on individual court documents is needed to determine how many of them are indeed shareholder derivative lawsuits, as we suspect.

Third, we suspect that many privacy violation and malicious data breach cases are dismissed for the lack of Article III standing. Although we performed a text search and found many cases are indeed dismissed for this reason, it is still not definitive evidence of the claim that the high dismissal rate is mainly attributed to the lack of standing. A more careful case review could be carried out to prove or disprove this claim.

V. CONCLUSION

In the first part of this study, we have shown that there is a substantial legal risk associated with cyber incidents, and the litigation probability depends on many factors. We examined a list of explanatory variables related to litigation probability, including incident type, whether or not there is the loss of personal sensitive information, number of breached records, company size, and whether or not the company is publicly traded. All of these variables have statistically significant main effects or interaction effects, but the size of the effect varies.

We find that the size and the type of a company have a great impact on the probability of it experiencing lawsuits after cyber incidents. Small

companies overall have a higher litigation probability than large ones, whereas public companies are riskier than nonpublic ones. This makes small, public companies the riskiest group among all companies.

In addition, the litigation probabilities of different types of cyber incidents differ drastically. Non-data-related cyber incidents have an extremely low litigation rate, and although privacy violations and malicious data breaches are both data-related incidents, the litigation rate of privacy violations is much higher than malicious data breaches. The difficulty in proving inadequate cyber security and the high barrier of class action might be the reasons for why malicious data breaches have a low litigation probability. Based on this result, we recommend that there should be a statutory duty to secure data so that the barriers for litigating data breach events may be lowered by making it easier for individuals impacted by data breaches to seek relief in court.

Loss of personal sensitive information has significant but small impact on litigation probability, except for small and public companies. Similarly, the number of breached records is statistically significant, but the increase in litigation probability for malicious data breach events is marginal, even if there is a substantial increase in the number of breached records.

Furthermore, we compared between models with and without interactions terms and found that many of the interaction effects exist and including interaction terms improves the statistical fit of our model. That is, the effect of one variable may depend on the value of other variables. This information suggests that it is not sufficient to only consider the isolated effects of explanatory variables, and this is especially useful for insurers and insurtech companies in predictive modeling.

In the second part of this study, we examined the dismissal rate and settlement cost of cyber-related litigation cases.

First, we find that around 50% of the cases are dismissed, and one reason could be the lack of Article III standing in data injury events. That is, the plaintiff fails to demonstrate that the loss of data causes substantial harm or concrete injury to satisfy the requirements for standing. Moreover, we find that class actions are more likely to be dismissed than individual actions, possibly because of the difficulty in meeting certification requirements under Rule 23.

Then, we identified a set of explanatory variables that can impact the cost of settling a case. We find that privacy violations, despite their high litigation rate, cost much less than malicious data breaches and non-data-related incidents. Additionally, a larger number of breached records would result in a higher settlement cost. Moreover, compared to nonpublic

companies, public companies bear higher settlement costs, and compared to individual actions, class actions cost more to settle.

This study has several implications. In terms of policymaking, the observed difference between malicious data breach incidents and privacy violation incidents suggests that there are hurdles in establishing a company's duty to secure data vel non, and thus it may be socially beneficial if courts and/or legislatures can recognize this legal duty to make it easier for the victims of data breaches to seek redress through the legal system.

Regarding cyber risk management, our findings show that different types of cyber incidents are associated with legal risks that have different frequency-severity profiles. Those insights can be embedded in enterprise risk management for choosing optimal risk treatment techniques. For risks that have a low frequency but a high impact, such as the legal risk of non-data-related incidents and the risk of facing class actions, risk transfer is typically a recommended treatment, and this highlights the importance of cyber insurance. Businesses need to consider the role of cyber insurance in their cyber risk management framework, and at the same time, insurers may want to take a more focused approach when developing cyber insurance products to meet market needs.

APPENDICES

A. DEFINITION OF INCIDENT TYPES

DB:
Data breaches caused by hacking, which includes incidents resulting from

- Malicious data breach,
- Physically lost or stolen data storage devices.

PV:
Data breaches and privacy violations caused by improper data disclosure and collection, which includes incidents resulting from

- Unauthorized contact or disclosure of privacy,
- Unauthorized data collection,
- Unintentional disclosure of data.

ND:
Cyber incidents that do not involve the breach of confidential information, including incidents that are

- Fraudulent use of identity,
- Phishing, spoofing and social engineering,
- Configuration and implementation errors in IT systems,

- Processing errors in IT systems,
- Cyber extortion,
- Network and website disruption,
- Skimming and physical tampering,
- Failure of industrial control and operation systems,
- Identity theft,
- Denial of service,
- Other.

B. COMPANY TYPES IN ORIGINAL DATASET

Public

- Public
- Public subsidiary, formerly public
- Public subsidiary

Nonpublic

- Private
- Private, formerly public
- Investment fund
- Nonprofit
- Government

C. ADDRESSING MISSINGNESS IN *BSIZE*

Table 15 describes the number of missing values of *BSIZE* in each category of incidents before those missing values are dealt with. Based on the incident type, we propose different methods to address the missing values issue. Some incidents do not have known number of breached records simply because those incidents are not data related, *i.e.*, the value of *ITYPE* variable is **ND**. Thus, we believe it is reasonable to fill the missing *BSIZE* values of those incidents with 0, and we can recover 1,469 missing values in that way.

	ITYPE		
	ND	**DB**	**PV**
Observations with missing *BSIZE*	1469	532	4546
Total observations	2709	2586	24679

Table 15: Number of missing values of *BSIZE* (number of breached records) in each class of *ITYPE* (Incident type) they are imputed or removed.

For those missing values in the other two *ITYPE* classes, *i.e.*, **DB**, **PV**, we are not able to impute their values in the same way. Because they only constitute a small proportion of each class, we simply discard those observations with missing *BSIZE* values. This removal leads to a final sample that is complete and has a size of 24,896 as mentioned in the main text. We use this complete sample for our analysis in this study.

WHAT EVEN IS A BITCOIN? COMMENT ON HOW DEFINING CRYPTOCURRENCY WILL HAVE DIFFERENT IMPLICATIONS FOR COVERAGE UNDER A HOMEOWNERS POLICY

MALLORY STONE*

TABLE OF CONTENTS

I. INTRODUCTION

Cryptocurrency is a recent technological development that poses numerous legal challenges. In particular, insurance companies face a new virtual asset that may need to be covered. More and more people are beginning to invest in this unconventional type of currency. Approximately 360,000 transactions are sent daily on the Bitcoin pay system.[1] Owning cryptocurrency, such as Bitcoin, occupies many risks—risks that the insurance industry has, and will find themselves being asked to protect. Cryptocurrency is entirely virtual and not backed by any government, making this wholly uncharted territory. The legal classification of cryptocurrency has yet to be defined; however, different regulatory agencies have taken steps to try to classify the volatile virtual currency. Even still, there is no clear direction for the insurance industry on how to properly define cryptocurrency.

In this Comment, I will explore how coverage for cryptocurrency assets under a homeowners policy can depend on which definition the assets fall under, in conjunction with the implications of a recent trial court decision. Section II of this comment gives a general background on cryptocurrency. Section III discusses a recent trial court case, *Kimmelman v. Wayne Insurance Group*, that has taken a

* J.D., University School of Law 2021; B.A., Political Science, Loyola University Maryland 2018.

[1] Scott D. Hughes, *Cryptocurrency Regulations and Enforcement in the U.S.*, 45 W. ST. L. REV. 1, 5 (2017).

stance on how cryptocurrency should be defined under a homeowners policy. Section IV discusses different classifications of cryptocurrency from different regulatory agencies. Additionally, this section will look to international influences to see how other countries are classifying cryptocurrency. Section V discusses different options for both insurers and policyholders for dealing with cryptocurrency and the challenges it presents. Finally, Section VI contains a brief conclusion of the Comment, incorporating the author's notes.

II. BACKGROUND ON CRYPTOCURRENCY

Cryptocurrency, at its core, is a form of virtual currency that uses cryptography as a security mechanism for creating units of currency.[2] However, not all cryptocurrency was intended to be used as traditional currency.[3] Some developments were created to be platforms for new applications, instead of a way of transferring tokens.[4] Nowadays, most cryptocurrency technology is used to exchange virtual coins and tokens.[5] Like most digital money, it is not backed by a central bank or funded by any government.[6] This type of currency does not rely on a centralized authority to regulate its transactions,[7] thus it offers consumers various benefits, such as lower transaction fees and a quicker method for transferring payment.[8] An obstacle to digital currency is the problem of "double-spending," or using a unit of currency more than once.[9] In 2008, Satoshi Nakamoto created a system, known as Bitcoin, that resolved this double-spending problem.[10] Nakamoto developed an electric payment system that verified all transactions with one

---

[2] SAMAN JAFARI, TIEN VO-HUU, BAHRUZ JABIYEV, ALEJANDRO MERA, & REZA MIRZAZADE FARKHANI, CRYPTOCURRENCY: A CHALLENGE TO LEGAL SYSTEM 3 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172489.

[3] Carol R. Goforth, *U.S. Law: Crypto is Money, Property, a Commodity, and a Security, All at the Same Time*, 49 J. FIN. TRANSFORMATION 102, 102 (2019).

[4] Michael Menapace, *Individuals Should Not Rely on Insurance to Protect Their Cryptocurrency Holdings*, TRIPLE-I BLOG (Feb. 11, 2020), https://www.iii.org/insuranceindustryblog/individuals-should-not-rely-on-insurance-to-protect-their-cryptocurrency-holdings.

[5] *Id.*

[6] JAFARI ET AL., *supra* note 2.

[7] Joseph Lavoie, *A Cryptocurrency Orientation for Property Insurance Professionals*, 49 AM. BAR ASS'N 1 (2019).

[8] JAFARI ET AL., *supra* note 2.

[9] Lavoie, *supra* note 7, at 2.

[10] *Id.*

decentralized distributed ledger, therefore, preventing individuals from fraudulently spending the same unit of currency more than once.[11]

Cryptocurrency uses a blockchain that records all the transactions and stores all other information relating to the virtual currency.[12] This is Bitcoin's ledger. The blockchain is coded with cryptography, giving each participant a unique coded signature, also known as a key.[13] In order for a transaction to be validated, both the sender and the receiver must sign with their respective keys. Then, the transaction is sent to the virtual network for validation, where it is recorded on the blockchain.[14]

Since Bitcoin's inception in 2008, numerous other virtual currencies have developed, including Ethereum, Litecoin, and Ripple.[15] While these virtual currencies follow the same model, Bitcoin still stands as the most profitable and widely used form of cryptocurrency to date.[16]

III. A CASE OF FIRST IMPRESSION

Recently, in Kimmelman v. Wayne Insurance Group, an Ohio Trial Court considered whether Bitcoin was recognized under a homeowners policy as money or property.[17] In August of 2017, the Plaintiff, James Kimmelman, reported a claim for stolen Bitcoin to the Defendant, Wayne Insurance Company ("the insurer"). Kimmelman had a standard homeowners policy with the insurer.[18] The Bitcoin was

---

[11] *Id.* at 2 ("Bitcoin addressed the double spending problem through complete transparency: '[t]he only way to confirm the absence of a [previous] transaction is to be aware of all transactions.'") (alteration in original) (quoting SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), https://bitcoin.org/bitcoin.pdf)).

[12] Lavoie, *supra* note 7, at 2–3.

[13] Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG. 495, 505 (2015).

[14] *Id.*

[15] *Understanding the Different Types of Cryptocurrency*, BITDEGREE (Jan. 5, 2020), https://www.bitdegree.org/tutorials/types-of-cryptocurrency/.

[16] Elizabeth Macauley, *What Are the Most Popular Cryptocurrencies?*, THE HARTFORD (Dec. 13, 2019), https://sba.thehartford.com/finance/cryptocurrency/what-are-the-most-popular-cryptocurrencies (noting as of July 2019, Bitcoin was worth $4,931 US Dollars).

[17] Kimmelman v. Wayne Ins. Grp., No. 18 CV 1041, 2018 Ohio Misc. LEXIS 1953, at *1–4 (Ct. Com. Pl. Sept. 25, 2018).

[18] William Craven, *Crypto Covered Under Homeowner's Policy? Ohio Trial Court Holds Coverage and Bad Faith Claims for Bitcoin Theft Survive Motion for Judgment on the Pleadings*, COZEN O'CONNOR, https://www.nobadfaith.com/crypto-covered-under-homeowners-policy-ohio-trial-court-holds-coverage-and-bad-faith-claims-for-bitcoin-theft-survive-motion-for-judgment-on-the-pleadings (last visited Apr. 19, 2021).

stolen from Kimmelman's personal digital wallet.[19] The homeowners policy between the two parties had a sublimit of $200 for any monetary losses suffered by the plaintiff.[20] The amount of cryptocurrency lost by Kimmelman was approximately $16,000 worth of Bitcoin.[21] After investigating the claim, the insurer determined the Bitcoin fell within the definition of monetary losses, thus covered but subject to the $200 sublimit under the policy.[22] Kimmelman disagreed, arguing that the lost Bitcoin constituted property and should not be subject to the $200 sublimit. [23] Therefore, he sued the insurer for breach of the parties' contract, the homeowners insurance policy, and bad faith on the part of the insurer.[24]

The issue before the court was whether the sublimit for monetary losses limited Kimmelman's recovery for the stolen Bitcoin.[25] The insurer claimed that, because the Bitcoin was recognized as "money" under the policy and this assessment was proper, Plaintiff failed to state a claim for bad faith or breach of contract.[26] Thus, Defendant moved for a judgment on the pleadings.[27] The trial court found that Kimmelman had properly plead his breach of contract and bad faith claims, therefore denying the Defendant's motion for judgment on the pleadings.[28]

In support of its position, the insurer cited several respected news sources that all described Bitcoin as money. [29] The sole legal reference that the insurer cited

---

[19] *Id.*

[20] Kimmelman, 2018 Ohio Misc. LEXIS 1953, at *1; *see also* Kesha Hodge, *Is Cryptocurrency Covered by Insurance? It Depends, Is Cryptocurrency "Money" or "Property"?*, MERLIN L. GRP.: PROP. INS. COVERAGE L. BLOG (Oct. 17, 2018), https://www.propertyinsurancecoveragelaw.com/2018/10/articles/insurance/is-cryptocurrency-covered-by-insurance-it-depends-is-cryptocurrency-money-or-property/ ("The special limit for each category shown below is the total limit for each loss of all property in that category. These special limits do no [sic] increase the Coverage C limit of liability. a. $200 on money, bank notes, bullion, gold other than goldware, silver other than silverware, platinum other than platinumware, coins, medals, scrip, stored value cards and smart cards.").

[21] *Kimmelman*, 2018 Ohio Misc. LEXIS 1953, at *1.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.* at *3–4.

[29] *Id.* at *2–3 (noting the Wayne Insurance Group cited articles from CNN, CNET and The New York Times in its motion; all of the articles cited recognized cryptocurrency as "money"*).*

was the Internal Revenue Service ("IRS") Notice 2014-21.[30] The insurer claimed that the IRS Notice 2014-21 supported its assessment of Bitcoin as money because the IRS referred to the cryptocurrency as "virtual currency."[31] The court dismissed this argument, determining that the defendant was only citing a limited portion of said notice.[32] Further in Notice 2014-21, the IRS stated, "For federal tax purposes, virtual currency is treated as *property.*"[33] The trial court found that this supported the conclusion that Bitcoin should be considered property under the homeowners policy, not money.[34] Therefore, the loss was covered and not subject to the $200 sublimit for monetary losses.[35]

It is unclear whether a court will reiterate this position if the two parties file additional motions or how the outcome of the case may be affected with subsequent proceedings. The homeowners policy also contained limits for recovery of "electronic funds" ($500) and "securities" ($1,500). [36] The court's opinion did not contain an analysis of whether any other sublimit could apply to the Bitcoin.[37] *Kimmelman* highlights the lack of caselaw and regulation for a court to rely on in determining the legal treatment of cryptocurrency.

IV. DEVELOPING CLASSIFICATIONS OF CRYPTOCURRENCY

How do we classify this new asset, one that seems malleable enough to fit many legal definitions? Despite the lack of authority on the definition of cryptocurrency for courts to rely on, various regulatory authorities have begun to develop their own definition of cryptocurrency.

For one, the Financial Crimes Enforcement Network (FinCEN) issued guidance on virtual currency in 2013.[38] The guidance defined virtual currency as a:

> [M]edium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status

[30] *Id.* at *3.
[31] *Id.*
[32] *Id.* at *3–4.
[33] I.R.S. Notice 2014-21 (2014) (emphasis added).
[34] *Kimmelman*, 2018 Ohio Misc. LEXIS 1953, at *3–4.
[35] *Id.*
[36] Craven, *supra* note 18.
[37] *Id.*
[38] Hughes & Middlebrook, *supra* note 13, at 501.

> . . . virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.[39]

The term *legal tender* refers to a form of money that is lawfully established by the government.[40] For FinCEN, along with other regulatory agencies, cryptocurrency does not establish the legal tender necessary to equate the virtual money to actual currency.[41]

The Securities and Exchange Commission took a different stance on cryptocurrency. The Chairman of the SEC, Jay Clayton, made a statement urging that the SEC "appl[y] longstanding securities law principles to demonstrate that a particular token constituted an investment contract and was therefore a security under our federal securities law."[42] The SEC believed that cryptocurrency should be treated no differently than other tangible currency,[43] like dollars or bank notes. Whether cryptocurrency will be treated as a security, and therefore fall under the purview of the SEC, is still undetermined.[44]

The IRS made clear that cryptocurrency was to be treated, for tax purposes, as virtual currency taxable as property.[45] The IRS did not classify this asset as currency, following the lead of the FinCEN.[46] In Notice 2014-21, the IRS addressed how tax principles were going to be applied to transactions using virtual currency.[47]

---

[39] FIN. CRIMES ENF'T NETWORK, DEP'T OF TREASURY, FIN-2013-G001, APPLICATION OF THE FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[40] Hughes & Middlebrook, *supra* note 13, at 505. *See also id.* at 503 ("'Legal tender' . . . refers to a form of national money lawfully established by the government to serve as a medium of payment of taxes and used for commercial exchange.").

[41] Deidre A. Liedel, *The Taxation of Bitcoin: How the IRS Views Cryptocurrencies*, 66 DRAKE L. REV. 107, 126 (2018).

[42] Kellis K. Tankersley, Ashley R. Davis & Alexandra G. Ah Loy, *Legal and Regulatory Developments Arising from the Growth of Cryptocurrency*, 89 OKLA. B.J. 18, 20 (2018).

[43] *Id.*

[44] The complex analysis of what constitutes a security and how the decentralized nature of cryptocurrency presents challenges to the SEC falls outside the scope of this Comment. For more information on this topic, see Peter Van Valkenburgh, *What Could "Decentralization" Mean in the Context of the Law?*, COIN CTR. (June 15, 2018), https://coincenter.org/entry/what-could-decentralization-mean-in-the-context-of-the-law.

[45] Tankersley et al., *supra* note 42, at 21; *see also* Hodge, *supra* note 20.

[46] Goforth, *supra* note 3, at 104.

[47] Liedel, *supra* note 41, at 116.

The Notice stated, "[f]or federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency."[48]

While these definitions seem very similar, each has its own implications. Coverage for specific losses is often limited based upon the language in an insurance policy.[49] The limitations can differ based on the definition the lost asset falls under.[50] Many insurance policies limit the amount recoverable for losses of "money," "securities," or "other property."[51] If cryptocurrency fits within one of these categories, then there may be different types of coverage. Kimmelman was not subject to a $200 limit for coverage because the trial court concluded the lost Bitcoin fell under the "other property" coverage of the homeowners policy, moving the lost asset out of the "money" coverage. Evidently, the difference in coverage will depend on what classification is given to the virtual coins. However, if cryptocurrency does not fit within these categories of coverage, then there may be *no* coverage, depending on the language of the homeowners policy.[52]

A potential source of guidance can be found outside of regulatory authorities of the United States. Regulators can look to observe how other countries are classifying cryptocurrency, as an international influence can offer direction in how to define the virtual currency. In the United Kingdom, the government has classified cryptocurrency as having its own "unique identity."[53] Basically, cryptocurrency is not viewed as investment or payment mechanisms[54]—it is in a category all on its own. For tax purposes, the taxation of a cryptocurrency transaction depends on the activity and the parties involved.[55]

In Russia and Japan, cryptocurrency is classified as property. Similar to the IRS, these two countries tax cryptocurrency as though it is property, not money.[56] In Russia, a bill was proposed in 2018 that classified virtual currency, coins and

---

[48] I.R.S. Notice 2014-21 (2014).

[49] TOM BAKER & KYLE D. LOGUE, INSURANCE LAW AND POLICY 145 (4th ed. 2017).

[50] Leland Jones, Edward Brown & Bonnie Thompson, *Cryptocurrencies: Money, Securities or Other Property?*, LAW 360 (Feb. 23, 2018, 1:54 PM), https://www.law360.com/articles/1015602.

[51] *Id.*

[52] *Id.*

[53] GLOB. LEGAL RSCH. CTR, U.S. L. LIBR. CONG., REGULATION OF CRYPTOCURRENCY AROUND THE WORLD, 59 (2018) [hereinafter GLOBAL]; *see also Cryptocurrency Regulations in the UK*, COMPLY ADVANTAGE, https://complyadvantage.com/knowledgebase/crypto-regulations/ cryptocurrency-regulations-uk-united-kingdom (last visited Apr. 18, 2021).

[54] GLOBAL, *supra* note 53.

[55] *Id.*

[56] *Id.* at 75–76, 111.

tokens, as property having no legal tender.[57] In Japan, cryptocurrency is more regulated than in most countries. Japan's Payment Services Act defines cryptocurrency consistently as a "property value."[58]

In China, regulators have not recognized virtual currency as a substitute for paper bills, coins or credit cards.[59] China took a step further and banned the use of cryptocurrency in the market as currency, reasoning that assets like Bitcoin do not have the requisite legal tender and are not issued or backed by any monetary authority.[60] The Chinese government seems to agree with FinCEN; however, takes it a step further by clearly establishing that virtual currency cannot be used as currency in its market.

VI. WHAT CAN AN INSURER OR A POLICYHOLDER DO?

From an insurer's perspective, there are a few options for dealing with the challenges that cryptocurrency presents. The first step that insurers can take is explicitly defining cryptocurrency within their homeowners policies. By defining what the policy will recognize as cryptocurrency, the insurer can prevent a policyholder from arguing the policy is unclear or ambiguous.[61] If Wayne Insurance Company had defined money to include cryptocurrency within the policy, then it would have had a stronger argument that Kimmelman was limited to only recovering $200, rather than the $16,000. The court may not have looked to outside sources, such as the IRS Notice, to determine what was covered as money or property under the agreed upon policy.

The attempt to navigate cryptocurrency does not stop with an insurer plainly drafting how cryptocurrency will be recognized under a homeowners policy. The next issue that could arise for insurers issuing homeowners policies is whether the loss of cryptocurrency will constitute a named peril. In a homeowners policy, the insurer can outline certain claims for loss of personal property that are only covered when the damage results from a specifically named peril.[62] Unlike coverage for a

---

[57] *Id.* at 75–76.

[58] *Id.* at 111–12.

[59] *Id.* at 106.

[60] *Id.* at 106–07; *see also Cryptocurrency Regulations in China*, COMPLY ADVANTAGE, https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-china/ (last visited Apr. 20, 2021).

[61] BAKER & LOGUE, *supra* note 49, at 180.

[62] *Id.* at 145.

dwelling in a homeowners policy,[63] coverage for personal property can be limited based on how the property is lost. Policy drafters can limit the causes of loss for cryptocurrency within the homeowners policy.

After the definition and causation issues of cryptocurrency are addressed by a homeowners policy, the insurer may also have a valuation problem when covering cryptocurrency. Should the recovery be the value of the Bitcoin at the time it was lost? Or should the cost reflect the value of the Bitcoin at the time of recovery for loss, given the fact that the value of Bitcoin is constantly changing?[64]

Additionally, insurers can create policies specifically designed to protect cryptocurrency, also known as crypto-insurance policies. These policies often come with high premiums, reflecting the risky nature of virtual money.[65] One problem that insurers face with crypto-insurance policies is valuation. The value of cryptocurrency continues to fluctuate at rapidly different rates compared to currency or gold.[66] The price volatility of cryptocurrency makes it a challenge for insurers to create a pricing model to insure such assets.[67] Not only that, but there is little history for professionals to base the risk calculation on.[68] Actuaries will have a difficulty pricing the risk of a Bitcoin, due to its volatile nature and the lack of historical data. When a policy is covering an unpredictable risk, the price of the respective premium will rise exponentially.[69]

Another issue for insurers to consider when developing a crypto-insurance policy is moral hazard. Moral hazard is a principle of insurance that describes the theoretical tendency for individuals who purchase insurance to subsequently act more carelessly.[70] This principle applied in the cryptocurrency context could amount to a policyholder taking larger risks if she believes her virtual money will be covered. A policyholder could make riskier moves with her cryptocurrency, using cheaper—and therefore—less secure networks for purchasing virtual coins or tokens.[71] This

---

[63] *Id.* (noting that coverage for a dwelling in a homeowners policy typically falls under an all-risk policy. If not excluded, the loss will be covered no matter the reason for the loss).

[64] The complex issue of valuing cryptocurrency after it has been determined that the homeowners policy covers a cryptocurrency loss falls outside the scope of this comment.

[65] Michael Abramowicz, *Cryptoinsurance*, 50 WAKE FOREST L. REV. 671, 690 (2015).

[66] *Id.* at 681.

[67] Jonathan McGoran, *Cryptocurrency Is a Massive Uninsurable Risk: Here's How to Protect Your Assets*, RISK & INS. (Mar. 18, 2020), https://riskandinsurance.com/cryptocurrency-is-a-massive-uninsurable-risk-heres-how-to-protect-your-assets/.

[68] *Id.*

[69] *See* BAKER & LOGUE, *supra* note 49, at 8.

[70] *Id.* at 6–7.

[71] Menapace, *supra* note 4.

could make policyholders more vulnerable to hackers and phishing scams.[72] Depending on the policy language, insurers issuing crypto-insurance policies could be on the hook for coverage in these scenarios, even though it was the policyholder who took an unnecessary risk.

Another option for insurers is to explicitly exclude cryptocurrency from coverage. An insurer can limit its liability by making it clear that cryptocurrency is not covered within its homeowners policy through an exclusion.[73] For example, in response to the onset of cryptocurrency and crime, the Insurance Service Office created a broad exclusion within its commercial crime program to address cryptocurrency.[74] Insurers can follow this example and create an explicit exclusion within a homeowners policy.

While cryptocurrency is still relatively new, insurers should prepare for more policyholders to want their virtual currency to be covered. If insurance companies do not take steps to navigate this innovative and complicated issue, they may find themselves subject to some pricey payouts.

Alternatively, there are steps a policyholder can take to protect her interest in her virtual money. First and foremost, an informed consumer of insurance is always better situated than an uninformed consumer. If a policyholder is concerned about protecting her virtual currency, then she must be diligent in researching the kind of insurance coverage she is purchasing. During initial discussions and negotiations with an insurer, she must make it known that she is seeking a policy that would cover her cryptocurrency. As we have seen, some courts may find coverage under homeowners policies for cryptocurrency;[75] however, there is no guarantee that other courts will follow this example. Not only that, but policyholders will be better protected with policies that explicitly define cryptocurrency as either money or property. This way, policyholders are on notice for how this new type of currency is being classified by the insurers under the policy. Then, if an insurer subsequently tries to deny coverage, the policyholder will have several legal

---

[72] Fiona A. Chaney, *2 Avenues of Insurance Coverage for Cryptocurrency Theft*, LAW 360 (June 20, 2018, 3:30 PM), https://www.law360.com/articles/1055625/2-avenues-of-insurance-coverage-for-cryptocurrency-theft.

[73] Craven, *supra* note 18.

[74] Jones et al., *supra* note 50; *see also* Chaney, *supra* note 72 ("[I]ncluded an exclusion to its form commercial crime policy stating that it did not cover 'loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious, including, but not limited to, digital currency, crypto currency, or any other type of electronic currency.'").

[75] Kimmelman, 2018 Ohio Misc. LEXIS 1953, at *1–4.

doctrines to argue that her virtual money was in fact covered under the policy issued.[76]

VII. CONCLUSION

While *Kimmelman v. Wayne Insurance Group* does not present a source of authoritative precedent as it has only reached the trial court level, the case can give both insurers and policyholders a sense of how a court may rule, should a similar issue be litigated in the future. *Kimmelman* represents the first pro-policyholder decision that will likely be cited in future cases addressing the legal identity of cryptocurrency in relation to a homeowners policy. This area of insurance law is still uncertain. With the increasing use of cryptocurrency and the emerging risks that technology presents, other courts may soon find themselves having to take a stance on how this asset is legally defined. One option for the courts is to follow the IRS and the Ohio trial court's ruling in *Kimmelman* in viewing cryptocurrency as property. The legal definition of cryptocurrency remains unclear, but we have seen the first steps taken by a trial court to determine what even is a Bitcoin.

[76] Policyholders have within their toolbox of legal doctrines many legal foundations for arguing for coverage. These include, but are not limited to, the doctrine of contra proferentum, the doctrine of reasonable expectations, and the doctrine of unconscionability. The application of these legal doctrines on a cryptocurrency coverage challenge are outside the scope of this comment.